

BELEID ALGEMENE VERORDENING GEGEVENSBESCHERMING 2023 – 2026



Bouwbedrijf Verkerk





Vestigingsplaats:	Adres: Tielsestraat 54 4021 HD Maurik NL
	Telefoon: 0344 700242
	E-mail: info@bouwbedrijfverkerk.nl
	Website: www.bouwbedrijfverkerk.nl
Vastgesteld door	Safety Analyse
Datum inventarisatie	11-4-2023
Uitgevoerd door	Safety Analyse
	Telefoon 085 0700895 / 0591 555985
	Website: www.safetyanalyse.nl
	E-Mail info@safetyanalyse.nl
Auteur	Safety Analyse
Versie	V 1.0,
Status	Definitief

©Safety Analyse. Niets uit dit bestek/drukwerk mag worden veeelvoudigd en/of openbaar gemaakt d.m.v. drukwerk fotokopie, microfilm op welke andere wijze ook, zonder voorafgaande schriftelijk toestemming van Safety Analyse, noch mag het zonder dergelijke toestemming worden gebruikt voor enig ander werk dan waarvoor het is vervaardigd.



INHOUD

INLEIDING	5
Privacy-beleid organisatie	5
Privacy-missie organisatie	6
Juridisch kader	6
Informatiebeveiligingsbeleid	6
Reikwijdte	6
Definities	7
ORGANISATIE	9
De wettelijke verantwoordelijkheden	9
Organisatorische inbedding	9
Naleving, sturing en monitoring	10
UITGANGSPUNTEN ZORGVULDIGE GEGEVENSVERWERKING	12
Rechtmatigheid, behoorlijkheid, transparantie	12
Grondslag en doelbinding	12
Toestemming	13
Minimale gegevensverwerking en opslagbeperking	13
Juistheid	13
Integriteit en vertrouwelijkheid	13
PLICHTEN VAN DE ORGANISATIE	14
Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)	14
Register van verwerkingen (Artikel 30, AVG)	14
Delen met derden	14
Gegevens beschermingseffect beoordeling (Artikel 35, AVG)	15
Dataclassificatie	15
Logging van gegevensgebruik	16
Bewaren en vernietigen van gegevens	16
Datalekken (Artikel 33,34, AVG)	16
Bewust omgaan met persoonsgegevens	16
Intranet	17
RECHTEN VAN DE BETROKENEN	18
Recht op informatie over verzameling persoonsgegevens	18



Recht op inzage in eigen persoonsgegevens	18
Recht op rectificatie van persoonsgegevens	18
Recht op gegevenswissing/vergetelheid	19
Recht op beperking van verwerking van eigen persoonsgegevens.....	19
Recht op dataportabiliteit.....	19
Recht van bezwaar	19
Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming	19
Indienen van verzoek	20
Vaststellen identiteit.....	20
Besluit.....	20
DATALEKKEN	21
Wat is een datalek.....	21
Melden van een datalek binnen de ambtelijke organisatie	21
Melden aan Autoriteit Persoonsgegevens.....	21
Melden aan de getroffen personen	22
Gevolgen van niet melden	23
Wanneer hoeft een datalek niet gemeld te worden	23
Bewaren van informatie over datalek	24
Afspraken met verwerkers.....	24
BIJLAGES.....	25
Privacyverklaring	25



INLEIDING

Privacy is volop in ontwikkeling. Daarnaast wordt de bescherming van persoonlijke gegevens steeds complexer. Zwakke beveiliging en/of niet adequate verwerking van persoonsgegevens kan leiden tot onacceptabele situaties, waarbij bijvoorbeeld iemands identiteit wordt 'gestolen' en misbruikt.

Maar niet alleen op nationaal niveau heeft privacy een grote toevlucht genomen, ook op Europees niveau. Met de komst van de Algemene Verordening (AVG) wordt het verwerken van persoonsgegevens in de hele Europese Unie op eenduidige manier geregeld. Per 25 mei 2018 moeten alle organisaties die betrokken zijn bij het verwerken van persoonsgegevens aan de AVG voldoen. Het doel van deze Europese verordening is harmonisatie van de regels rond de bescherming van persoonsgegevens en de bevordering van vrij verkeer van gegevens binnen de EU. De rechten van burgers op het gebied van privacy worden versterkt door bijvoorbeeld het vastleggen van het recht om 'vergeten te worden' en het recht van burgers om van de overheid of een bedrijf hun persoonsgegevens in een standaardformaat te krijgen (data portabiliteit).

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de privacywetgeving en streeft voortdurend naar een behoorlijke en zorgvuldige verwerking van persoonsgegevens. Vanaf 25 mei 2018 heeft de Autoriteit Persoonsgegevens meer en zwaardere bevoegdheden gekregen om te handhaven tegen overtredingen van de AVG. De boetes kunnen zelfs oplopen tot €20.000.000, -.

Privacy-beleid organisatie

Binnen de organisatie wordt veel gewerkt met persoonsgegevens van medewerkers en (keten)partners. De organisatie hecht veel waarde aan dat de verwerkingen van persoonsgegevens zorgvuldig, rechtmatig en veilig gebeurt. Bescherming van persoonsgegevens is een grondrecht. Het verwerken van gegevens gebeurt op een faire, veilige en betrouwbare manier. Een zorgvuldige omgang met gegevens van personen vormt een essentiële bouwsteen voor het vertrouwen in de organisatie.

In deze tijd gaat ook organisatie mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De organisatie is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

De organisatie geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de organisatie. Dit privacy beleid is in lijn met het algemene beleid van de relevante lokale, regionale, nationale en Europese wet- en regelgeving. Bij dit beleid gaat het niet alleen om naleving van de wet, maar het leidt ook tot efficiënter werken, omdat het deel uitmaakt van het kwaliteitsbeleid. Met dit beleid zorgen wij voor een goed gedocumenteerd stelsel van interne afspraken waarmee we persoonlijke belangen kunnen waarborgen. In dit beleid staan kaders beschreven voor het verwerken van privacygevoelige informatie oftewel persoonsgegevens, de bescherming van deze gegevens en omgang met deze gegevens. Ook bepaalt het de richting voor het nader vast te stellen procesbeschrijvingen.



Processen worden uitgevoerd door mensen. Daarom streeft de organisatie naar een actief beleid dat vooral gericht is op bewustwording, een open en kritische cultuur en kennisoverdracht.

In gevallen waarin dit beleid niet voorziet, beslist de directie.

