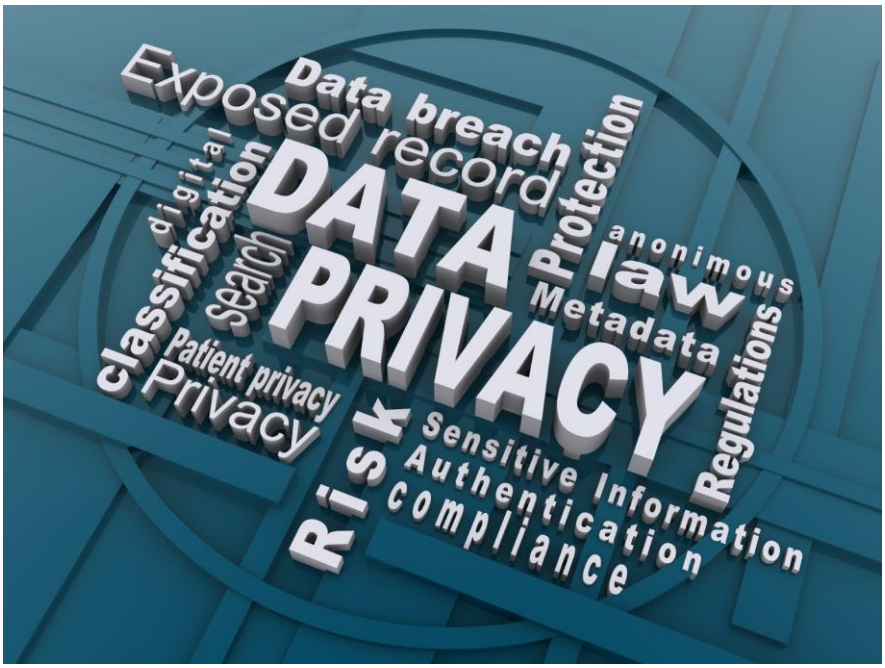
1021804036

Algemene Verordening Gegevensverwerking (AVG)

Een overzicht wat te doen.



General Data Protection Regulation (GDPR, 2016/279)

Inhoudsopgave

In dit overzicht treft u achtereenvolgens aan:

1021804036

Wat is de Algemene Verordening Gegevensbescherming?
Dit is de nieuwe privacywetgeving die vanaf 25 mei 2018 van kracht wordt en borduurt in feite door op de reeds bestaande privacywetgeving. Het zijn de Europese normen die voor de hele EU gaan gelden voor alle bedrijven en organisaties die persoonsgegevens vastleggen van klanten, personeel of andere personen. Namen, adressen, maar ook gegevens gekoppeld aan IP-, MAC-adressen, cookies, etc. vallen hieronder, ook al is niet direct bekend wie er als persoon achter zit. Overigens geldt dit ook voor camerabeelden waarop personen geregistreerd worden.

De wet is opgesteld met als nadruk dat u als organisatie moet aantonen dat u voldoet aan de wet.

De Autoriteit Persoonsgegevens heeft een stappenplan opgezet, in de bijlage een kort overzicht.

Wat verandert er allemaal?
1. Activiteiten vallen sneller onder de privacywetgeving.
2. De privacyverklaring moeten transparanter en duidelijker.
3. Alle datalekken moeten intern worden gedocumenteerd.
4. Alle verwerkingen van persoonlijke gegevens documenteren, ook nieuwsbrieven.
5. Verwerkersovereenkomsten afsluiten met leveranciers en afnemers (voorheen bewerkersovereenkomst).
6. Boetes zijn zeer hoog.
7. Soms is er een speciale privacy officer nodig (Functionaris Gegevensbescherming).
8. Bij risicovolle verwerking dient een Privacy Impact Assessment vooraf te gaan.
9. Privacygevoelige informatie mag zo weinig mogelijk verzameld en moet zo snel mogelijk weer verwijderd worden.
10. Software en diensten moeten vanaf ontwerp rekening houden met privacy.
11. De beveiliging moet op orde zijn.
12. Er is een intern privacy beleid gepubliceerd waarin staat wie welke rol heeft bij omgang persoonsgegevens.
13. Er is recht op inzage en correctie.
14. Onlinediensten waarbij persoonsgegevens worden bijgehouden moeten geëxporteerd kunnen worden in een standaardformaat voor transport naar een andere bestemming.
15. Bij handel met het buitenland is van belang of binnen of buiten de EU-persoonsgegevens worden opgeslagen. Voor buiten de EU gelden speciale regels.
16. Interesseprofielen of risicoanalyse van klanten/bezoekers moeten voorzien zijn van uitleg en doel.
17. Bij gebruik biometrie voor bijvoorbeeld toegangsvereisten is extra alertheid i.v.m. zwaardere eisen.

Wat zijn uw 10 stappen

Stap 1: Zorg dat iedereen in de organisatie weet dat er nieuwe privacyregels gelden en dat er daardoor ook nieuwe afspraken gemaakt worden die conform wet zijn. Maar ook dat niet zomaar meer gegevens van klanten, derden, personen bewaard, opgetekend, dan wel geregistreerd worden zonder dat de AVG-procedure hiervoor doorlopen is. Naast bewustwording is het dus zaak een procedure/protocol op te stellen waarin in eenvoudige taal verwoord wordt wat wel/niet mag en wie verantwoordelijk is voor het registreren van gegevens en wat daar vervolgens mee gedaan wordt. De hiervoor gestelde stappen kunt u als basis voor het bedrijfsspecifieke protocol hanteren.

