PRIVACYWETGEVING

VOLDOET UW BEDRIJF AAN DE AVG?

(Algemene Verordening Gegevensbescherming)

INLEIDING

In dit document leggen wij u in hoofdlijnen uit waar u op moet letten om te voldoen aan de belangrijkste wettelijke eisen met betrekking tot de bescherming van persoonsgegevens. Tevens nemen we hyperlinks op naar belangrijke documenten. Veel informatie uit dit document is afkomstig van de Autoriteit Persoonsgegevens zelf.

WAT VERANDERT ER?

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG versterkt de positie van de betrokkenen (onder meer uw klanten en uw werknemers/ZZP'ers). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Bedrijven die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van bedrijven om te kunnen aantonen dat zij zich aan de wet houden. Bestudeer het mooie grafische overzicht "de AVG in een notendop" van de AP. Op internet staan diverse informatieve filmpjes. Voor u hebben wij vier filmpjes geselecteerd. Zeker de moeite waard om hier 'even' een blik op te werpen.

- https://www.youtube.com/watch?v=AaOUlz1nv2E
- https://www.youtube.com/watch?v=kLfSL09wQyE
- https://www.youtube.com/watch?v=afyxuxHK1Xc
- https://www.youtube.com/watch?v=tgK6hKvsqZ8

WAT KAN IK DOEN?

Als bedrijf kunt u nu alvast stappen ondernemen om straks klaar te zijn voor de AVG. Op de eerste plaats door nu alvast het eerder genoemde stappenplan uit te voeren. Creëer ook bewustwording in uw organisatie over de AVG. Zorg ervoor dat de relevante mensen in uw organisatie op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee. Indien u een functionaris gegevensbescherming (hierna FG) aanstelt dan kunt u het stappenplan door uw FG laten uitvoeren. Het hoogste management blijft echter wel eindverantwoordelijk. De FG (of directie bij het ontbreken van de FG) moet het personeel goed instrueren over relevante zaken. Denk hier aan het naleven van de beveiligingsmaatregelen, informeren van relevante afdelingen omtrent de rechten van betrokkenen, het melden van datalekken aan de FG (zodat hij/zij dit kan melden aan de AP) en dergelijke.

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

WIE IS VERANTWOORDELIJK VOOR DE NALEVING VAN DE AVG?

Het hoogste management is eindverantwoordelijk. Overtreedt een organisatie de AVG? De AP kan dan een boete opleggen. Er zijn twee categorieën overtredingen en bijbehorende maximale boetes.

1) Verantwoordelijken (organisaties die persoonsgegevens verwerken) hebben onder de AVG bepaalde verplichtingen, zoals de verantwoordingsplicht. Komt een verantwoordelijke (een van) deze verplichtingen niet na? Dan kan de AP een boete opleggen van maximaal 10 miljoen euro. Of een boete van 2% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.
2) Overtreedt een verantwoordelijke de beginselen of grondslagen van de AVG? Of de privacy rechten van de betrokkenen (de mensen van wie de organisatie gegevens verwerkt)? Dan kan de AP een boete opleggen van maximaal 20 miljoen euro. Of een boete van 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.

PRIVACYWETGEVING VERSUS CYBERSECURITY

Privacywetgeving en cybersecurity zijn onlosmakelijk met elkaar verbonden. Door een goede cybersecurity is de kans immers veel kleiner dat persoonsgegevens "op straat" komen te liggen. We hebben ook een document cybersecurity voor u gemaakt. Deze komt in een later stadium op de website.

DE MELDPLICHT DATALEKKEN

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

Per 1 januari 2016 is de meldplicht datalekken ingevoerd. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Organisaties die een datalek willen melden bij de Autoriteit Persoonsgegevens kunnen dat doen via het meldloket datalekken. Voorbeelden van datalekken zijn: 1 een kwijtgeraakte USB-stick met persoonsgegevens, 2 een gestolen laptop, IPad of telefoon, 3 een inbraak in een databestand door een hacker.

De Autoriteit Persoonsgegevens kan bij overtreding van de meldplicht datalekken hoge boetes opleggen. Op de website van de Autoriteit Persoonsgegevens vindt u uitgebreide informatie, zie Meldplicht datalekken. Zie ook de Beleidsregels-meldplicht-datalekken.

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Onderstaand geven wij u een mogelijk **stappenplan** voor de AVG:

1_____

Check of u een verwerkingsregister moet opstellen. Meer info

2_____

Breng de rechten van klanten in kaart en informeer iedereen. Meer info

3_____

Doe aan compliance management.

Toon aan dat u toestemming van betrokkenen heeft. Meer info

4_____

Maak uw organisatie vertrouwd met privacy by design & privacy by default. Meer info

5_____

Check of u een functionaris voor de gegevensbescherming (FG) aan moet stellen. Meer info

6_____

Check of u een data protection impact assessment (DPIA) moet uitvoeren. Meer info

7_____

Zorg dat u voldoet aan de Meldplicht datalekken. Meer info

8_____

Check of u verwerkersovereenkomsten af moet sluiten. Meer info

9_____

Doe de privacy quick scan van VNONCW.