Privacy-missie organisatie

Op basis van het privacy-beleid zoals hiervoor beschreven heeft de organisatie de volgende privacy missie geformuleerd:

Klanten en medewerkers van de organisatie kunnen erop rekenen dat bij onze organisatie de verwerking en bescherming van persoonsgegevens een hoge prioriteit heeft. De organisatie verwerkt en bewaart persoonsgegevens ten behoeve van de dienstverlening.

Visie op gegevensbescherming De verwerking van persoonsgegevens is inherent aan de taakuitoefening. Onze dienstverlening is heel divers. Het is dan ook onontkoombaar dat daarbij informatie over personen wordt verwerkt. Voor een goede en zorgvuldige dienstverlening moeten wij de gegevens van klanten en medewerkers verwerken en soms met andere instanties delen. Informatieverwerking gaat gepaard met de verantwoordelijkheid om effectieve privacybescherming te bieden. Het uitgangspunt hierbij is, dat wij respect hebben voor de persoonlijke levenssfeer van onze klanten en medewerkers. Daarbij houdt de organisatie zich aan de wettelijke regels op het gebied van de verwerking van de persoonsgegevens.

Juridisch kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkenen voorop. Er moet voorkomen worden dat er onnodige of te vergaande inbreuk wordt gemaakt op de rechten en vrijheden van betrokkenen. De Algemene Verordening Gegevensbescherming, aangevuld met uitvoeringswet en aanpassingswet AVG die een nadere invulling geven van de bepalingen uit de AVG, biedt hiervoor het wettelijk kader.

Informatiebeveiligingsbeleid

Het beschermen van persoonsgegevens kan niet geborgd worden zonder adequate informatiebeveiliging. Het beleid en uitvoering op het gebied van informatiebeveiliging wordt beschreven in het Informatiebeveiligingsplan van de organisatie.

Reikwijdte

Het privacy-beleid is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens binnen onze administratieve en bestuurlijke organisatie, waarop de wet van toepassing is en waarvoor het management verantwoordelijk is. Daarnaast is het van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. De kaders die in dit beleid staan beschreven gelden voor iedereen (zowel intern als externe verwerkers) die gegevens verwerken. Daarnaast is het beleid van toepassing op alle taken en processen waar de organisatie verantwoordelijk voor is. Overigens geldt het privacy-beleid niet alleen voor de organisatie, maar ook voor alle personen van wie de organisatie gegevens beschikt.



Het privacy-beleid is niet van toepassing op de gegevensverwerking die onder één van de aangewezen, uitgezonderde, verwerkingen van persoonsgegevens uit artikel 2 AVG vallen:

- In het kader van activiteiten die buiten de werkingssfeer van het Unirecht vallen;
- Door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;
- Door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;
- Door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Definities

Alvorens inhoudelijk op het beleid in te gaan is het van belang om enkele belangrijke definities uit de AVG te noemen.

Betrokkene:

De natuurlijke persoon op wie de persoonsgegevens betrekking hebben, van wie persoonsgegevens worden verwerkt.

Verwerker:

De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

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 aan de hand van indicatoren zoals naam, adres, geboortedatum. Naast deze gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals gezondheid, etnische achtergrond, politieke voorkeuren.

Gegevens beschermingseffect beoordeling:

Met een gegevens beschermingseffect beoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment (PIA).

Verwerkingsverantwoordelijke:

Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking:

Een verwerking is alles wat je met een persoonsgegeven doet, zoals: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen raadplegen, gebruiken, verstrekken aan een ander, en vernietigen.



Proces

Privacy-borging is een continu proces. Daarnaast is de regelgeving op het gebied van gegevensverwerking en de technologische ontwikkelingen voortdurend in beweging. Voor dit beleid betekent het dan ook dat:

- Het privacy-beleid minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, wordt geëvalueerd (door een onafhankelijke deskundige), beoordeeld en zo nodig bijgesteld en vastgesteld.
- Eén keer per jaar worden opzet, bestaande werking van de maatregelen voor de bescherming van persoonsgegevens besproken in het managementteam van de organisatie en hiervan wordt een verslag opgemaakt.
- Op basis van het beleid en de beleidsevaluaties worden middelen beschikbaar gesteld om geconstateerde tekortkomingen weg te nemen.

Ingangsdatum

Nadat de directie het privacy-beleid heeft vastgesteld treedt het in werking. Met inwerkingtreding van het privacy-beleid wordt Beleid gegevensverwerking en meldplicht datalekken ingetrokken.



ORGANISATIE.

De wettelijke verantwoordelijkheden

De manier waarop wij dit beleid binnen de organisatie verankeren, vormt het fundament van de privacy borging.

Directie

De directie is verantwoordelijk voor de juiste naleving van de AVG en het beleid op het gebied van de gegevensverwerking. Echter deze verantwoordelijkheid beperkt zich niet tot het management. Zorgvuldige gegevensverwerking geldt voor iedereen die binnen de organisatie werkzaam is. Het niet in acht nemen van privacy-gedragsregels of ernstige schending daarvan kan leiden tot het nemen van sancties.

Management

Ook het management geeft privacy een hoge prioriteit. Het management informeert daarom binnen de jaarlijkse planning en control cyclus over de risico's en over de getroffen privacy-beheersmaatregelen binnen de processen waar de organisatie voor verantwoordelijk is.

Naast het jaarlijkse verantwoorden, hebben zowel het management als de directie afzonderlijk de algemene informatieplicht om organisatie te informeren over bijzonderheden (incidenten) ten aanzien van gegevensverwerking.

Organisatorische inbedding

Juist omdat privacy voor een belangrijk deel mensenwerk is, moet op alle niveaus binnen de organisatie ruime aandacht zijn voor het cyclisch denken. Door privacy vast op de diverse agenda's te plaatsen, ontstaat een continu proces van veranderen en verbeteren. Door vanuit verschillende niveaus en rollen binnen de organisatie naar de kwaliteit van de uitvoering van privacy te kijken, ontstaat een evenwichtig systeem van checks-and-balances. Hieronder beschrijven we de belangrijkste elementen van deze borging.

Vaststellen beleid

De directie stelt het beleid op het gebied van gegevensverwerking vast en draagt zorg dat deze regelmatig wordt geëvalueerd en zo nodig aangepast.

Uitvoering van beleid

Het management wijst uit haar midden een portefeuillehouder privacy aan. Die is verantwoordelijk voor de uitvoering van het beleid en voor de controle op de naleving van afspraken. De portefeuillehouder privacy ziet toe op de ontwikkeling en uitvoering van themagericht privacy beleid (themabeleid). Deze kan ondersteuning van 'experts' op het gebied van gegevensverwerking en informatiebeveiliging krijgen.