- ***Stel protocol persoonsgegevens op***
- ***Leg vast dat werknemers verplicht zijn datalekken en niet navolgen privacy voorschriften te melden***

Stap 2: Informeer door middel van een privacyverklaring die eenvoudig te vinden moet zijn wanneer u persoonsgegevens vraagt. Daarin is minimaal verwoord:
– uw bedrijfsgegevens met de identiteit en contactgegevens van de eindverantwoordelijke
– de contactgegevens van de eventuele verwerkingsverantwoordelijke (Functionaris Gegevensbescherming)
– doel, gebruik en wettelijke basis van registratie
– welke gegevens geregistreerd worden
– met wie deze gedeeld (kunnen/moeten) worden
– de bewaartermijn
– uitleg over cookies en de reden van gebruik
– de beveiligingsmaatregelen die getroffen zijn rondom de vastgelegde gegevens
– recht op inzage, correctie, verwijdering en het meenemen van eigen gegevens (dit is een al bestaand recht)
– recht op intrekking van verleende toestemming
– mogelijkheid klachtenrecht (via Autoriteit Persoonsgegevens)
– verklaring van het gerechtvaardigd belang van de verantwoordelijke indien de verwerking is gebaseerd op een gerechtvaardigd belang.

Klanten moeten dus kunnen nalezen over: **identiteiten - doel – registratiegegevens - gebruik cookies - rechten inzage en correctie/verwijdering - beveiliging**

Personen moeten actief toestemming geven om persoonsgegevens te verwerken. Het is bijvoorbeeld verboden om een toestemmingskeuze vooraf standaard te hebben aangekruist. Intrekken van die toestemming moet net zo eenvoudig zijn als het verlenen daarvan. Dit is eveneens van toepassing wanneer de gegevens via andere bronnen dan door de persoon zelf is verwerkt. In dat geval moet de bron vermeld worden en welke gegevens gebruikt zijn

(bijvoorbeeld sociale media). Daarnaast kan verwerking van persoonsgegevens nodig zijn zonder toestemming omdat:

- verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de persoon partij is
- verwerking volgt uit een wettelijke verantwoordelijkheid
- verwerking noodzakelijk is om vitale belangen persoon te beschermen
- verwerking noodzakelijk is voor de vervulling van een taak voor het algemeen belang
- verwerking noodzakelijk is voor behartiging van het legitiem belang van de verwerkersverantwoordelijke.

Er is dus altijd een van deze grondslagen noodzakelijk en deze moet vooraf bekend zijn.

De bewaartermijn is de strikt noodzakelijke en alleen voor het oorspronkelijke doel. Bij bijvoorbeeld een recruitment mogen gegevens na afwijzing alleen met instemming voor een mogelijk vervolg bewaard worden.

Zie hier een uitgebreid voorbeeld van een privacyverklaring voor een gemeentelijke website. Op internet zijn diverse autogeneratoren en voorbeelden te vinden voor dit soort verklaringen. Let op dat deze nog niet allemaal zijn ingericht op de nieuwe privacywetgeving.

- **Zorg voor vindbare privacyverklaring**
- **Alleen noodzakelijke registratie**
- **Actieve toestemmingsverklaring**

Stap 3: Houdt een verwerkingsregister bij, dit is een verplichting. Documentatie en accountability plicht (u voldoet aan de wet) moet aantoonbaar zijn.

- wanneer u meer dan 250 werknemers heeft
- risicovolle persoonsgegevens verwerkt, zoals gezondheid, religie, politieke geaardheid, etc.
- gegevens structureel en niet incidenteel verwerkt
  De meeste bedrijven worden dus verplicht gezien klanten/leveranciers- of personeelsbeheer.

  Op te nemen en bij te houden register vermeldt:
- contactgegevens verantwoordelijke, eventueel gezamenlijke verwerkingsverantwoordelijken en de Functionaris Gegevensbescherming
- soort persoonsgegevens
- categorieën betrokkenen
- categorieën ontvangers
- doel

- locatie opslag
- met wie gedeeld (bij wijzigingen dit eveneens weer delen)
- informatie over delen buiten EU
- bewaartermijn
- beveiliging
- logbestand met wie toegang heeft gehad.

Een voorbeeld is te vinden op PrivacyBlox.nl. Maar het kan ook in Excel.

- **Zorg voor een register verwerking persoonsgegevens**
- **Geregistreerden hebben recht op inzage logbestand van zijn/haar gegevens**

Stap 4: Bij het verwerken met hoog privacy risico is een data protection impact analyse verplicht. Zijn de risico's na analyse inderdaad hoog dan kunt u maatregelen nemen om deze te verkleinen. Een DPIA is verplicht wanneer:

- religie, gezondheid, politieke, biometrische gegevens, etc. grootschalig worden verwerkt
- systematisch mensen worden gevolgd in een publiek toegankelijk gebied (cameratoezicht bijvoorbeeld)
- profiling hanteert en gegevens combineert dat indeling in groepen mogelijk maakt
  Er zijn **negen toets criteria** op de site van Autoriteit Persoonsgegevens te vinden.

- **Check of een data protection impact analyse noodzakelijk is > JA - NEE**

Stap 5: Privacy by design en default, wat inhoudt dat u bij het inrichten van systemen en processen in uw organisatie vanaf de start alles wat met persoonsgegevensregistratie/verwerking te maken heeft opneemt. Als voorbeeld is het verzenden van digitale nieuwsbrieven, een woonplaats gegeven is dan niet relevant (al ligt het eraan hoe kwetsbaar de persoon is, dan kan een woonplaats toch relevant zijn). Daarnaast moeten de standaardinstellingen van alle systemen zo privacy vriendelijk mogelijk zijn. Zo mogen er bijvoorbeeld geen vakjes zijn aangekruist bij een webformulier. Ook mag u aan klanten geen automatische informatie toezenden wanneer hiervoor geen toestemming is gegeven.

- **Privacy by design en default is basisinrichting systemen**

Stap 6: Soms is het verplicht een Functionaris Gegevensbescherming aan te stellen. Dit is een onafhankelijk persoon die rapporteert en adviseert over naleving van de AVG-wet. De verplichting is er wanneer:

- de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan
- de kernactiviteit van uw organisatie het verwerken van persoonsgegevens is

- uw organisatie structureel mensen observeert (fysiek of digitaal)
- De functionaris kan intern- of extern (dus uit te besteden aan een andere partij) aangesteld worden.

