Belangenvereniging
intensieve kindzorg
www.bvikz.nl
Info@bvikz.nl

ALGEMENE VERORDENING GEGEVENSBESCHERMING

1. Bewustwording

1.1. Persoonsgegevens:
Bij persoonsgegevens gaat het om alle informatie over een natuurlijke persoon die (indirect) iets over iemand zeggen, zijn persoonsgegevens. Dit betekent dus dat deze informatie:
- ofwel direct over iemand gaat,
- ofwel naar een persoon te herleiden is.

Voorbeelden van persoonsgegevens zijn:
- naam, adres en woonplaats,
- locatiegegevens (zoals GPS),
- IP-adressen
- Familiedossiers
- Alle overige informatie welke te herleiden is naar natuurlijke personen.

Naast de 'gewone' persoonsgegevens bestaan er ook **bijzondere persoonsgegevens**, zoals gegevens over iemands gezondheid, godsdienst of ras. Schending daarvan kan leiden tot grote privacy-inbreuken, met een grotere impact voor de betreffende persoon.

Bijzondere persoonsgegevens volgens AVG:
- Persoonsgegevens waaruit ras of etnische afkomst blijkt;
- Persoonsgegevens waaruit politieke opvattingen blijken;
- Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- Persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt;
- Gegevens over gezondheid;
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon.

Het gebruik van deze gegevens vereist meer aandacht en zorgvuldigheid bij verwerking ervan. In de AVG worden daarom voorwaarden genoemd wanneer je bijzondere persoonsgegevens mag verwerken. Je moet je, bij het gebruiken van deze gegevens, dus extra afvragen of ze nodig zijn voor het uitvoeren van het werk.

Verwerking persoonsgegevens
'Verwerken' is een zeer ruim begrip. Het omvat **alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen**.
Je verwerkt dus bijvoorbeeld persoonsgegevens wanneer je ze:
- Raadpleegt
- Bewaart
- Bijwerkt
- Met elkaar in verband brengt
- Opvraagt
- Opslaat
- Ordent / structureert
- Vastlegt
- Verspreidt
- Ter beschikking stelt of doorstuurt
- Wijzigt

Zelfs het afschermen, uitwissen, combineren en vernietigen van persoonsgegevens wordt aangemerkt als een verwerking. Je spreekt dus al heel snel over het verwerken van persoonsgegevens.

1.2. Welke rol neem je in bij gegevensverwerking?

Dit heeft onder andere te maken met het begrip "**betrokkene**". Kort gezegd komt het neer op het volgende: Je bent zelf betrokkene en je verwerkt gegevens van een betrokkene. We verwerken veel en vaak persoonsgegevens.

Regels AVG voor jou

De AVG wetgeving betekent voor jou dat wanneer je met persoonsgegevens werkt, je dat op een zorgvuldige manier moet doen. Een aantal regels zijn van toepassing bij het verwerken van persoonsgegevens:

- Rechtmatigheid
- Eerlijkheid
- Transparantie
- Doelbinding
- Dataminimalisatie
- Juistheid
- Opslagbeperking
- Integriteit en vertrouwelijkheid

Rechtmatigheid, eerlijkheid en transparantie

Persoonsgegevens moeten allereerst **rechtmatig, eerlijk en transparant worden verwerkt**. Dit betekent dat je alleen maar gegevens mag verwerken **als dit past rechtsgeldig is** en dat jij de **bevoegdheid** hebt gekregen om die taken uit te voeren.