Management

Het borgen van privacy en het compliant zijn is directe verantwoordelijkheid van de directie. De managers zijn verantwoordelijk voor de borging van de uitgangspunten van dit beleid binnen hun proces.



Functionaris gegevensbescherming (FG)

Het management heeft een FG aangesteld, voorkomende uit de verplichting uit de AVG (Art. 37). De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De FG informeert, adviseert, houdt toezicht en treedt op als contactpersoon van de Autoriteit Persoonsgegevens (AP).

CISO/informatiemanager

Het borgen van de privacy is onlosmakelijk verbonden met informatiebeveiliging. De CISO (Chief Information Security Officer) is een belangrijke speler als het gaat om de beveiliging van informatie. Hij/zij is verantwoordelijk voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid binnen de organisatie.

Privacy-team

Om de processen te ondersteunen zullen interne 'vak-experts' ingezet worden op het gebied van gegevensverwerking en informatiebeveiliging. Deze experts werken nauw met elkaar en de informatiemanager samen.

Naleving, sturing en monitoring

Met een reeks maatregelen willen wij waarborgen dat wij continu werken aan het optimaliseren en borgen van de kwaliteit van de werkprocessen waarbij privacy een rol speelt. Elke manager is verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar proces plaatsvindt. Het is daarom ook hun verantwoordelijkheid om te monitoren of persoonsgegevens zorgvuldig verwerkt worden, en dit zo nodig bij te sturen.

Ook wordt van iedereen die voor de organisatie werkzaam is (zowel intern als extern) verwacht dat zij de privacywetten en dit beleid naleven. Dit is in het belang van de organisatie zelf én van degenen wiens gegevens verwerkt worden. Gebeurt dat toch niet, dan kan dat consequenties hebben.

Werkinstructies, procedures, protocollen

Dit beleid beschrijft in hoofdlijnen de wettelijke kaders. Om dit beleid in praktijk goed te kunnen uitvoeren dienen per proces werkinstructies en procesbeschrijvingen te komen, hoe binnen bepaald proces de privacy wordt geborgd.

Werkoverleggen

Managers en medewerkers maken privacy tot een vast onderdeel van hun werkoverleg. Zo nodig schuiven de 'experts' op het gebied van gegevensverwerking en informatiebeveiliging bij de overleggen aan. Hiermee werken wij actief aan een open cultuur, aan het optimaliseren van kennis en een transparante procesuitvoering. Bevindingen of vragen kan iedereen voorleggen aan de functionaris gegevensbescherming en CISO.

Toezicht

Voor onafhankelijk toezicht op de uitvoering van het privacy beleid wijst het management een functionaris voor de gegevensbescherming aan conform artikel 37-39 van de AVG. De FG toetst of de aanwezigheid en werking van het beleid afdoende is ingericht. De FG heeft vrij toegang tot systemen



en processen van de organisatie. De FG rapporteert rechtstreeks aan de directie en management. De FG is onafhankelijk en staat niet in hiërarchische relatie tot enige leidinggevende.

Plan en control proces

Privacy vormt een aparte paragraaf binnen het plan en control proces. Jaarlijks legt het management verantwoording af aan de directie over de risico's en beheersmaatregelen met betrekking tot dit beleid. Daarnaast wordt de privacy een vaste paragraaf binnen alle (deel)plannen van de organisatie. Hierdoor ontstaat ruimte voor beleidsmatige verbeteringen.



UITGANGSPUNTEN ZORGVULDIGE GEGEVENSVERWERKING

Omgaan met persoonsgegevens

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Dit betekent dat persoonsgegevens alleen worden verwerkt voor het uitvoeren van bepaalde wettelijke taken en vastgestelde regelingen. Dit ter uitvoering van voorgeschreven doelbinding en proportionaliteit. Dit houdt in dat persoonsgegevens alleen voor specifieke, uitdrukkelijke en legitieme doeleinden mogen worden verzameld en dat er niet meer persoonsgegevens worden verwerkt dan voor dat doel noodzakelijk is. Daarbij wordt tenminste rekening gehouden met de verwantschap van doelen, de aard van de gegevens, de gevolgen van de verdere verwerking voor de betrokkene, de wijze waarop de gegevens zijn verkregen en de gestelde waarborgen ter bescherming van de persoonlijke levenssfeer.

De AVG somt in de artikelen 5 de volgende beginselen inzake de verwerking van persoonsgegevens:

- Rechtmatigheid, behoorlijkheid, transparantie ;
- Grondslag en doelbinding;
- Minimale gegevensverwerking;
- Juistheid;
- Opslagbeperking;
- Integriteit en vertrouwelijkheid.

Rechtmatigheid, behoorlijkheid, transparantie

Op het moment dat persoonsgegevens verwerkt worden, is bekend ter uitvoering van welke taak c.q. op basis van welke wet dat gebeurt en welke specifieke eisen deze taak c.q. wet aan de gegevensverwerking stelt.

Hoe gevoeliger de persoonsgegevens zijn die verwerkt worden, des te zwaarder zijn de technische én organisatorische maatregelen ter bescherming daarvan. Een privacy impactanalyse helpt bij de concretisering van de risico's die aan de verwerking verbonden zijn en de maatregelen die ter compensatie of opheffing hiervan genomen moeten worden.

De betrokkene wordt op het moment van dan wel zo spoedig mogelijk na een eerste verwerking hiervan op de hoogte gesteld, tenzij een wettelijke uitzonderingsgrond deze verplichting (tijdelijk)buiten werking stelt. Waar nodig stelt een proces ten behoeve hiervan een specifiek privacyverklaring op. In ieder geval is ieder proces in het bezit van een generiek privacyverklaring (bijlage privacyverklaring). Deze privacyverklaring wordt opgesteld in voor betrokkenen begrijpelijke taal, bevat informatie over de verwerking en wijst betrokkene op zijn rechten.

Grondslag en doelbinding

Persoonsgegevens worden alleen verwerkt als er voor deze verwerking een doel en een grondslagaanwezig is. Het verwerkingsdoel wordt per proces bepaald.

De grondslagen van een verwerking van persoonsgegevens staan limitatief opgesomd in artikel 6 AVG:

- Noodzakelijk ter uitvoering van een overeenkomst waarbij de betrokkene partij is;



- Noodzakelijk om als verwerkingsverantwoordelijke te voldoen aan een wettelijke verplichting;
- Noodzakelijk om de vitale belangen van een persoon te beschermen;
- Noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag;
- Toestemming van betrokkene.