  - **Check of een functionaris gegevensbescherming verplicht is > JA – NEE**
  - **Bij nee, leg vast waarom het niet verplicht is om aan te tonen dat er met de betreffende factoren rekening is gehouden**

Stap 7: Een datalek is het punt waar alles om draait. Data kan gehackt worden, ongeoorloofd gewijzigd, gestolen, verloren of anderszins verspreid, verstrekt of ingezien worden, buiten de kring van personen welke geautoriseerd toegang hadden tot de persoonsgegevens op basis van het verwerkingsregister en privacy protocol. Een gestolen of zoekgeraakte tablet, telefoon of papieren uitdraai kan hiertoe behoren. Dit geldt ook voor een verkeerd verzonden e-mail of brief. Er is (interne) meldplicht binnen 72 uur. Indien u gegevens voor anderen verwerkt dient u dat de opdrachtgever eveneens te melden.

Wat u moet registreren bij een datalek:

- korte omschrijving van het lek
- wanneer
- wat er met de gegevens is gebeurd
- welke groepen van personen er gegevens zijn gelekt
- hoeveel personen
- welke persoonsgegevens gelekt zijn
- gevolgen van de inbreuk (bijvoorbeeld risico op identiteitsfraude, reputatieschade)
- genomen maatregelen om schade te voorkomen/beperken (zoals bijvoorbeeld het op afstand wissen van data, wijzigen van wachtwoorden en het op voorhand gebruik van encryptie zodat gegevens onleesbaar zijn zonder sleutel)
- genomen maatregelen ter voorkomen voor volgende keer.

Doel is leren van fouten en het aantonen aan Autoriteit Persoonsgegevens dat u datalekken monitort en opvolgt. Tip is om werknemers te verplichten om alle datalekken te melden.

Niet elk datalek hoeft te worden gemeld aan de Autoriteit Persoonsgegevens. Meldingsplicht is er altijd wanneer er negatieve gevolgen zijn voor identiteitsfraude of reputatieschade. In bepaalde gevallen moet u ook de betrokkenen (over wie de gegevens gaan) op de hoogte stellen.

De EU guidelines die de basis vormen van de meldplicht zijn op dit moment nog niet definitief. U kunt de website van de Autoriteit Persoonsgegevens volgen voor de laatste informatie en ontwikkelingen.

Zie hier een uitgebreid voorbeeld van hoe gemeenten handelen bij datalekken en meldplicht zoals deze reeds luidt onder de huidige wetgeving en ook zoals het er nu uit ziet van toepassing blijft. De afwijkingen zitten met name in de boetebedragen en verplichting tot interne registratie van álle datalekken.

- **Meldplicht binnen 72 uur van een lek**
- **Registratieplicht ter monitoren en leren van lekkage**

Stap 8: Opnieuw aandacht voor de bewerkersovereenkomst, die heet nu de verwerkersovereenkomst, met bedrijven die uw persoonsgegevens verwerkt, opslaat of kan inzien, wat staat daarin, wat moet u overeenkomen:

- het doel, de aard van de verwerking en welk soort persoonsgegevens
- verwerking uitsluitend op basis van uw schriftelijke instructies en geen gebruik voor andere doeleinden
- geheimhoudingsplicht voor personen in dienst van verwerker
- de technische en organisatorische maatregelen die zijn getroffen door verwerker om de persoonsgegevens te beveiligen
- zonder schriftelijke toestemming verbod op uitvoering door een ander
- de hulp om te voldoen aan verzoeken van betrokken als het gaat om hun privacy rechten (inzage, correctie, vergetelheid en dataportabiliteit-transport)
- de hulp bij nakoming van andere verplichtingen (zoals melding datalekken)
- na afloop van de verwerkingsdienst het verwijderen van gegevens, of terugsturen, inclusief kopieën, tenzij de verwerker een bewaarplicht heeft
- de medewerking aan audits van u of een derde partij, het beschikbaar stellen van alle relevante informatie zodat bepaald kan worden dat de verwerker zich aan zijn verplichtingen houdt.

Een recent handig overzicht is te vinden op PrivacyCompany.eu.

- **Check of uw bewerkingsovereenkomsten voldoen aan de nieuwe eisen van een verwerkingsovereenkomst**
- **Ook inzage in persoonsgegevens valt onder verwerken**

Stap 9: U dient een leidend toezichthouder aan te stellen bij internationaal handelsverkeer. Deze stap is in dit kader niet verder uitgewerkt.

Stap 10: In het bezit zijn van een geldig en bewuste toestemming voor het verwerken van persoonsgegevens (anders dan berustend op wettelijke verplichting, een overeenkomst of een andere rechtsgrond). Deze moet kunnen worden ingetrokken met tevens het verzoek tot

verwijderen en/of overdracht van gegevens. De wetgeving gaat hierbij uit van specifiek en geïnformeerd. U moet kunnen laten zien op basis van welke informatie door betrokkene besloten is en welk proces hieraan ten grondslag ligt. Hoe heeft de betrokkene hiervan kennis kunnen nemen en het besluit kenbaar kunnen maken. Onder het principe van gelijk oversteken. Informatie in ruil voor actieve toestemming. Automatische registratie onder verwijzing naar websiteinformatie is onvoldoende. De informatie hoort bij de toestemming aanwezig te zijn. De link tussen verwerking en toestemming moet duidelijk aangetoond kunnen worden. Meer data verzamelen dan waarvoor is toegestaan, of dat voor het beoogde doel noodzakelijk is, is niet toegestaan. Deze stap valt samen met alle stappen hierboven waarin u voldoende heeft opgenomen en gedocumenteerd wat het doel, proces, handeling(en), opvolging(en) en monitoring is van de verwerking van persoonsgegevens.

