Federale Overheidsdienst Binnenlandse Zaken
Algemene Directie Instellingen en bevolking
Rijksregister
Externe Relaties

3153668

Aan de gebruikers van het Rijksregister

Uw contactpersoon
Stefan Van de Venster
Isabel Leliaert

T
02 518 20 74
02 518 21 41

E-mail
Stefan.VandeVenster@rrn.fgov.be
Isabel.Leliaert@rrn.fgov.be

F

Uw kenmerk

Ons kenmerk

Bijlagen

Brussel
7 -08- 2017

Uitvoering van de Verordening (EU) 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (AVG of Algemene Verordening Gegevensbescherming)

Dames,

Heren,

Ik heb herhaaldelijk de aandacht gevestigd op de verplichtingen opgelegd in toepassing van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (die de Richtlijn 95/46 EU omzet). Deze verplichtingen zijn van toepassing op de verantwoordelijken voor de verwerking binnen de overheden en instellingen die wettelijk gemachtigd zijn om toegang te hebben tot het RR, alsook tot de maatregelen met als doel de veiligheid van de gegevens te waarborgen.

Het lijkt mij, met het oog op de volgende inwerkingtreding op 25 mei 2018 van de Europese Verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (AVG), noodzakelijk om de aandacht van de bovenvermelde overheden en instellingen te vestigen op de noodzaak om de maatregel van de door de AVG opgelegde verplichtingen te nemen.[1]

De AVG richt zich op een globale logica van **responsabilisering van alle actoren**. Men stelt een aanzienlijke verlichting van de verplichtingen inzake voorafgaande formaliteiten vast, aangezien het aangiftestelsel (waarvan de bevolkingsregisters evenwel vrijgesteld waren) volledig afgeschaft wordt, om over te gaan tot een systeem voor het "Beheer" van de persoonsgegevens. Men gaat immers van een logica van controle vooraf naar een

[1] De grote principes die reeds vervat zijn in de wet voor de bescherming van de persoonlijke levenssfeer, wijzigen niet, maar de AVG **versterkt de verplichtingen inzake transparantie van de verwerkingen** en **respect voor de rechten van de personen** en versterkt de rol van de controleautoriteit (Commissie voor de bescherming van de persoonlijke levenssfeer) **door haar sanctionerende bevoegdheid aanzienlijk te versterken**. Zo zal zij, naast publieke waarschuwingen, ook zware administratieve geldboetes kunnen uitspreken. Er dient een nieuw principe inzake **gegevensbescherming** te worden geïntegreerd **vanaf het ontwerp** (Privacy by design) van de verwerking en **standaard** (Privacy by default). Zo zal men zo vroeg mogelijk, vanaf de ontwerpfase van het product, de dienst of de verwerking, rekening moeten houden met de standaardinstellingen en de essentiële principes van de gegevensbescherming. Het is in het bijzonder de bedoeling om de impact van de uitgevoerde verwerking op de persoonlijke levenssfeer te minimaliseren, zoals bijvoorbeeld *het zo veel mogelijk beperken van het recht op toegang tot de gegevens en de verrichtingen die uitgevoerd kunnen worden.*

logica van voortdurende responsabilisering van de verantwoordelijken voor de verwerking. Dit betekent dat de **conformiteit met de AVG permanent en dynamisch zal moeten zijn**. Er zullen technische en organisatorische maatregelen genomen en geactualiseerd moeten worden om zich er te allen tijde van te vergewissen en aan te tonen dat er werkelijk een optimaal niveau van bescherming van de behandelde gegevens geboden wordt. Zo zullen de verantwoordelijken voor de verwerking een **register van hun verwerkingsactiviteiten** moeten bijhouden.

De openbare en private instellingen waaraan de gemeenten de volledige of gedeeltelijke uitvoering van hun verwerkingen **uitbesteden** (bv. dienstverleners die gegevens hosten), zullen verplicht moeten deelnemen aan de inregelstelling, door hen te helpen om te voldoen aan hun diverse verplichtingen, op straffe van sancties.

Deze nota heeft niet tot doel om over te gaan tot een volledige analyse van de door de gemeenten of de informaticafirma's te voeren acties om zich in regel te stellen met de AVG. De AVG valt buiten het bevoegdheidsdomein van het departement binnen de gemeenten. U verwerkt immers dagelijks talrijke persoonsgegevens om het administratieve beheer van uw structuur (human resources-bestanden), de beveiliging van uw lokalen (toegangscontrole met badge, camerabewaking) of het beheer van de verschillende overheidsdiensten en activiteiten waarmee u belast bent, te waarborgen: beheer van de bevolkingsregisters, beheer van de burgerlijke stand, kieslijsten, ontwikkeling van telediensten, enz. Het departement moet zich niet mengen in dit beheer. Het lijkt mij evenwel noodzakelijk om onze partners te helpen om zich voor te bereiden en te anticiperen op de veranderingen die gekoppeld zijn aan de inwerkingtreding van de AVG.