Toestemming

Toestemming wordt alleen als grondslag gebruikt als er geen andere grondslag aanwezig is. Daarnaast moet toestemming door een betrokkene vrij, specifiek, geïnformeerd en ondubbelzinnig gegeven worden. Informatie aan betrokkene ten behoeve van het geven van toestemming wordt niet alleen verstrekt over de verwerking waarvoor de toestemming gevraagd wordt, maar ook over de dan reeds voorzienbare verdere verwerkingen. Een omgekeerde toestemming/stilzwijgende toestemming (met andere woorden; als wij niets van u horen gaan wij er vanuit dat u toestemming voor geeft) is niet mogelijk.

In het sociaal domein vindt de verwerking van persoonsgegevens in eerste instantie plaats om te voldoen aan een wettelijke verplichting of ter vervulling van een taak van algemeen belang. Bij verwerking van persoonsgegevens binnen één domein, zullen deze twee grondslagen vaak voldoende zijn. Domein overstijgende gegevensverwerking (tijdens en n.a.v. keukentafelgesprekken) of verwerking van persoonsgegevens in het kader van vroeg signalering is vrijwel niet geregeld in de domeinwetten. Gegevensverwerking is in die gevallen dan alleen mogelijk als kan worden aangetoond dat een vrije toestemming hiervoor gegeven is; dus een toestemming die niet geregeerd wordt door de afhankelijkheidsrelatie waarin de betrokkene zich t.o.v. de organisatie bevindt.

Minimale gegevensverwerking en opslagbeperking

Er wordt niet meer, maar ook niet minder persoonsgegevens verwerkt dan noodzakelijk is in het kader van het doel waarvoor ze verwerkt worden.

Wanneer de persoonsgegevens niet langer nodig zijn voor het doel waarvoor ze verwerkt werden, worden ze vernietigd, geanonimiseerd, gepseudonimiseerd of gearchiveerd bij DIV, afhankelijk van de vraag:

- Of ze helemaal niet meer nodig zijn;
- Alleen nog in niet (direct) tot de persoon te herleiden gegevens nodig zijn;
- De Archiefwet op deze gegevens van toepassing is.

Juistheid

Persoonsgegevens die worden gebruikt ter uitvoering van een overheidstaak zijn juist en actueel. Bij twijfel over de juistheid of actualiteit van (persoons)gegevens wordt navraag gedaan bij de betrokkene, een ketenpartner of wordt een basisregistratie geraadpleegd.

Integriteit en vertrouwelijkheid

Wij gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij treft het management passende technische en



organisatorische maatregelen ter bescherming, bevordering van de juistheid en volledigheid van de persoonsgegevens en ter voorkoming van inbreuk, verlies en onrechtmatige verwerking van de persoonsgegevens, zorgt de organisatie voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid. De organisatorische beveiliging van persoonsgegevens is een taak van de processen zelf.

PLICHTEN VAN DE ORGANISATIE

Om AVG-compliant te zijn er aantal verplichtingen uit de AVG waaraan dient te worden voldaan.

Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)

Het management heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, en optreden als contactpersoon. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de processen overneemt. De processen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de organisatie richtlijnen op het gebied van privacy. De FG rapport jaarlijks aan het management over de stand van zaken, de risico's en nieuwe ontwikkelingen op het gebied van gegevensverwerking. Tussentijds heeft de FG per kwartaal een over met de portefeuillehouder over tussentijdse constatering, datalekken en voortgang van de implementatie. Ernstige datalekken en datalekken die gemeld worden bij Autoriteit Persoonsgegevens worden direct aan de portefeuillehouder gemeld.

Register van verwerkingen (Artikel 30, AVG)

Het management heeft een register van verwerkingen waarvan de organisatie de verwerkingsverantwoordelijke is. Het register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van de soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

Delen met derden

Bij veel processen worden gegevens verwerkt door derden. Het uitbesteden van werkzaamheden aan derden brengt risico's met zich mee op het gebied van gegevensverwerking en informatiebeveiliging. Het management blijft verantwoordelijk voor de verwerking van de gegevens. Zij moeten er daarom op toezien dat gegevens juist verwerkt en beveiligd worden.



Met het oog op de omgang met privacy door alle partijen waar de organisatie mee samenwerkt en waarbij persoonsgegevens worden verwerkt, worden verwerkersovereenkomsten en convenanten/protocollen afgesloten. Hiervoor hebben wij een standaard verwerkingsovereenkomst opgesteld. De procesmanager die een uitbesteding, samenwerking of uitwisseling aangaat, ziet toe op de totstandkoming van deze afspraken. De FG wordt bij de totstandkoming betrokken en ziet toe op de naleving ervan.

Daarnaast is in de inkoopvoorwaarden een en ander geregeld. Inkoopvoorwaarden zijn standaard van toepassing bij de uitbesteding.

Een samenwerking met externen wordt verder alleen aangegaan als deze afdoende garanties bieden m.b.t. het toepassen van passend technische en organisatorische maatregelen. Verwerkers worden in ieder geval geacht deze garanties te bieden als zij op het moment van afsluiten van de overeenkomst gecertificeerd zijn.

Met ketenpartners worden veelvuldig persoonsgegevens uitgewisseld. Afspraken omtrent deze uitwisseling kunnen worden vormgegeven in een privacy-convenant. In ieder geval bij de uitwisseling van gevoelige persoonsgegevens wordt met de ketenpartners overlegd of zij bereid zijn afspraken hierover te maken en deze vast te leggen in een privacy-convenant.

Gegevens beschermingseffect beoordeling (Artikel 35, AVG)

Met een gegevens beschermingseffect beoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.

Deze worden uitgevoerd wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

De volgende indicatoren worden daarbij als toetsingskader gehanteerd:

- Een nieuwe of veranderde organisatorische taak;
- Aanleg van een groot databestand;
- Verwerking van bijzondere persoonsgegevens;
- Aanschaf van een nieuw informatiesysteem;
- Systematische gegevensuitwisseling met een derde.

Dataclassificatie

De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen, is niet voor elk proces en informatiesysteem hetzelfde. Daarom is het nodig dat alle processen en informatiesystemen die gegevens verwerken een dataclassificatie ontvangen. Dataclassificatie heeft als doel om de continuïteit, integriteit en vertrouwelijkheid van het proces en het informatiesysteem te benoemen. Dit maakt inzichtelijk welke maatregelen genomen moeten worden om de gegevens die verwerkt worden te beschermen.



Logging van gegevensgebruik

Elk geautomatiseerd systeem dat persoonsgegevens verwerkt, moet logging bijhouden van de verwerkingen. In deze logging staat minimaal vermeld welke gebruiker, op welke moment, welke gegevens heeft verwerkt. Logging houdt in:

- Chronologische registratie van gegevens over van belang zijnde gebeurtenissen, die zich gedurende een periode in een verwerking voordoen;
- Het vastleggen in een log, bijvoorbeeld een systeem log of een security log, van feitelijk uitgevoerde bewerkingen en/of pogingen daartoe.