- **Toon aan hoe geldig bewuste toestemming tot het verwerking van persoonsgegevens is verkregen**

Overzicht to do

- ☐ Verwerk stap 1 t/m 10 in een persoonsgegevens protocol.
- ☐ Maak een volledige inventarisatie gegevensverwerkingen (privacy impact assessments uitvoeren bij hoog risicoverwerkingen).
- ☐ Stel uw systemen in volgens beginselen van privacy by design/privacy by default; passende beveiligingsmaatregelen documenteren, toepassen en indien nodig updaten.
- ☐ Stel een intern schriftelijk privacybeleid en externe privacyverklaring op.
- ☐ Stel en houdt een schriftelijk register van alle gegevensverwerkingen op/bij.
- ☐ Benoem eventueel een Functionaris Gegevensbescherming;
- ☐ Pas de huidige bewerkersovereenkomsten aan, en sluit nieuwe verwerkingsovereenkomsten indien ontbrekend.
- ☐ Maak alle werknemers bewust van het belang en noodzaak van de omgang met privacygevoelige gegevens.

Uitgelicht privacy werknemer

Als werkgever verwerkt u verplicht persoonsgegevens van uw werknemer(s). Echter registreert u vaak meer dan verplicht is. Denk aan camerabeelden, e-mailverkeer dat bijgehouden wordt of het gebruik van internet dat geanalyseerd wordt (denk hierbij ook aan IP- en MAC-adressen), opnames telefoon/chatgesprekken, beheer van devices op afstand, tracking- en locatiegegevens van bedrijfsauto’s/apparatuur, etc.. Voor rechtmatige verwerking is er een wettelijke grond nodig zoals:

- voor uitvoering van de arbeidsovereenkomst
- om te voldoen aan wetgeving
- om vitale belangen van een werknemer of ander natuurlijk persoon te beschermen
- voor het vervullen van een taak van het algemeen belang (of uitoefening openbaar gezag)

- voor behartiging gerechtvaardigde belangen van u als werkgever of een derde, tenzij de fundamentele belangen van een werknemer zwaarder wegen
- toestemming van een werknemer (of diens vertegenwoordiging OR) voor één of meer specifieke doeleinden.

Toestemming is de meest gebruikelijke grondslag bij het verwerken van persoonsgegevens, maar bij een werkgever-werknemer relatie is er door de gezagsverhouding geen vrijwillige toestemming. Er moet dus altijd een andere grondslag genomen worden dan de individuele toestemming. U kunt bijvoorbeeld gebruik maken van de noodzakelijkheid i.v.m. uitvoering van de overeenkomst of de wettelijke plicht. Het belang van u als werkgever of een derde moet ook een zorgvuldige belangenafweging zijn, waarbij de noodzaak en proportionaliteit aangetoond moet worden. Deze proportionaliteit kan aangetoond worden door stap 4 te doorlopen, hierbij wordt rekening gehouden met alle omstandigheden van het geval. Ook geldt het privacy vriendelijk inrichten, stap 5, toon daarbij aan dat de juiste balans is gemaakt tussen het belang van werkgever en werknemer. Belangen van de werkgever kunnen hierbij zijn:

- bescherming van het intellectueel en materieel eigendom
- verbeteren van productiviteit
- verbeteren bescherming persoonsgegevens.

Niet toegestaan is:

- Monitoren in gevoelige ruimten (sanitaire gelegenheden, pauze of religieuze locaties)
- geautomatiseerde besluiten over prestaties
- continu registreren i.p.v. steekproefsgewijs
- heimelijke registratie (tenzij bij gegronde verdenking van een strafbaar feit of het lekken van bedrijfsgeheimen)

De privacy dient gewaarborgd te worden door:

- slechts verwerken van relevante gegevens (doelbindingeis)
- de OR heeft toestemming verleend voor het gebruik van volgsystemen
- werknemers zijn op de hoogte
- er is recht op inzage, correctie, verwijdering en blokkering
- gegevens moeten worden verwijderd en niet langer worden bewaard dan nodig is
- beveiligd door passende maatregelen (er zijn bekende standaarden zoals: ISO 27001, 27002, 27018 of NEN 7510, 7512 en 7513)

Ook nu geldt als hiervoor geschetst een informatieplicht:

- of en wanneer monitoring plaatsvind

- de doeleinden van de verwerking
- de gebruikte middelen
- overzicht gegevens en bewaartermijn
- wie toegang heeft tot welke onderdelen
- de beveiliging
- de rechten van de werknemer

Deze informatieplicht geldt ook nog eens achteraf. De werknemers die zijn gemonitord moeten hiervan op de hoogte gesteld worden.

Inzage in sociale media bij aanname, tijdens de werkzame periode of na ontslag is toegestaan onder gelijke voorwaarden als hiervoor geschetst. Bij sollicitatie dient dit vooraf kenbaar gemaakt te worden, bij controle van een concurrentiebeding na ontslag (LinkedIn). Let op, ook hier geldt dat het gerechtvaardigde belang moet opwegen tegen de privacy van de persoon.

Camerabewaking is verboden voor het monitoren van prestaties of aanwezigheid, net als gezichtsherkenning. Ook controle van mailverkeer is aan strengere eisen onderworpen. De impact op de privacy moet maximaal beschermd zijn bij datalekken door preventie software. Duidelijk en transparant moet zijn op grond waarvan selectie/registratie plaats kan vinden. Het bijhouden van het mailverkeer en alle toetsaanslagen is niet proportioneel.

Real-time volgen van vervoersmiddelen moet tegen dezelfde wijze als hiervoor afgewogen worden. Het continu volgen is niet proportioneel en maakt in de meeste gevallen te veel inbreuk op de privacy.

Voor freelancers, stagiairs en ZZP’ers kunt u bovenstaande gelijkstellen.