10_____

Raadpleeg regelmatig de website van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens plaats hier vaak nieuwe informatie en belangrijke uitspraken. Abonneer u ook op de nieuwsbrief van de AP.

11_____

Communiceer in heldere en begrijpelijke communicatie. Meer info

12_____

Lees ook het document Cybersecurity op onze website zodat u ook voldoende ICT beveiligingsmaatregelen in acht neemt.

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 1: Check of u een verwerkingsregister op moet stellen.

In een Excelbestand kunt u eenvoudig een verwerkingsregister opstellen. Ons advies is om dit te doen, ook als het niet verplicht is. U leert hieruit namelijk ook met welke partijen u een verwerkingsovereenkomst moet afsluiten alsmede laat u richting de Autoriteit Persoonsgegevens zien dat u privacybescherming op de agenda heeft staan. Onder de AVG heeft u een documentatieplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.
U kunt het overzicht ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of te verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

De Autoriteit Persoonsgegevens geeft aan:

- **Ben ik verplicht om een register van verwerkingsactiviteiten op te stellen?**

  In de Algemene verordening gegevensbescherming (AVG) staan een aantal verplichte maatregelen genoemd waarmee u aan uw verantwoordingsplicht (accountability) kunt voldoen. Een van die verplichtingen is het 'register van verwerkingsactiviteiten'. Of u zo'n verwerkingsregister moet opstellen, hangt af van de omvang van uw organisatie en het type gegevens dat u verwerkt.

  Organisaties met meer dan 250 medewerkers

  Heeft uw organisatie meer dan 250 medewerkers? Dan bent u verplicht om een verwerkingsregister bij te houden.

  Organisaties met minder dan 250 medewerkers

  Heeft uw organisatie minder dan 250 medewerkers? Dan moet u over een verwerkingsregister beschikken wanneer u persoonsgegevens verwerkt:

  - die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of;
  - waarvan de verwerking niet incidenteel is en/of;
  - die vallen onder de categorie bijzondere persoonsgegevens. Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

  Bent u verplicht om een verwerkingsregister op te stellen? Dan moet u dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt.

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

- **Wat moet een bedrijf in het register van verwerkingsactiviteiten opnemen?**

  De Algemene verordening gegevensbescherming (AVG) schrijft voor welke informatie organisaties minimaal in het register van verwerkingsactiviteiten moeten opnemen. Dit geldt ook voor scholen.

  In het register moet in ieder geval staan:

  - de naam en contactgegevens van:
    - uw organisatie, of de vertegenwoordiger van uw organisatie;
    - eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
    - de Functionaris voor de gegevensbescherming (FG) als u die heeft aangesteld;
    - eventuele andere internationale organisaties waar u persoonsgegevens mee deelt.
  - de doelen waarvoor u de persoonsgegevens verwerkt;
  - een beschrijving van de categorieën van personen van wie u gegevens verwerkt. Denk hierbij onder meer aan ouders, voogden, leerlingen, docenten, begeleiders;
  - een beschrijving van de categorieën van persoonsgegevens. Denk hierbij aan onder meer administratiegegevens van leerlingen, verzuimgegevens, gegevens over vorderingen en resultaten van leerlingen, handelingsplannen;
  - de datum waarop u de gegevens moet wissen als dat bekend is;
  - de categorieën van ontvangers aan wie u persoonsgegevens verstrekt. Denk hierbij onder meer aan externe instanties;
  - deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan moet u dit aangeven in het register;
  - een algemene beschrijving van de technische en organisatorische maatregelen die u heeft genomen om persoonsgegevens die u verwerkt te beveiligen.

  Over het register van verwerkingsactiviteiten

  Organisaties, waaronder ook scholen, kunnen onder de AVG verplicht zijn om een register van verwerkingsactiviteiten op te stellen. In het register staat informatie over de persoonsgegevens die u verwerkt. Als de Autoriteit Persoonsgegevens (AP) daar om vraagt, moet u het register kunnen laten zien. Dit maakt onderdeel uit van de verantwoordingsplicht.

Wij adviseren ook om op te nemen:

- met welk doel u dit doet en de wettelijke grondslag (bijvoorbeeld: soort contract);
- waar deze gegevens vandaan komen (klant zelf, maar het kan ook de werkgever zijn);
- met wie u ze deelt (bijvoorbeeld: administratiekantoor?);
- wie toegang hebben tot deze gegevens (personeel/afdeling/stagiairs/ZZP,); TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 2: Breng de rechten van deelnemers/cursisten in kaart en informeer iedereen

"Wat zijn de rechten van klanten?