Bewaren en vernietigen van gegevens

Het bewaren van persoonsgegevens is nodig om de organisatorische taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. De AVG schrijft echter voor dat gegevens niet langer bewaard mogen worden dan het doel waar ze voor nodig zijn. Dit doel wordt beschreven in de wet, daarom lopen de bewaartermijnen van persoonsgegevens uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kan het management een besluit over de bewaartermijn nemen. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten.

Voor vernietiging van gegevens is altijd een getekend proces verbaal van vernietiging van de archivaris vereist. Bij het overbrengen van te bewaren gegevens naar de archiefbewaarplaats is het mogelijk om privacygevoelige gegevens van openbaarheid uit te zonderen voor een periode van maximaal 75 jaar.

Datalekken (Artikel 33,34, AVG)

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt het management dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de organisatie dit aan de betrokkenen in eenvoudige en duidelijke taal. In protocol melden datalekken wordt uitgebreid de procedure beschreven.

Bewust omgaan met persoonsgegevens

De organisatie streeft naar een cultuur waarbij iedereen elkaar in alle openheid aanspreekt op het eigen gedrag rondom privacy en daarmee van elkaar leert. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden om een optimaal privacy-beleid te realiseren. Het management en alle binnen de organisatie werkzame personen behandelen alle informatie over individuele personen, die hij/zij ten behoeve van de uitvoering van met opdrachtgevers gesloten overeenkomsten verkrijgt, vertrouwelijk en draagt er zorg voor dat deze informatie niet aan derden beschikbaar komt. Iedereen moet zich bij de uitoefening van zijn/haar taken voortdurend bewust zijn van het belang van het waarborgen van de rechten van alle betrokkenen. Zij moeten persoonsgegevens op een zorgvuldige manier verwerken, zoals omschreven in dit beleid.



Intranet

Mijn informatiebeveiliging wordt relevante informatie gezet betreffende de privacy, zoals nieuwsberichten, standaarden, protocollen, beleid.

Om bewustwording te realiseren is kennisoverdracht nodig. De informatiemanager/CISO zorgt ervoor dat informatie over gegevensbescherming en informatiebeveiliging herhaaldelijk onder de aandacht wordt gebracht binnen de organisatie.



RECHTEN VAN DE BETROKENEN

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- Recht op informatie;
- Inzagerecht;
- Correctierecht;
- Recht om vergeten te worden;
- Recht op bezwaar;
- Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming.

Recht op informatie over verzameling persoonsgegevens

Betrokkenen hebben het recht te weten dat er over hen binnen de organisatie persoonsgegevens verwerkt worden. Betrokkenen van iedere nieuwe verwerking persoonlijk in kennis stellen, vergt een onevenredige inspanning van de medewerkers en maakt het er voor betrokkenen ook niet duidelijker op. Daarom wordt het register van verwerkingsactiviteiten op de organisatie website geplaatst en komen per domein/team privacy-verklaringen beschikbaar voor betrokkenen. In deze verklaringen staat specifieke c.q. aanvullende informatie over gegevensverwerkingen, die niet in het register is opgenomen.

Recht op inzage in eigen persoonsgegevens

Iedere betrokkene heeft het recht om op te vragen welke persoonsgegevens van hem of haar voor welke doeleinden verwerkt worden. Dit wordt het inzagerecht genoemd.

Het inzagerecht is niet van toepassing op interne notities die de persoonlijke gedachten van medewerkers bevatten en uitsluitend bedoeld zijn voor intern overleg en beraad.

Het kan voorkomen dat persoonsgegevens van meerdere personen in één dossier of document staan; bijvoorbeeld een plan van aanpak. Er moet dan rekening gehouden worden met de privacy bij het beschikbaar stellen van de gegevens. Dit wil zeggen dat de informatie over partners en kinderen ouder dan 16 jaar niet zonder toestemming van die personen verstrekt mag worden.

Een verzoek om inzage in gegevens die bij een specifiek proces aanwezig zijn, wordt door dat proces afgehandeld. Een algemeen inzageverzoek in de trant van: "ik wil inzage in alle gegevens die door de organisatie over mij verzameld zijn", wordt gecoördineerd door de FG.

Recht op rectificatie van persoonsgegevens

Daarnaast heeft de betrokkene ook het recht om deze gegevens te laten verbeteren, aan te vullen, als deze feitelijk onjuist, onvolledig of niet ter zake zijn. Een verzoek om rectificatie is meestal een gevolg van het besluit tot inzage in eigen persoonsgegevens.

Indien de gegevens ook daadwerkelijk onjuist zijn, worden ze binnen vier weken gerectificeerd door het proces dat de persoonsgegevens verwerkt. Zo spoedig mogelijk daarna worden alle ontvangers van de – voorheen onjuiste – persoonsgegevens op de hoogte gesteld van de rectificatie. Hiervan kan slechts worden afgezien als dit écht niet mogelijk is.



Recht op gegevenswissing/vergetelheid

Verwerkingsverantwoordelijken hebben de plicht persoonsgegevens te vernietigen, niet langer tot de persoon herleidbaar te maken of te archiveren als ze niet langer het doel dienen waarvoor ze werden verwerkt. Het verzoek om persoonsgegevens te wissen is het spiegelbeeld van deze plicht. Op het recht wordt naar verwachting vooral een beroep gedaan als verwerking van de gegevens plaatsvond met toestemming van betrokkene en betrokkene deze toestemming intrekt. Net als van een rectificatie, worden eerdere ontvangers van een gegevenswissing – zo mogelijk – op de hoogte gesteld.

Recht op beperking van verwerking van eigen persoonsgegevens

Tijdens de behandeling van een verzoek om rectificatie of bezwaar, kan een betrokkene vragen zijn persoonsgegevens tijdelijk niet te verwerken. Aan dit verzoek wordt gehoor gegeven, bijvoorbeeld door de persoonsgegevens van betrokkene tijdelijk in een afgezonderd deel van het systeem/het bestand te zetten. In het systeem/bestand wordt vervolgens aangetekend dat de gegevens van betrokkene beperkt verwerkt mogen worden. De beperking wordt opgeheven zodra de reden voor het opleggen daarvan vervalst; bijvoorbeeld omdat een besluit op het verzoek om rectificatie is genomen.