Tot slot

De stappen logisch opvolgen geeft voldoende inzage in hetgeen u wettelijk dient op te volgen en in te richten. Over het algemeen heeft u veel al in uitvoering en vergt dit op een aantal processen nadere beschouwing en aanscherping. Let hierbij bijvoorbeeld op het hanteren van uw algemene inkoop- en verkoopvoorwaarden en check bijvoorbeeld u personeelsbeleid op een verplichting van de melding van datalekken. Van belang is dat iedere werknemer en uzelf bent doordrongen dat privacyregels strenger worden ingevuld en persoonsgegevens op zeer veel plekken vaak onbewust in het geding zijn. Maar ook dat deze vaak eenvoudig toegankelijk zijn. Zaak is dat nu bewust te worden en af te wegen welke gegevens strikt noodzakelijk zijn en voor welk doel. Wees hierover transparant, zet een privacyverklaring op en zorg voor toestemming van verwerking. Regel een adequate beveiliging en log iedere activiteit bij verwerking. Het is goed om uw bedrijfsjurist vanaf de start te betrekken in de opzet van het protocol en mogelijke aanpassing van werkwijzen en juridische documenten.

Geraadpleegde bronnen

- Autoriteit Persoonsgegevens
- Kamer van Koophandel
- Informatie Beveiligingsdienst Gemeenten
- Servicedocument Gegevensbescherming Pensioenfederatie
- Europese Unie GDPR
- Diverse juridische, ICT en adviesorganisaties waaronder ICTrecht, Justitia.nl, Bullhorn, Nederland ICT, Privacy Management Partners, Privacy Company, AWVN en MKB servicedesk

Bijlage 1 AVG – privacywetgeving Stappenplan

1. Bewustwording: zorg dat beleidsverantwoordelijken op de hoogte zijn van de AVG. Zie de richtlijnen en instructies op www.autoriteitpersoonsgegevens.nl. Bij niet naleven is er een boete van 4% van de omzet met een maximum van 20 miljoen EURO.
2. Personen waarvan een bedrijf persoonsgegevens in bezit heeft/verwerkt, hebben recht op inzage, correctie, verwijdering en dataportabiliteit (gegevens meenemen).
3. Overzicht gegevensverwerking: deze moeten in kaart worden gebracht om te verantwoorden dat de verwerking conform AVG-wetgeving is. Het bijhouden van een register van verwerken hoort hierbij.
4. Data Protection Impact Assessment: een risico-inventarisatie voor wanneer grote hoeveelheden persoonsgegevens worden verwerkt. Bijvoorbeeld een bedrijf maakt profiling van persoonlijke aspecten van haar klanten. Voor personeelsgegevens is dit niet van toepassing. Wel als indien in publiek toegankelijk gebied cameraregistratie uitgevoerd wordt en systematisch mensen gevolgd.
5. Privacy by design en privacy by default: van begin af aan hoort bij iedere beleidsontwikkeling privacy-aspecten meegewogen te worden vanuit een basis dat er niet meer persoonsgegevens worden verzamelt dan strikt noodzakelijk voor het product en/of doel van de verzameling. Dit geldt al bij het uitgeven van digitale nieuwsbrieven.
6. Aanstellen functionaris gegevensverwerking: deze zal voor de textielverzorging niet nodig zijn.
7. Meldplicht datalekken: deze blijft van kracht zoals nu reeds onder de huidige wetgeving. De regels zijn wel strenger. Zo moet ieder lek gedocumenteerd worden. Draag hierbij zorg dat werknemers die toegang hebben tot persoonsgegevens alert zijn en verplicht worden om ieder lek te melden.
8. Bewerkersovereenkomst: bij uitbesteden van verwerking van persoonsgegevens (zoals bijvoorbeeld salarissen), moet er een bewerkersovereenkomst gesloten worden. De reeds bestaande moeten voldoen aan de nieuwe eisen. Organisaties die gegevens verwerken zullen de komende periode hier aandacht voor vragen. Let op: een bedrijf dat uitbesteed blijft zelf verantwoordelijk dat die ook op orde is.
9. Leidend toezichthouder: deze is alleen van toepassing voor organisaties die internationaal werkzaam zijn.
10. Toestemming gegevensverwerking: er moet kunnen aangetoond worden dat betrokkenen toestemming hebben gegeven voor het verwerken van gegevens. Uit de verantwoording moet blijken dat de toestemming specifiek is verleend voor het gevraagde doel en ook op basis van welke informatie de toestemming is verleend.

Op www.autoriteitpersoonsgegevens.nl is toegankelijke informatie te vinden. De onderdelen 1, 2, 3, 5, 7, 8 en 10 zijn belangrijk om nadere kennis over op te doen, waarbij 3, 7 en 8 essentieel zijn. Op basis van WOR 27 heeft de Ondernemingsraad instemmingsrecht bij regelingen voor het verwerken van persoonsgegevens van werknemers. Zie ook infographic.

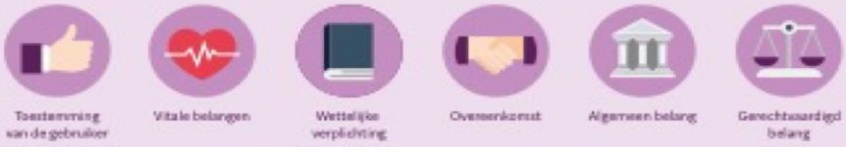
NETEX
NEDERLANDSE VERENIGING VAN TEXTIELREINIGERS

1021804036

AUTORITEIT PERSOONSGEGEVENS

Nieuwe privacywetgeving vanaf 25 mei 2018
De AVG in een notendop

Op basis hiervan mag je persoonsgegevens verzamelen
De grondslag



Het begint aan de tekentafel
Zorgvuldigheid

Technische en organisatorische maatregelen
Verplichtingen

Mensen moeten controle kunnen uitoefenen
Rechten van de betrokkenen

De AVG geldt vanaf 25 mei 2018

Gegevens zijn beschermd!

U heeft een goed privacyverhaal

Aan de slag met het AVG-stappenplan!
Bereid je nu voor op de AVG

Naar het stappenplan →

Bijlage 2 AVG: voorbeeld/format privacy-statement

De in dit voorbeeld/format opgenomen informatie is bedoeld als indicatie voor gegevens en onderwerpen die van belang kunnen zijn voor een privacy-statement. Uiteraard is de feitelijke inhoud afhankelijk van de analyse die u voor uw bedrijf heeft gemaakt volgens het stappenplan.