Daarom stelt het departement u een methodologie in 5 fases voor om dit te doen:

- Fase 1: De aanwijzing van een piloot: de Data Privacy Officer (DPO)
- Fase 2: De uitwerking van een Register van de verwerkingen (RV)
- Fase 3: De kritische analyse van het RV
- Fase 4: De herevaluatie van de interne processen
- Fase 5: De conformiteitsdocumentatie

De verwezenlijking van de fases 3, 4 en 5 is afhankelijk van de timing die de toekomstige hervorming van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens door de FOD Justitie oplegt, alsook van een daaropvolgende bijwerking van onze eigen reglementeringen: men dient derhalve het nieuwe wettelijke kader inzake bescherming van de persoonsgegevens af te wachten. Het is evenwel noodzakelijk om de inregelstelling nu reeds aan te vatten door de eerste 2 fases op te starten.

Park Atrium
Koloniënstraat 11
1000 BRUSSEL

T 02 518 21 31
F 02 518 26 31

callcenter.rrn@rrn.fgov.be
www.ibz.rrn.fgov.be

I. Fase 1: De aanwijzing van een piloot: de DPO

Vanaf 25 mei 2018 zal de aanwijzing van een functionaris voor gegevensbescherming (*Data Privacy Officer*) verplicht zijn voor de publieke overheden en instellingen, en dus voor de gemeenten[2].

Er wordt gevraagd naar de cumul van de functie van veiligheidsconsulent en de functie van DPO. De CBPL benadrukt in haar **Aanbeveling 04/2017**[3] van 24 mei 2017 dat *men niet mag besluiten dat de vandaag in dienst zijnde veiligheidsconsulent automatisch de functionaris voor gegevensbescherming van morgen wordt. Zoals reeds vermeld, is het voortaan afgemeten aan de functie van functionaris voor gegevensbescherming, zoals beschreven in de AVG, dat dit aspect moet worden onderzocht.*
De AVG stelt dat de functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen, wat méér inhoudt dan enkel het voorzien in een adequate beveiliging en de verplichtingen met betrekking tot de verplichte beveiliging.

De functionaris zal **als voornaamste opdrachten** hebben: :

- *Informeren, opleiden en adviseren* van de verantwoordelijke voor de verwerking, de verwerkers en het personeel;
- *Controleren* van de conformiteit van de verwerkingen met de AVG en andere analoge bepalingen;
- *Het contactpunt* van de controleautoriteit *zijn* wat de vragen in verband met de verwerking van de persoonsgegevens betreft.

In de uitoefening van deze opdrachten, zal de functionaris zich buiten belangenconflicten houden, rechtstreeks verslag uitbrengen aan het hoogste hiërarchische niveau en enige vrijheid genieten in de acties die hij beslist te ondernemen.

Expertise en middelen

Men dient zich ervan te vergewissen dat de DPO over voldoende **expertise en middelen beschikt om zijn rol efficiënt uit te oefenen**. Zo zal de functionaris:

- aangewezen moeten worden op grond van zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming;
- tijdig en op passende wijze betrokken moeten worden bij alle vragen die onder zijn opdrachten vallen;
- de middelen en opleidingen moeten genieten die noodzakelijk zijn om zijn opdrachten tot een goed einde te brengen.

[2] Wat de private instellingen betreft, verwijs ik naar de specifieke bepalingen van de AVG.
[3] https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_04_2017_0.pdf

In deze context, voor de gemeenten die dezelfde bekommernissen hebben, is de aanwijzing van slechts één DPO en een externe DPO niet uitgesloten.

Tot slot kunnen dezelfde gemeenten, zonder de DPO te "delen", op passende wijze samen werken om zich zo goed mogelijk voor te bereiden op de nieuwe door de AVG opgelegde verplichtingen: identificatie van ieders noden, bepaling van een actieplan dat verschillende fases omvat, ontwikkeling van een gezamenlijke tool voor het delen van informatie en kennis, enz.

II. Fase 2: De uitwerking van een Register van de verwerkingen

Het betreft een fundamentele fase: het opmaken van de inventaris van alle bestanden met persoonsgegevens verwerkt binnen uw organisatie.

Er dient in de eerste plaats te worden verwezen naar de **Aanbeveling 06/2017 van 14 juni 2017 van de CBPL**[4] betreffende het Register van de verwerkingsactiviteiten waarvan de rol erin bestaat de gebreken te identificeren, en de te voeren acties te beschrijven om zich in regel te stellen met de huidige en toekomstige verplichtingen ten aanzien van de risico's die uw verwerkingen teweegbrengen voor de rechten en de vrijheden van de betrokken personen. Het register moet welbepaalde informatie bevatten:

1. De lijst opstellen van de verwerkingen per hoofddoel (en niet per gebruikte tool of toepassing) en de soorten verwerkte gegevens;
2. Identificeren van de verwerkers die bij elke verwerking tussenkomen;
3. Bepalen aan wie en naar waar de gegevens worden doorgestuurd;
4. Bepalen waar uw gegevens opgeslagen worden en zorgen voor een back-up;
5. Bepalen hoelang deze gegevens worden bewaard;
6. Inventariseren van de veiligheidsmaatregelen.