Dat zijn er een hele trits, maar om er een paar te noemen:

1. ***Recht op inzage in van diens persoonsgegevens** die door het bedrijf worden verwerkt, waaronder:*
2. ***Recht om o**njuiste/incomplete persoonsgegevens te (laten) corrigeren / aan te vullen.*
3. ***Recht op verwijdering persoonsgegevens uit jouw database***
4. ***Recht op vergetelheid;** klanten/cursisten hebben al het recht om een bedrijf te vragen hun persoonsgegevens te verwijderen. Straks kunnen zij daarnaast eisen dat de organisatie de verwijdering doorgeeft aan alle andere organisaties die deze gegevens van deze organisatie hebben gekregen."*

Verder geeft de AP op de website aan:

Onder de AVG krijgen betrokkenen (onder meer uw cursisten en uw werknemers/ZZP'ers) meer en verbeterde privacy rechten. Zorg er daarom voor dat zij hun privacy rechten goed kunnen uitoefenen. Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen (bijvoorbeeld: een cursist kiest een andere opleider). Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen. Zorg dat uw medewerkers op relevante afdelingen de procedure kennen. TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 3: Toon aan dat u toestemming van betrokkenen heeft

Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven. Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 4: Maak uw organisatie vertrouwd met privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default* en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 5: Check wel/geen functionaris voor de gegevensbescherming

De Autoriteit Persoonsgegevens gaf aan:

"Wel of geen FG aanstellen?

Een FG is verplicht:

1. *voor de overheid en publieke organisaties*
2. *voor organisaties die op grote schaal individuen volgen.*
3. *voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken (denk aan gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden).*

Algemene informatie op de website van de AP.

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Wacht hier niet te lang mee en stel indien van toepassing iemand alvast aan.. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

U moet zelf bepalen of een FG verplicht is. Indien een FG verplicht is dan mag dit ook een externe zijn (bijvoorbeeld uw accountant).

De volgende organisaties zijn in ieder geval verplicht een FG aan te stellen:

Ten eerste zijn overheidsinstanties en publieke organisaties altijd verplicht om een FG aan te stellen, ongeacht het type gegevens dat ze verwerken. Het kan gaan om de rijksoverheid, gemeenten en provincies, maar ook om bijvoorbeeld zorg- en bekostigde onderwijsinstellingen (private zoeken we nog uit).

Ten tweede geldt de verplichting om een FG aan te stellen voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via *wearables*.

Relevant hierbij zijn onder meer het aantal mensen dat een organisatie volgt, de hoeveelheid gegevens die deze organisatie verwerkt en hoe lang de organisatie mensen volgt.

Ten derde zijn organisaties verplicht een FG te benoemen als ze op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. Bijzondere persoonsgegevens zijn

bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

Naast hetgeen hierboven staat, geeft de AP aan:

Als organisatie bent u volgens de AVG onder meer verplicht een FG te benoemen en een data protection impact assessment (DPIA) uit te voeren als u op grote schaal:

- *individuen volgt; of*
- *bijzondere persoonsgegevens van individuen verwerkt.*

Voor beide aspecten geldt dat dit een kernactiviteit van de organisatie moet zijn. In de AVG staat niet precies uitgelegd wat 'grootschalig' inhoudt. Wel zijn er criteria en voorbeelden die u op weg helpen.

Criteria grootschalige gegevensverwerking

Wilt u bepalen of uw organisatie volgens de wet op grote schaal (bijzondere) persoonsgegevens verwerkt? Kijk dan naar deze criteria:

- *het aantal betrokkenen (de mensen van wie u gegevens verwerkt);*
- *de hoeveelheid gegevens die u verwerkt;*
- *de duur van de gegevensverwerking;*
- *de geografische reikwijdte van de verwerking."*

TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 6: Voer een data protection impact assessment (DPIA) uit

Onder de AVG kunt u verplicht zijn een zogeheten Data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen, en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 7: Zorg dat u voldoet aan de Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de gemelde datalekken. TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 8 check of u verwerkersovereenkomsten moet afsluiten

De kans is vrij groot dat u enkele verwerkingsovereenkomsten (opnieuw) moet afsluiten.

De in het verleden afgesloten verwerkingsovereenkomsten moeten worden aangepast aan de AVG. Een goede verwerkingsovereenkomst kunt u hier vinden.

Wanneer een verwerkingsovereenkomst?
Geeft u persoonsgegevens van uw medewerkers/leerlingen/ cursisten aan een verwerker, een externe partij die ten behoeve van u persoonsgegevens van deze medewerkers/leerlingen/cursisten gaat verwerken. Sluit dan een verwerkingsovereenkomst (denk bijvoorbeeld aan: administratiekantoor, cloud leverancier, ICT leverancier, accountant, leasemaatschappij, incassopartij, ZZP'ers met wie u samenwerkt, dochterbedrijf…).

Algemene informatie kunt u ook vinden op

- https://www.ibdgemeenten.nl/wp-content/uploads/2017/03/20170314-factsheet-verwerkersovereenkomsten-v1.00-2.pdf
- http://www.ictvalley.nl/blog/is-uw-bewerkersovereenkomst-toekomstproof

TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)

Stap 11: Communiceer in heldere en begrijpelijke communicatie.

Check onder meer de volgende documenten:

- Uw algemene voorwaarden (indien u eigen algemene voorwaarden heeft)
- Uw privacyverklaring (op de website, in studiegidsen etc.).
- Uw cookieverklaring

TERUG^

Bron: Nederlandse Raad voor Training en Opleiding (NRTO)