Privacy-statement

<BEDRIJFSNAAM> , gevestigd aan <ADRES/WOONPLAATS>, is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacyverklaring.

Contactgegevens:
<WEBSITE>
<TELEFOONNUMMER>
<EMAILADRES>

<NAAM> is de Functionaris Gegevensbescherming van <BEDRIJFSNAAM>.Hij/zij is te bereiken via <EMAILADRES>.

Persoonsgegevens die wij verwerken
<BEDRIJFSNAAM> verwerkt uw persoonsgegevens doordat u gebruik maakt van onze diensten en/of omdat u deze zelf aan ons verstrekt. Hieronder vindt u een overzicht van de persoonsgegevens die wij verwerken:

- Voor- en achternaam
- Geslacht
- Geboortedatum
- Geboorteplaats
- Adresgegevens
- Telefoonnummer
- E-mailadres
- IP-adres
- Overige persoonsgegevens die u actief verstrekt bijvoorbeeld door een profiel op deze website aan te maken, in correspondentie en telefonisch
- Locatiegegevens
- Gegevens over uw activiteiten op onze website
- Gegevens over uw surfgedrag over verschillende websites heen (bijvoorbeeld omdat dit bedrijf onderdeel is van een advertentienetwerk)
- Lijst met contactgegevens van de klant via een app
- Internetbrowser en apparaat type

- Bankrekeningnummer

Bijzondere en/of gevoelige persoonsgegevens die wij verwerken
<BEDRIJFSNAAM> verwerkt de volgende bijzondere en/of gevoelige persoonsgegevens van u:

- Lidmaatschap vakbond
- Strafrechtelijk verleden
- Kredietwaardigheidscheck
  Bij <BEDRIJFSNAAM> is het mogelijk om achteraf te betalen voor de producten die u koopt. Om dit mogelijk te maken en u en onszelf te beschermen tegen misbruik, laten we uw kredietwaardigheid toetsen. Dit doen wij door de noodzakelijke persoonsgegevens (waaronder uw adresgegevens) te verstrekken aan een kredietwaardigheidsbeoordelaar [naam & eventueel adresgegevens beoordelaar], die deze gegevens alleen voor dit doel mag gebruiken.
- Gegevens van personen jonger dan 16 jaar Onze website en/of dienst heeft niet de intentie gegevens te verzamelen over websitebezoekers die jonger zijn dan 16 jaar. Tenzij ze toestemming hebben van ouders of voogd. We kunnen echter niet controleren of een bezoeker ouder dan 16 is. Wij raden ouders dan ook aan betrokken te zijn bij de online activiteiten van hun kinderen, om zo te voorkomen dat er gegevens over kinderen verzameld worden zonder ouderlijke toestemming. Als u er van overtuigd bent dat wij zonder die toestemming persoonlijke gegevens hebben verzameld over een minderjarige, neem dan contact met ons op via EMAILADRES>, dan verwijderen wij deze informatie.
- Burgerservicenummer (BSN)

Met welk doel en op basis van welke grondslag wij persoonsgegevens verwerken
<BEDRIJFSNAAM> verwerkt uw persoonsgegevens voor de volgende doelen:

- Het afhandelen van uw betaling
- Verzenden van onze nieuwsbrief en/of reclamefolder
- U te kunnen bellen of e-mailen indien dit nodig is om onze dienstverlening uit te kunnen voeren
- U te informeren over wijzigingen van onze diensten en producten
- U de mogelijkheid te bieden een account aan te maken
- Om goederen en diensten bij u af te leveren
- <BEDRIJFSNAAM> analyseert uw gedrag op de website om daarmee de website te verbeteren en het aanbod van producten en diensten af te stemmen op uw voorkeuren.
- <BEDRIJFSNAAM> volgt uw surfgedrag over verschillende websites waarmee wij onze producten en diensten afstemmen op uw behoefte.

- <BEDRIJFSNAAM> verwerkt ook persoonsgegevens als wij hier wettelijk toe verplicht zijn, zoals gegevens die wij nodig hebben voor onze belastingaangifte.

Geautomatiseerde besluitvorming
<BEDRIJFSNAAM> neemt [wel / niet] op basis van geautomatiseerde verwerkingen besluiten over zaken die (aanzienlijke) gevolgen kunnen hebben voor personen. Het gaat hier om

- Besluiten die worden genomen door computerprogramma's of -systemen, zonder dat daar een mens (bijvoorbeeld een medewerker van <BEDRIJFSNAAM>) tussen zit.
- <BEDRIJFSNAAM> gebruikt de volgende computerprogramma's of -systemen: [aanvullen met naam van het systeem, waarom het gebruikt wordt, onderliggende logica, belang en verwachte gevolgen voor betrokkene]

Hoe lang we persoonsgegevens bewaren
<BEDRIJFSNAAM> bewaart uw persoonsgegevens niet langer dan strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld. Wij hanteren de volgende bewaartermijnen voor de volgende (categorieën) van persoonsgegevens:
(Categorie) persoonsgegevens > Bewaartermijn > Reden
Personalia > Bewaartermijn > Reden
Adres > Bewaartermijn > Reden
Enzovoort > Bewaartermijn > Reden

Delen van persoonsgegevens met derden
<BEDRIJFSNAAM> deelt uw persoonsgegevens met verschillende derden als dit noodzakelijk is voor het uitvoeren van de overeenkomst en om te voldoen aan een eventuele wettelijke verplichting. Met bedrijven die u gegevens verwerken in onze opdracht, sluiten wij een bewerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. <BEDRIJFSNAAM> blijft verantwoordelijk voor deze verwerkingen. Daarnaast verstrekt <BEDRIJFSNAAM> uw persoonsgegevens aan andere derden. Dit doen wij alleen met uw nadrukkelijke toestemming. [voeg hier een tabel toe met: de categorie waar derde toe behoort, naam en jurisdictie, doel en welke gegevens.]