Doelbinding

Doelbinding betekent dat je alleen maar gegevens mag verzamelen *voor **welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen***. Simpel gezegd betekent dit dat voordat je gegevens gaat verwerken (bijvoorbeeld raadplegen of verzamelen), je weet waarvoor je die gegevens nodig hebt: **het doel.** Dit doel moet **formeel zijn vastgelegd in een officieel document**, bijvoorbeeld een opdracht. Je mag dus geen gegevens verzamelen, omdat die in toekomst misschien van pas zullen komen. Daarnaast is het belangrijk dat het **doel** moet zijn vastgelegd, voordat de gegevens worden verwerkt.
Gegevens die je voor een bepaald doel verzameld hebt, mag je niet zomaar voor een ander doel gaan gebruiken. Dit mag alleen als het nieuwe doel past binnen het oorspronkelijke doel. Dit heet: een verenigbaar doel

Dataminimalisatie

Een andere belangrijke regel is *dataminimalisatie*. Dit houdt in dat je alleen die gegevens verwerkt, die strikt noodzakelijk zijn voor het doel waarvoor je die gegevens nodig hebt.

Juistheid en opslagbeperking

Juistheid houdt in dat de persoonsgegevens correct moeten zijn. Dit betekent bijvoorbeeld dat data geactualiseerd is. Daarnaast mogen gegevens niet langer worden bewaard dan noodzakelijk is (*opslagbeperking*).

Integriteit en vertrouwelijkheid

Integriteit en *vertrouwelijkheid* betekenen dat persoonsgegevens moeten worden beschermd, door op een veilige manier met deze gegevens om te gaan. Deze plicht geldt voor elke vrijwilliger van de Bvikz.

1.3. Het verwerkingsregister

De Bvikz heeft een register van de gegevensverwerkingen.[1] Dit register maakt duidelijk waarom we bepaalde persoonsgegevens hebben en wat daarmee gebeurt.
Je doet het goed als je bewust bent van het feit dat je persoonsgegevens verwerkt of gaat verwerken en dat hier risico's aan kunnen kleven. Als je hierover twijfelt, dan roep je de hulp in van een privacy-expert. Binnen de Bvikz wordt die rol vervult door de penningmeester/secretaris. De PIA kan gebruikt worden om de situatie te analyseren. Een PIA is een specialistisch instrument dat vraagt om zowel juridische als proceskennis.

[1] Register van Verwerkingsactiviteiten BVIKZ

1.4 Wat zijn de gevolgen als er iets mis gaat?
Het overtreden van de regels van de AVG kan grote gevolgen hebben. Deze regels zijn hiervoor behandeld. Het schenden van deze regels kan leiden tot bijvoorbeeld problemen voor de betrokkene, negatieve publiciteit en imagoschade. Het kan leiden tot forse boetes voor de Bvikz. Deze boetes worden opgelegd door de Autoriteit Persoonsgegevens (AP). De boete wordt onder andere bepaald op basis van: de ernst van de overtreding, in hoeverre er sprake is van opzet of nalatigheid en welke maatregelen er genomen worden.

2. Dataregister

Met dit *register* brengt de Bvikz zorgvuldig in kaart welke persoonsgegevens zij bijhoudt, waar deze vandaan komen en met wie deze worden gedeeld. De Bvikz adviseert alle vrijwilligers om alle verwerkingen te registreren.

Heeft u bepaald hoe lang u de persoonsgegevens gaat *bewaren* en/of de criteria voor het vaststellen van de bewaartermijn bepaald? de gegevens worden niet langer bewaart dan strikt noodzakelijk en
de toegang tot de gegevens is beperkt tot waarvoor het noodzakelijk is.
Alle digitale bestanden zijn beveiligd met een wachtwoord (code). Indien er bestanden per email (openbare net) zullen de beveiligde bestanden via verzending van een wachtwoord via sms of whatsapp kenbaar worden gemaakt aan de rechtmatige ontvanger van de bestanden.

Heeft u de juiste maatregelen genomen om **persoonsgegevens te beveiligen?**
In de AVG staat dat u persoonsgegevens goed moet beveiligen. Daarom moet u van tevoren goed in kaart brengen wat voor verwerkingen u uitvoert. Vervolgens bepaalt u welke technische en organisatorische maatregelen nodig zijn om ervoor te zorgen dat die verwerkingen goed beveiligd zijn.

3. Communicatie
De AVG vereist dat deze privacyverklaring wordt aangevuld met nieuwe informatietypes. Zo zal je voortaan de wettelijke grondslag voor de gegevensverwerking moeten meedelen, de termijnen gedurende dewelke je de informatie zal bijhouden.