Recht op dataportabiliteit

De persoonsgegevens die een betrokkene aan een verwerkingsverantwoordelijke heeft verstrekt én die geautomatiseerd worden verwerkt op grond van toestemming van betrokkene of ter uitvoering van een overeenkomst, moeten op zijn verzoek geautomatiseerd aan hem of – als dit technisch mogelijk is – een andere verwerkingsverantwoordelijke worden verstrekt. Het recht op dataportabiliteit geldt niet voor persoonsgegevens die op basis van andere grondslagen worden verwerkt. Omdat veel verwerkingen binnen de organisatie plaatsvinden op basis van een wettelijke verplichting of taak van algemeen belang, heeft dit recht verwerkingen maar een beperkte betekenis. In het register van verwerkingsactiviteiten kan worden nagegaan op basis van welke grondslagen een verwerking plaatsvindt en of een betrokkene dit recht toekomt.

Recht van bezwaar

Een betrokkene kan bezwaar maken tegen het feit dat zijn persoonsgegevens worden verwerkt ter vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag. Hij moet hierbij specifieke omstandigheden aanvoeren, die door de verwerkingsverantwoordelijke moeten worden afgewogen tegen de gerechtvaardigde belangen op voortzetting van de verwerking van de persoonsgegevens van betrokkene.

Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming

De verwerking van persoonsgegevens is mensenwerk. Tenzij een betrokkene hiervoor uitdrukkelijk toestemming geeft of de AVG het expliciet toestaat, mogen persoonsgegevens in het kader van het nemen van een besluit daarom niet door een computer worden verwerkt zonder menselijke tussenkomst. In de organisatie worden geen geautomatiseerde besluiten genomen.



Indienen van verzoek

De betrokkene moeten worden gewezen op hun rechten. Dat gebeurt door middel van privacyverklaring. In het sociaal domein, worden de betrokken tijdens keukentafelgesprek gewezen op hun rechten.

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan alleen schriftelijk ingediend worden. Indiening via elektronische weg, zoals, in ieder geval, maar niet beperkt tot, email, fax, telefoon, is uitgesloten. Het verzoek moet duidelijk weergeven van welk recht er gebruik gemaakt wordt en redenen waarom.

Het is niet toegestaan om gegevens van andere personen in te zien. Eventueel kan een betrokkene iemand anders machtigen om voor hem/haar een verzoek in te dienen. In de machtiging moet specifiek omschrijven worden van welke recht gebruik wordt gemaakt. In geval van een machtiging wordt bij betrokkene geverifieerd of de machtiging daadwerkelijk is afgegeven.

Bij kinderen of in geval van onder curatele stelling, kan alleen de wettelijke vertegenwoordiger een verzoek tot gebruikmaking van toegekend recht doen.

Vaststellen identiteit

Alvorens een verzoek in behandeling kan worden genomen, moet de identiteit van de aanvrager/ster vastgesteld worden. Dit is noodzakelijk om de veiligheid van persoonsgegevens te waarborgen en fraude te voorkomen.

Identiteit wordt in beginsel vastgesteld aan de hand van persoonlijke identificatie, aan de hand van een van de documenten, zoals die staan opgenomen in artikel 1 van de Wet op de identificatieplicht.

Besluit

Op een verzoek moet er binnen vier weken na ontvangst van het verzoek, een besluit over het verzoek genomen worden. Als betrokkene het niet eens is met het besluit staat er daartegen bezwaar open.

Uitgangspunt is dat de behandeling van een verzoek kosteloos is. Echter, wanneer het verzoek buitensporig is of bij herhaling wordt ingediend, kan de organisatie een redelijke vergoeding in rekening brengen of weigeren gevolg te geven aan het ingediende verzoek.



DATALEKKEN

De meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens. In bepaalde gevallen moet ook de betrokkene van wie persoonsgegevens zijn gelekt geïnformeerd worden. Elk concreet datalek moet worden beoordeeld en de verwerkingsverantwoordelijke moet een afweging maken of het onder de wettelijke meldplicht valt. Hieronder worden handvatten gegeven voor de beoordeling van het datalek en de melding daarvan.

Het niet voldoen aan de meldplicht kan leiden tot handhaving door de Autoriteit Persoonsgegevens. Bij een ernstige schending van de meldplicht kan een boete worden opgelegd.

Wat is een datalek

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is. Wij spreken van een datalek als er inbreuk is op de beveiliging van persoonsgegevens (zoals beschreven in artikel 33 van de AVG). Bij een datalek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking- dus aan degene waartegen de beveiligingsmaatregelen bescherming moeten bieden. Er is dus niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Ook verlies van een laptop, of het sturen van een mailing met adressen in het CC-veld in plaats van het BCC-veld geldt al als datalek. En zelfs verlies van gegevens door een brand in het datacentrum (waarbij er geen back-up beschikbaar is), ziet de wet als een datalek.

Melden van een datalek binnen de ambtelijke organisatie

De medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens meldt dit direct aan de FG, CISO en aan zijn procesmanager. De melding verloopt altijd via het meldsysteem. Op deze manier hebben wij een overzicht van alle meldingen en hoe deze worden afgehandeld. De FG beoordeeld samen met de CISO of het betreffende datalek onder de meldingsplicht valt. Zo ja, dan zorgt de FG dat er een melding wordt gedaan bij de Autoriteit Persoonsgegevens.

Melden aan Autoriteit Persoonsgegevens

Het datalek wordt conform artikel 33 van de AVG onverwijld gemeld aan de Autoriteit Persoonsgegevens. De termijn voor het melden van het datalek begint te lopen op het moment dat de verwerkingsverantwoordelijke, of een verwerker, op de hoogte is gesteld van een incident dat mogelijk onder de meldplicht valt. Wat in een concreet geval als 'onverwijld' wordt aangemerkt zal afhangen van de omstandigheden. De melding wordt in ieder geval zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, gedaan, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Indien het incident later dan 72 uur na ontdekking wordt gemeld, wordt er gemotiveerd waarom de melding later is gedaan.

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht. Een lek kan ernstig zijn als



het een grote hoeveelheid data betreft (kwantitatief ernstig), maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig). Een paar voorbeelden uit de tweede categorie zijn:

- Inloggegevens;
- Financiële gegevens;
- Kopieën van identiteitsbewijzen;
- School- of werkprestaties;
- Gegevens die betrekking hebben op levensovertuiging;
- Gegevens die betrekking hebben op gezondheid.

Hierbij is het niet van belang hoe een datalek is ontstaan. Met andere woorden, doet het in deze gevallen er niet toe of het datalek door een fout is ontstaan of het gevolg was van overmacht. Het moet hoe dan ook gemeld worden.