Cookies, of vergelijkbare technieken, die wij gebruiken
<BEDRIJFSNAAM> gebruikt alleen technische en functionele cookies. En analytische cookies die geen inbreuk maken op uw privacy. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan deze website wordt opgeslagen op uw computer, tablet of smartphone. De cookies die wij gebruiken zijn noodzakelijk voor de technische werking van de website en uw gebruiksgemak. Ze zorgen ervoor dat de website naar behoren werkt en onthouden bijvoorbeeld uw voorkeursinstellingen. Ook kunnen wij hiermee onze website optimaliseren. U kunt zich afmelden voor cookies door uw internetbrowser zo in te stellen dat deze geen cookies meer opslaat. Daarnaast kunt u ook alle informatie die eerder is opgeslagen via de instellingen van uw browser verwijderen.

Gegevens inzien, aanpassen of verwijderen
U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door <BEDRIJFSNAAM> en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u beschikken in een computerbestand naar u of een ander, door u genoemde organisatie, te sturen. U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar <EMAILADRES>.

Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie uw pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van uw privacy. We reageren zo snel mogelijk, maar binnen vier weken, op uw verzoek.

<BEDRIJFSNAAM> wil u er tevens op wijzen dat u de mogelijkheid heeft om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. Dat kan via de volgende link: https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons

Hoe wij persoonsgegevens beveiligen
<BEDRIJFSNAAM> neemt de bescherming van uw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op met onze klantenservice of via <EMAILADRES>

.

Bijlage 3 AVG voorbeeld/format verwerkersovereenkomst

De in dit voorbeeld/format opgenomen informatie is bedoeld als indicatie voor gegevens en onderwerpen die van belang kunnen zijn voor een privacy-statement. Uiteraard is de feitelijke inhoud afhankelijk van de analyse die u voor uw bedrijf heeft gemaakt volgens het stappenplan.

Contractspartijen:

1. Verantwoordelijke te weten _____, statutair gevestigd te_____, vertegenwoordigd door _____

   hierna te noemen: “Partij A”,

   en

2. Verwerker te weten _____, statutair gevestigd te _____, vertegenwoordigd door _____

   hierna te noemen: “Partij B”,

   gezamenlijk aan te duiden als: “Partijen”;

Overwegende dat:
Partijen hebben op _____ _____ een Overeenkomst met betrekking tot _____ gesloten. Ter uitvoering van onze Overeenkomst worden Persoonsgegevens verwerkt.

Partij A hecht grote waarde aan het beschermen van deze Persoonsgegevens, daarom is Partij A verantwoordelijk voor de gegevens die Partij B gaat verwerken en leggen Partijen in deze Verwerkersovereenkomst en de daarbij behorende bijlagen:

1. Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen
2. Overzicht met beveiligingsmaatregelen
3. Proces rondom het melden van Datalekken en de te verstrekken informatie

vast wat Jij wel en niet mag doen met de Persoonsgegevens.

1. **Definities:**

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de

fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

1.2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

1.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen ("**Verantwoordelijke**");

1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt ("**Bewerker**");

1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegeven betrekking hebben;

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen ("**Bewerkersovereenkomst**");

1.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit

1.8 Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens ("**Datalek**");

1.9 Gegevensbeschermingseffectbeoordeling: het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens.

1.10 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens

2. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.

2.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.

2.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.

2.4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor jou, zoals het melden van Datalekken, waarbij de Persoonsgegevens van mij betrokken zijn, en de plicht tot geheimhouding blijven voortduren

3. **Verwerken Persoonsgegevens**

3.1 Partij B zal alleen Persoonsgegevens verwerken in mijn opdracht en hebt geen zeggenschap over de Persoonsgegevens. Partij B volgt mijn instructies hierover op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Partij A aan Partij B daar van te voren toestemming of opdracht voor geeft.

3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Partij B precies zal verwerken en voor welke verwerkingsdoeleinden.

3.3 Partij B houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

3.4 Partij B mag zonder voorafgaande schriftelijke toestemming van Partij A geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

3.5 Wanneer Partij B met toestemming van Partij A andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.

3.6 Wanneer Partij A een verzoek krijgt van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werkt Partij B daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

3.7 Wanneer Partij A aan Partij B verzoekt om Partij A informatie te geven, dan zal Partij B de informatie verstrekken die Partij A nodig heeft voor het uitvoeren van een Gegevensbeschermingseffectbeoordeling. Partij A heeft dit nodig om in te kunnen schatten wat het risico van de Verwerking is die Partij B namens Partij B uitvoert.

4. **Beveiligen van Persoonsgegevens**

4.1 Partij B zorgt ervoor dat Partij B de Persoonsgegevens voldoende beveiligt. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Partij B passende technische en organisatorische maatregelen.

4.2 Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover neemt Partij B op in Bijlage 2.

4.3 Ter controle zal Partij B aan Partij A ieder jaar een rapportage sturen waarin de genomen beveiligingsmaatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor zal Partij B aan Partij A geen kosten in rekening brengen.

4.4 Partij A mag een inspectie of audit in de organisatie van Partij B laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zal Partij B medewerking verlenen,

waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

4.5 De kosten voor de uitvoering van deze audit zullen voor rekening van Partij B komen wanneer blijkt dat Partij B zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.

4.6 De controle op de algehele verwerking van Persoonsgegevens door Partij B kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. Partij B zal hierbij aan Partij A een rapport verstrekken waarin Partij B aantoont dat wordt voldaan aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Partij B.

4.7 Wanneer een van ons vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van degene die de kosten maakt.

5. **Exporteren Persoonsgegevens**

5.1 Partij B mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van Partij A.

6. **Geheimhouding**

6.1 Partij B zal de aan haar verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.

6.2 Jij zult ervoor zorgen dat ook jouw personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

7. **Datalekken**

7.1 In geval van een ontdekking van een mogelijk Datalek Partij B Partij A hierover informeren binnen 24 uur via _____ en Partij A de informatie verstrekken die is aangegeven in Bijlage 3, zodat Partij A indien nodig een melding bij de Toezichthouder kan doen**.**

7.2 Na de melding van een Datalek aan Partij A, zal Partij B Partij A op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die Partij B getroffen heeft om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

7.3 Het is niet toegestaan dat Partij B een melding van een Datalek doet aan de Toezichthouder en ook mag Partij B de Betrokkenen niet informeren over het Datalek. Dit is de verantwoordelijkheid van Partij A.