4. Rechten van betrokkene[2]
Onder de AVG krijgen de mensen van wie we persoonsgegevens verwerken meer en verbeterde privacy rechten. Betrokkenen hebben verschillende rechten waarop ze zich kunnen beroepen in het kader van de AVG **De AVG-privacy rechten**
Het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen (NIEUW).
Het recht op vergetelheid. Het recht om 'vergeten' te worden (NIEUW).
Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien.
Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die u verwerkt te wijzigen.
Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.
Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
Het recht om bezwaar te maken tegen de gegevensverwerking.
Ten slotte hebben mensen recht op duidelijke informatie over wat u met hun persoonsgegevens doet. Onder de AVG moet u aan een aantal specifieke eisen voldoen.

5. Verzoek tot toegang
De AVG stelt regels over hoe met verzoeken omgegaan moet worden. De termijn aan het voorzien van een informatieverzoek bedraagt 30 dagen. Verzoeken kunnen per email of schriftelijk worden gedaan.

[2] Zie ook: "Privacy reglement BVIKZ"

6. **Wettelijke grondslag voor het verwerken van persoonsgegevens**
   Noodzakelijk voor de behartiging van de gerechtvaardigde belangen
   U kunt een beroep doen op deze grondslag als u aan drie voorwaarden voldoet:

   Ten eerste moet het gaat om een gerechtvaardigd belang. Dit belang moet rechtmatig zijn, voldoende duidelijk zijn verwoord en het moet om een belang gaan dat ook echt aanwezig is.
   Ten tweede moet de verwerking van de persoonsgegevens noodzakelijk zijn voor de behartiging van het gerechtvaardigde belang. U moet de verwerking daarom toetsen aan de eisen van proportionaliteit en subsidiariteit . Dat betekent dat u moet nagaan of het doel van de verwerking in verhouding staat tot de inbreuk voor de personen van wie u persoonsgegevens verwerkt. Ook moet u nagaan of u het doel niet op een voor de betrokken personen minder nadelige manier kan bereiken.

   Ten derde moet u een afweging maken tussen uw belangen en de belangen van de personen van wie u persoonsgegevens verwerkt. Ook moet u hierbij eventueel maatregelen treffen om ervoor te zorgen dat de rechten en vrijheden van deze personen niet zwaarder wegen dan uw gerechtvaardigd belang.
   Dit betekent onder meer dat u de gegevens niet langer mag bewaren dan nodig is voor het doel van de verwerking. Gaat het bijvoorbeeld om de verwerking van persoonsgegevens van kinderen, dus jonger dan 16 jaar? Dan weegt uw gerechtvaardigd belang minder snel op tegen hun rechten en vrijheden.

7. **Kinderen**
   Start vandaag met de ontwikkeling van systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen. Voor het eerst zal de AVG speciale bescherming bieden aan de persoonsgegevens van kinderen, in het bijzonder in de context van commerciële internetdiensten zoals sociale netwerken. Kortweg, indien jouw bedrijf of organisatie gegevens van kinderen – onder de 16 jaar – verzamelt, zal een ouder of voogd toestemming moeten geven opdat de gegevensverwerking rechtmatig zou zijn.

8. **Datalekken**
   Wat is een datalek?
   Een van de overtredingen binnen de AVG is het datalek*. We spreken van een datalek als onbevoegde personen toegang (kunnen) krijgen tot persoonsgegevens. Dit kan gebeuren door bijvoorbeeld het verlies van dossiers, gegevensdragers of apparaten (zoals USB-sticks, laptops, smartphones en tablets) maar ook door inbraken op het systeem (hacken).
   Als persoonsgegevens en/of klantdata per ongeluk bij de verkeerde persoon of instantie terechtkomen, spreken we ook over een datalek. Daarnaast spreken we ook van een datalek als persoonsgegevens mogelijk in verkeerde handen terecht kunnen komen, omdat ze met e-mail vanuit de Bvikz naar een persoonlijk e-mailadres als Gmail of persoonsgegevens die worden gedeeld via WhatsApp.