Melden aan de getroffen personen

Indien het datalek waarschijnlijk (een aanzienlijke kans op) ongunstige gevolgen heeft voor het privéleven van de personen van wie de gegevens gelekt zijn, wordt - naast de melding aan de Autoriteit Persoonsgegevens - het lek tevens onverwijld gemeld aan betrokkenen. Ongunstige gevolgen zijn bijvoorbeeld:

- Identiteitsfraude;
- Discriminatie;
- Reputatieschade.

Wanneer kwantitatief ernstige gegevens zijn gelekt, is er altijd sprake van een ongunstig gevolg. Dit wordt dus ook altijd worden gemeld aan de getroffen persoon(en).

In de kennisgeving aan betrokkene(n) wordt, conform artikel 34 lid 2 AVG in ieder geval het volgende vermeld:

- Een omschrijving van de aard van de inbreuk;
- De naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- De waarschijnlijke gevolgen van de inbreuk voor betrokkenen;
- De voorgestelde of genomen maatregelen om de inbreuk aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Op grond van artikel 34 AVG wordt de kennisgeving aan de betrokkene op zo'n manier gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

In de meeste gevallen betreft het een individu. Bij meer omvangrijke incidenten wordt er gekozen voor een combinatie van algemene voorlichting en het op individuele basis informeren van betrokkenen. Het uitgangspunt van de informatie is dat zo veel mogelijk betrokkenen bereikt worden met informatie die hen helpt om de gevolgen van het datalek voor hun persoonlijke levenssfeer zo veel mogelijk te beperken.



In de melding aan de Autoriteit Persoonsgegevens wordt aangegeven of het datalek al aan de betrokkenen is gemeld en, zo niet, wanneer dat wordt gedaan. Mocht deze termijn bij nader inzien niet haalbaar blijken, dan wordt dit aan de Autoriteit Persoonsgegevens doorgegeven middels een aanpassing van de melding.

Gevolgen van niet melden

De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. De ontvangen datalek meldingen stellen de Autoriteit Persoonsgegevens in staat om erop toe te zien dat betrokkenen adequaat worden geïnformeerd over datalekken die hen persoonlijke raken, of waarvan zij last kunnen ondervinden.

Als een datalek waarvoor een meldingsplicht geldt niet is gemeld aan de betrokkene kan de Autoriteit Persoonsgegevens, indien deze van oordeel is dat het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de betrokkene, verlangen om dit alsnog te doen. Dit staat gelijk aan een bindende aanwijzing, en het niet-nakomen van zo'n aanwijzing kan worden bestraft met een bestuurlijke boete.

Ook kan de Autoriteit Persoonsgegevens op basis van de ontvangen datalek meldingen actie ondernemen om de adequate beveiliging van persoonsgegevens meer in de breedte te bevorderen. Als uit de ontvangen datalek meldingen blijkt dat de beveiliging van persoonsgegevens mogelijk niet op orde is, dan kan dat voor de Autoriteit Persoonsgegevens aanleiding vormen voor nader onderzoek naar de naleving van de beveiligingsverplichtingen uit de AVG. Heeft de Autoriteit Persoonsgegevens tijdens het onderzoek overtredingen geconstateerd die voortduren, dan kan deze handhavend optreden (artikel 83 en 84 AVG). Daarbij kan de Autoriteit Persoonsgegevens gebruik maken van informatie uit ontvangen datalek meldingen. Op eventuele publicatie van deze informatie zijn de *Beleidsregels actieve openbaarmaking door de Autoriteit Persoonsgegevens* van toepassing.

Bij overtreding van datgene dat bij of krachtens artikel 34 AVG wordt bepaald, kan de Autoriteit Persoonsgegevens een bestuurlijke boete opleggen. Deze boetes kunnen onder meer opgelegd worden voor:

- Het niet melden van een datalek terwijl dat wel moet;
- Het niet op orde hebben van de beveiliging;
- Het verwerken van persoonsgegevens zonder toestemming;
- Export van persoonsgegevens naar landen buiten Europa zonder dat goed geregeld te hebben.

De boete kan oplopen tot € 20.000.000, -. Vaak zal er eerst een bindende aanwijzing gegeven worden, maar als sprake is van een overtreding van de AVG die opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, kan de toezichthouder direct een administratieve boete opleggen.

Wanneer hoeft een datalek niet gemeld te worden

Een datalek hoeft niet aan de getroffen personen gemeld te worden wanneer de gelekte persoonsgegevens onleesbaar zijn. Hiervan is bijvoorbeeld sprake wanneer de persoonsgegevens versleuteld zijn of wanneer de gegevens op afstand verwijderd kunnen worden van bijvoorbeeld een



gestolen laptop. Er moet dan echter wel zeker zijn dat niemand de gegevens heeft kunnen inzien. De bewijslast hiervoor rust bij de verwerkingsverantwoordelijke. De beoordeling of een datalek gemeld moet worden aan de Autoriteit Persoonsgegevens en/of de getroffen personen, ligt te allen tijde bij de verwerkingsverantwoordelijke.

Bewaren van informatie over datalek

Wanneer een datalek aan de Autoriteit Persoonsgegevens wordt gemeld, wordt er een overzicht hiervan bewaard. Dit overzicht bevat de feiten en gegevens van het lek zoals: de oorzaak van het lek, de soort gegevens die gelekt zijn, het moment dat het lek is ontdekt en op welke wijze het lek gedicht is. Als het datalek ook aan de getroffen personen is gemeld, wordt de communicatie hierover bewaard. De wet schrijft niet voor hoe lang het overzicht moet worden bewaard. In eerste instantie wordt er uitgegaan van een bewaartermijn van minimaal één jaar. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren. Zo moeten de gegevens minimaal drie jaar worden bewaard als er geen melding aan de betrokkene is gedaan omdat er zwaarwegende redenen waren of omdat er voldoende technische beschermingsmaatregelen zijn genomen, waardoor er geen ongunstige gevolgen voor de betrokkene zijn.

Afspraken met verwerkers

In veel gevallen wordt het verwerken van persoonsgegevens uitbesteed aan een derde partij (verwerker). Een verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke, zonder dat hij aan het rechtstreekse gezag van de verantwoordelijke is onderworpen (artikel 4, lid 8, AVG). Data kan bijvoorbeeld toegankelijk zijn voor een clouddienstverlener die updates uitvoert op software, opgeslagen staan bij een hostingprovider, of beschikbaar zijn voor het marketingbedrijf dat e-mails in opdracht van klanten verzendt. Voordat de persoonsgegevens voor de verwerking worden uitbesteed aan een verwerker, dan wordt eerst nagegaan of deze voldoende waarborgen biedt ten aanzien van de naleving van de meldplicht voor datalekken.