7.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

8. **Aansprakelijkheid**

8.1 Als Partij B haar verplichtingen uit deze Verwerkersovereenkomst niet nakomt, stelt Partij A Partij B daarvoor aansprakelijk.

8.2 Partij B is aansprakelijk voor alle schade geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door werkzaamheden van Partij B.

8.3 Indien Partij B de verplichtingen in deze Verwerkersovereenkomst overtreedt, is Partij B aan Partij A een direct opeisbare boete verschuldigd van _____ voor iedere overtreding en _____ voor iedere dag dat Partij B de overtreding begaat. Daarnaast behoudt Partij A het recht om schadevergoeding te vorderen.

8.4 Partij A is aansprakelijk voor de aan Partij A opgelegde bestuurlijke boete door de Toezichthouder als de geleden schade het gevolg is van onrechtmatig of nalatig handelen door Partij B.

8.5 Partij A is niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar Partij B de samenwerking mee is aangegaan of waarvan Partij B Persoonsgegevens verwerkt, als dit het gevolg is van onrechtmatig of nalatig handelen door Partij B.

9.Teruggave Persoonsgegevens en bewaartermijn

9.1 Na het beëindigen van deze Verwerkersovereenkomst geeft Partij Bde Persoonsgegevens terug. Eventuele achter gebleven Persoonsgegevens zal Partij B op een zorgvuldige en veilige manier vernietigen.

9.2 De Persoonsgegevens die Partij B verwerkt volgens deze Verwerkersovereenkomst zal Partij B vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Partij A. Een wettelijke bewaartermijn is er bijvoorbeeld wanneer Partij B de Persoonsgegevens moet bewaren om belastingtechnische redenen.

9.3 Partij B zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan Partij A verklaren dat Partij B de Persoonsgegevens niet langer heeft.

10.Slotbepalingen

10.1 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

10.2 Op deze Verwerkersovereenkomst en jouw werkzaamheden is het Nederlandse recht van toepassing.

10.3 Over eventuele geschillen tussen ons bepaald de rechter in de rechtbank binnen het gebied waar Partij A bedrijf gevestigd is.

Verantwoordelijke:

Ondertekend voor en namens:

_____

Naam: _____

Functie: _____

Datum en plaats:

_____

Handtekening:

_____

Bewerker:

Ondertekend voor en namens:

_____

Naam: _____

Functie: _____

Datum en plaats:

_____

Handtekening:

_____

Bijlage 1: Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Verwerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de persoonsgegevens worden verwerkt.

Beschrijving verwerkingsactiviteiten door Verwerker:

Verwerkingsdoelen:

Verwerkingsverantwoordelijke:

Verwerker:

Sub verwerkers:

Verwerkte Persoonsgegevens:

Locatie verwerkingen:

Bewaartermijn:

Bijlage 2: Overzicht met beveiligingsmaatregelen

Hier moet een overzicht van de beveiligingsnormen opgenomen worden die de Verwerkingsverantwoordelijke aan de Verwerker opgelegt. Om vast te stellen wat passende beveiligingsmaatregelen zijn moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- Het soort persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. *Gaat het bijvoorbeeld om een naam of een emailadres, wat minder gevoelige persoonsgegevens zijn, of gaat het om het verwerken van een BSN.*
- De hoeveelheid betrokkenen van wie gegevens worden verwerkt. *Hoe meer betrokkenen er zijn hoe meer eisen erworden gesteld aan de beveiliging van de gegevens.*
- Het doel waarvoor gegevens worden verwerkt.
- De duur en de wijze waarop gegevens bewaard moeten worden.

Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.

Technische beveiligingsmaatregelen

- ☐ Up to date virusscan
- ☐ Beveiligde USB-sticks
- ☐ Accurate beveilliging medewerkerstelefoon

- ☐ Bitlocker toegangsmechanisme
- ☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)
- ☐ Versleutelde email
- ☐ Geen onbeveiligde externe harde schijven
- ☐ Geen onbeveiligde back ups maken
- ☐ Geen documenten op privé laptop op slaan

Organisatorische beveiligingsmaatregelen

- ☐ Clean desk policy
- ☐ Laptop niet onbemand achterlaten
- ☐ Laptop nooit achterlaten in de auto
- ☐ Privacy-screens medewerkers
- ☐ Oude documenten op juiste manier vernietigen
- ☐ Zorgvuldig gebruik van USB-sticks

Bijlage 3: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met logingegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?

Als op basis van bovenstaande niet zeker is of er sprake is van een beveiligingsincident, zijn in ieder geval de volgende vragen een hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits-)fraude mee kan worden gepleegd, zoals een Burgerservicenummer.
- Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de

_____

Waar het beveiligingsincident te melden?

Als een beveiligingsincident is ontdekt, neem direct contact op met:

Naam: _____

Telefoon: _____

Email: _____

Geef in de e-mail beantwoording op de onderstaande vragen:

Partij A willen graag dat Partij B de onderstaande vragen beantwoord. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De _____ kan helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. **Geef een samenvatting van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd?**

   Vermeld hier ook de naam van het betrokken systeem.

2. **Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident?**

   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto enieder ander tot een persoon te herleiden gegeven.

3. **Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?**

   Geef a.u.b. een minimum en maximum aantal personen.

4. **Omschrijving groep personen om wiens gegevens het gaat.**

   Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandachtverdienen gegevens van een kwetsbare groepen personen, zoals kinderen.

5. **Zijn de contactgegevens van de betrokken personen bekend?**

   Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?

6. **Wat is de oorzaak (root cause) van het beveiligingsincident?**

   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?

7. **Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?**

   Geef dit a.u.b. zo specifiek mogelijk aan.