Het formaat van dit register is van weinig belang indien alle door de AVG gevraagde informatie erin terug te vinden is. U kunt zich echter inspireren op het volgende nuttige document:

https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten

[4] https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_06_2017_0.pdf

III. Fase 3: Kritische analyse van de verwerkingen

De kritische analyse van het Register van de verwerkingen zal u de mogelijkheid bieden om uw gebreken te identificeren en de te voeren acties te beschrijven om zich in regel te stellen met de huidige en toekomstige verplichtingen ten aanzien van de risico's die uw verwerkingen teweegbrengen voor de rechten en de vrijheden van de betrokken personen. Men dient het volgende te doen:

1. Nakijken dat **enkel de gegevens die strikt noodzakelijk zijn** voor het nastreven van de doelstellingen, worden verzameld en verwerkt.
2. Nakijken van **de juridische basis** waarop de verwerking zich baseert (bijvoorbeeld: toestemming van de betrokkene, gerechtvaardigd belang, overeenkomst, wettelijke verplichting) (art. 6).
3. Aanvullen van de **informatievermeldingen** (art. 12, 13 en 14 van de AVG).
4. Nakijken dat uw **verwerkers** hun nieuwe verplichtingen en hun verantwoordelijkheden kennen dankzij het bestaan van contractuele bepalingen die wijzen op hun verplichtingen inzake veiligheid, vertrouwelijkheid en bescherming van de verwerkte persoonsgegevens.
5. Nakijken dat de uitoefeningsmodaliteiten van de **rechten van de betrokken personen** (toegangsrecht, recht op rechtzetting, recht op de overdraagbaarheid, intrekking van de toestemming, ...) effectief zijn en deze desgevallend aanpassen.
6. Nakijken en aanpassen van de ingevoerde **veiligheidsmaatregelen**.

NB: voor bepaalde risicovolle verwerkingen zal het misschien noodzakelijk zijn om bijzondere maatregelen te nemen, zoals:

- Een Data Protection Impact Assessment (PIA) (gegevensbeschermingseffectbeoordeling),
- Versterkte informatie,
- Het verkrijgen van de toestemming,
- Een voorafgaande machtiging,
- Contractuele bepalingen.

IV. Fase 4: Herevalueren van de interne processen

Er dienen interne procedures tot stand worden gebracht, die de bescherming van de gegevens te allen tijde waarborgen, rekening houdend met alle gebeurtenissen die zich kunnen voordoen tijdens een verwerking (bv. veiligheidslek, beheer van de rechtzettings- of toegangsaanvragen, wijziging van de verzamelde gegevens, wijziging van dienstverlener) **opdat de reflexen inzake bescherming van de persoonsgegevens door iedereen zouden worden verworven, ook in geval van een incident.**

Park Atrium
Koloniënstraat 11
1000 BRUSSEL
T 02 518 21 31
F 02 518 26 31
callcenter.rrn@rrn.fgov.be
www.ibz.rrn.fgov.be

V. Fase 5: Documenteren van de conformiteit

Uw documentatie moet aantonen dat u de door de AVG voorziene verplichtingen naleeft. De in elke fase verwezenlijkte acties en documenten moeten regelmatig **geactualiseerd** worden om een voortdurende gegevensbescherming te waarborgen. Het dossier dat ter beschikking van de Controleautoriteit dient te worden gehouden, moet het volgende bevatten:

- **Het register van de verwerkingen** (voor de verantwoordelijken voor verwerkingen) of categorieën van verwerkingsactiviteiten (voor de verwerkers);
- **De Data Protection Impact Assessments** (PIA) voor de verwerkingen die verhoogde risico's voor de rechten en vrijheden van de personen kunnen teweegbrengen;
- **De begeleiding van de** gegevensoverdrachten buiten de Europese Unie (meer bepaald de standaard contractuele bepalingen, de BCR en certificaten); **De informatievermeldingen**; De modellen van **het verkrijgen van de toestemming van de betrokkenen**; De tot stand gebrachte procedures voor **de uitoefening van de rechten**; **De overeenkomsten met de verwerkers**; De interne procedures **in geval van schendingen van gegevens**.

* * *

* *

De toepassing van de AVG is dus een globaal proces dat het Rijksregister overschrijdt. In dit opzicht kunt u voor bijkomende inlichtingen de site van de Commissie voor de bescherming van de persoonlijke levenssfeer raadplegen (https://www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-0) voor al uw vragen ter zake.

Wij hopen dat deze informatie nuttig zal zijn voor u en dat wij u overtuigd hebben van het belang van de uitvoering van de AVG binnen uw organisaties, die wij u vragen te verwezenlijken met respect voor de rechten en verplichtingen van de verschillende actoren.

Jacques WIRTZ
Directeur-generaal

Park Atrium
Koloniënstraat 11
1000 BRUSSEL

T 02 518 21 31
F 02 518 26 31

callcenter.rrn@rrn.fgov.be
www.ibz.rrn.fgov.be