In veel gevallen is de verwerker de eerste die kennis krijgt van een opgetreden datalek. Om aan onze eindverantwoordelijkheid te voldoen moet de verwerker ons tijdig en adequaat informeren over de datalekken waarvan hij kennis krijgt. In elke verwerkingsovereenkomst worden daar afspraken over gemaakt.



BIJLAGES

Privacyverklaring



Privacyverklaring

Bouwbedrijf Verkerk gevestigd aan <Bezoekadres>, is verantwoordelijk voor de verwerking van persoonsgegevens zoals weergegeven in deze privacyverklaring.

Algemeen

Contactgegevens:

Bouwbedrijf Verkerk

Tielsestraat 54

4021 HD Maurik

Tel: 0344 700242

E-mail: info@bouwbedrijfverkerk.nl

KvK nummer: -

BTW nummer: -

Persoonsgegevens die wij verwerken:

Bouwbedrijf Verkerk verwerkt uw persoonsgegevens omdat 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
- Financiële gegevens (in de meest ruime zin van het woord)
- Juridische informatie o.m. over de rechtsvorm van uw onderneming
- Bankrekeningnummer
- Burgerlijke staat
- Overige persoonsgegevens die u actief verstrekt
- Burgerservicenummer (BSN)
- Gegevens van minderjarigen voor zover de gezinsleden van de ondernemer minderjarig zijn. Omdat deze gegevens uitsluitend door de ouder/voogd aan Bouwbedrijf Verkerk verstrekt worden, nemen we aan dat de ouder / voogd instemt met deze gegevensverstrekking.

Doel en grondslag verwerking persoonsgegevens

Bouwbedrijf Verkerk verwerkt uw persoonsgegevens met de volgende doelen:

- U te kunnen bellen, mailen en/of schriftelijk te communiceren indien dit nodig is om onze dienstverlening uit te kunnen voeren.



- Om administratieve diensten en aanvullende services zoals fiscale- en juridische adviesdiensten te leveren zoals overeengekomen in de Opdracht. Waar nodig worden voor deze dienstverlening, na overleg en met goedkeuring, derden ingeschakeld.
- Bouwbedrijf Verkerk verwerkt ook persoonsgegevens als wij hier wettelijk toe verplicht zijn, zoals gegevens die wij nodig hebben voor uw belastingaangifte en/of jaarrekening.

Geautomatiseerde gegevensverwerking en besluitvorming

Bouwbedrijf Verkerk neemt geen besluiten over zaken op basis van enkel en alleen geautomatiseerde gegevensverwerking die (aanzienlijke) gevolgen kunnen hebben voor personen. Het gaat hier om besluiten die worden genomen door computerprogramma's en/of systemen, zonder dat daar een persoon (bijvoorbeeld een medewerker van Bouwbedrijf Verkerk) tussen zit.

Bouwbedrijf Verkerk maakt ten behoeve van haar gegevensverwerking (deels) gebruik van cloud georiënteerde verwerkingsprogramma's en/of -systemen. Deze diensten zijn ondergebracht bij professionele in Nederland gevestigde partijen. Informatie betreffende deze partijen kunt u opvragen bij Bouwbedrijf Verkerk.

Hoe lang we persoonsgegevens bewaren

Bouwbedrijf Verkerk bewaart uw persoonsgegevens niet langer dan wettelijk strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld.

Er gelden daarbij nog al wat wettelijke verplichtingen voor uw administratiekantoor.

Om u een beeld te geven hoe lang we uw gegevens bewaren:

Zolang u klant bent bij Bouwbedrijf Verkerk bewaren we uw gegevens, zowel als service naar u, als ook om als opdrachtgever te kunnen voldoen aan onze natuurlijke adviesfunctie en zorgplicht.

Voor de WWFT moet Bouwbedrijf Verkerk zich houden aan de wettelijke bewaartermijn van 5 jaar. De wettelijke bewaartermijn van financiële informatie zoals jaarrekeningen en overige bescheiden, geldt een wettelijke bewaartermijn tot 7 jaar na afloop van het boekjaar; (en voor vastgoed tot 12 jaar).

Gegevens van voormalig klanten worden 1 jaar na afloop van de Opdracht opgeschoond. De gegevens die niet onder de diverse bewaartermijnen vallen worden dan daadwerkelijk verwijderd.

Delen van persoonsgegevens met derden

Bouwbedrijf Verkerk verkoopt uw gegevens niet aan derden.

Uw gegevens worden alleen verstrekt, uitsluitend indien nodig, voor de uitvoering van onze overeenkomst met u, om te voldoen aan een wettelijke verplichting of na overleg met uw goedkeuring. Zo verstrekken wij in uw opdracht gegevens aan de belastingdienst bij het doen van de aangifte, en onder andere aan de Kamer van Koophandel uit hoofde van de wettelijke publicatieplicht.

Verstrekken van gegevens aan overige partijen, bijvoorbeeld uw financier, doen wij alleen op uw verzoek en pas nadat u daarvoor akkoord heeft gegeven.

Met bedrijven die uw gegevens verwerken in onze opdracht, sluiten wij een verwerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens.



Verder wordt, uit hoofde van Audits en kwaliteitstoetsingen, beperkt inzage gegeven aan onze beroepsorganisatie en/of Bureau Financieel Toezicht.

Cookies, of vergelijkbare technieken, die wij gebruiken

Op de website van Bouwbedrijf Verkerk maken wij uitsluitend gebruik van functionele cookies. Cookies zijn kleine tekstbestanden die bij het eerste bezoek aan deze website worden opgeslagen in de browser van uw computer, tablet, of smartphone.

Bouwbedrijf Verkerk gebruikt cookies om te zorgen dat de website goed werkt. Ze zorgen er bijvoorbeeld voor dat de website zich automatisch aanpast aan het scherm van smartphone, tablet of computer.

Gegevens inzien, aanpassen of verwijderen

U heeft het recht uw persoonsgegevens in te zien, te laten corrigeren of te laten 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 Bouwbedrijf Verkerk en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u hebben, naar u of een ander, door u genoemde organisatie, te sturen. U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdracht van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen aan info@bouwbedrijfverkerk.nl.

Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, zullen wij daarna persoonlijk contact met u opnemen ter verificatie van het verzoek.

We reageren zo snel mogelijk, maar uiterlijk binnen vier weken, op uw verzoek. Bouwbedrijf Verkerk 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

Bouwbedrijf Verkerk 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 ons via info@bouwbedrijfverkerk.nl.