   Wat kun je zelf doen?
   Als je een datalek signaleert, dan ben je verplicht hier melding van te maken. Ook als dit buiten kantoortijden is. Je meldt dit als een vermoeden van een datalek bij de **privacy expert**. Indien nodig neemt hij hierna de regie op zich onder andere ten aanzien van het informeren van de betrokkenen en de Autoriteit Persoonsgegevens (AP).

9. **Gegevensbescherming door ontwerp en gegevensbeschermingseffectbeoordeling**
   Privacy by design betekent dat u al bij het ontwerp voorziet in technische en organisatorische maatregelen om de privacyrisico's voor mensen zo klein mogelijk te maken. Bijvoorbeeld door persoonsgegevens te pseudonimiseren en niet meer persoonsgegevens te verwerken dan noodzakelijk voor het doel van uw verwerking (dataminimalisatie).
   Concreet houdt **privacy by default** in dat u maatregelen treft die ervoor zorgen dat u alleen die persoonsgegevens verwerkt die noodzakelijk zijn voor de specifieke doelen waarvoor u de gegevens verkrijgt, de gegevens niet langer bewaart dan strikt noodzakelijk en de toegang tot de gegevens beperkt.

   De WMK-toets
   Bij de beoordeling van nieuwe maar ook bestaande gegevensverwerkingen worden de aspecten Willen, Mogen en Kunnen getoetst (WMK-toets). De WMK-toets bestaat uit een vragenlijst die onder begeleiding van een privacy-expert wordt ingevuld
   De WMK-toets kun je toepassen in de volgende situaties:
   Een bestaande situatie, waarbij al sprake is van gegevensverwerking;
   Een nieuwe situatie, waarbij nog geen gegevensverwerking plaatsvindt en nog niet bekend is wat daar de consequenties van zijn.

De WMK-toets in een bestaande situatie
In de praktijk gebeurt het regelmatig dat gegevens verwerkt worden, waarbij alleen het '**kunnen'** is aangetoond (doordat het al wordt gedaan). Er wordt dan zonder nader onderzoek aangenomen dat het bestuur het willen en het mogen correct heeft afgewogen.

Privacy impact assessment (PIA)
In sommige gevallen moet na een WMK-toets ook een PIA (of GEB, gegevensbeschermingseffectbeoordeling) worden uitgevoerd. Een PIA is een uitgebreidere risicobeoordeling van het aspect 'mogen' van de WMK-toets.
Vanuit de AVG is een PIA verplicht gesteld bij verwerkingen met een hoog privacy-risico. De privacy-expert kan bepalen of je naast de WMK ook een PIA moet uitvoeren.
1. Beoordelen van mensen op basis van persoonskenmerken
2. Geautomatiseerde beslissingen
3. Stelselmatige en grootschalige monitoring
4. Gevoelige gegevens
5. Grootschalige gegevensverwerkingen
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Blokkering van een recht, dienst of contract

Op grond van de regelhulp AVG is de uitkomst bepaald:
U heeft aangegeven dat uw verwerking(en) aan geen of slechts 1 van de criteria voldoet. Dat betekent dat er voor de Bvikz waarschijnlijk geen sprake is van een hoog privacy risico. Als dat inderdaad zo is, dan hoeft u geen DPIA uit te voeren.

10. Functionaris voor gegevensbescherming/privacy expert

Dit is iemand die binnen uw organisatie toezicht houdt op de toepassing en naleving van de AVG. Binnen de Bvikz zijn de taken en verantwoordelijkheden met betrekking tot privacyvraagstukken formeel belegd bij het dagelijks bestuur, bestaande uit de voorzitter en de secretaris/penningmeester. Deze laatste functionaris is aangewezen als privacy expert. Indien er sprake is van een mogelijk incident, dient er bij deze functionaris melding te worden gemaakt.