



Advies van de FG naar aanleiding van het periodiek onderzoek

Derde en vierde periode 2020-V1

P.M.H. Korremans - Functionaris Gegevensbescherming

10-03-2020 / 01-07-2020 / 12-08-2020

Inleiding

In het kader van de Algemene Verordening Gegevensbescherming (AVG) is in de afgelopen twee perioden onderzoek gedaan naar:

- Rechten van betrokkenen (art. 7, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 en 25 AVG)
- Samenwerking met derden (art. 26, 28 en 30 AVG)
- Beveiliging (art. 15, 25, 32, 33 en 34 AVG)
- Verantwoording (art. 6, 7, 12, 13, 14, 24, 30, 32, 33, 35 en 39 AVG).

Via een vooraf opgestelde auditlijsten wordt er inzicht verkregen in hoeverre de organisatie compliant is aan de AVG. De auditlijsten zijn in samenwerking met de VNG en Privacy Information Officer (PIO) tot stand gekomen. De beantwoording van de auditvragen heeft plaatsgevonden door de PIO in samenwerking met de privacycoördinatoren, Security Information Officer (CISO) en de directie.

Hiermee wordt de AVG onderzoekscyclus afgerond en ontstaat er een totaalbeeld van de verplichtingen die de organisaties heeft in het kader van de AVG en in welke fase de organisatie zich bevindt. Op de laatste pagina is een totaaloverzicht grafisch weergegeven.

Rechten van betrokkenen

De organisaties dient betrokkenen zowel actief als passief te informeren over de persoonsgegevens die zij verwerken. Daarnaast stelt de AVG-betrokkenen middels een aantal rechten in staat om controle uit te oefenen over zijn of haar persoonsgegevens.

Betrokkenen worden geïnformeerd over hun rechten

Een van de belangrijkste rechten binnen de AVG zijn die van betrokkenen (burgers). De persoonsgegevens zijn eigendom van de burger en op grond hiervan heeft deze het recht om zijn gegevens te controleren, te corrigeren (indien onjuist), de verwerking te beperken of op te schorten, de persoonsgegevens te verwijderen (voor zover dit kan) en indien noodzakelijk mee te nemen voor verwerking elders (data portabiliteit). Organisaties die persoonsgegevens van betrokkenen verwerken dienen aan te tonen hoe zij deze verwerken, met wie zij deze delen en niet langer te bewaren dan strikt noodzakelijk.

De burgers in Almere maken in beperkte mate gebruik van dit recht maar ook wordt dit recht ten onrechte gebruikt door organisaties die er een verdienmodel van hebben gemaakt!

Om burgers te helpen hun rechten op een juiste wijze uit te oefenen is het van belang een heldere en duidelijke procedure te hebben. Deze staat vermeldt op de gemeentelijke website.



Zijn de processen ingericht op de rechten van betrokkenen

Intern heeft de organisatie een proces ingericht om inzageverzoeken van burgers te behandelen. Via verschillende communicatiekanalen en afdelingen kan een burger een verzoek indienen. ¹¹⁽¹⁾

11(1)

Op verschillende wijze worden persoonsgegevens van burgers verwerkt in de processen en systemen. Op het moment dat verwerkingen plaatsvinden is het van belang dat betrokkenen (burgers) geïnformeerd zijn over het doel, de grondslag waarop deze worden verwerkt en aan wie de gegevens eventueel worden verstrekt. ^{10(2)g, 11(1)}

^{10(2)g, 11(1)}

11(1)

Producten, diensten en systemen zijn privacyvriendelijk ingericht

Het verzamelen van persoonsgegevens voor verwerkingen dienen afgestemd te zijn op het doel en de grondslag van verwerking. In 2018 is dit opgepakt ^{10(2)g, 11(1)}

^{10(2)g, 11(1)}

Eind 2018 is er door de FG een meervoudig advies gegeven aan de ^{10(2)g} over dit onderwerp. Een van de adviezen had betrekking op het onderwerp verzamelen van persoonsgegevens ^{10(2)g}

Een terugkoppeling van de adviezen is nog niet ontvangen.

Wel is er door de afdeling in de tweede helft van 2019 een start gemaakt met het bewust maken van medewerkers t.a.v. het verzamelen, beheren, opslaan en verwijderen van persoonsgegevens. Tevens worden er voorbereidingen getroffen om te komen tot een aanbesteding voor een nieuw softwaresysteem waarin de noodzakelijke eisen t.a.v. de AVG worden meegenomen.

11(1)



Samenwerking met derden

Gemeenten werken op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. In veelvoorkomende gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. Partijen moeten daarom daarover afspraken maken.

Verstreking van informatie aan derde partijen

De gemeente Almere werkt met veel partijen samen waarmee persoonsgegevens worden uitgewisseld. Met ongeveer 45 organisaties worden zorgtaken uitgevoerd waar persoonsgegevens en ook dossiers worden gedeeld. Binnen wijkteams wordt samengewerkt met al deze partijen.

Burgerzaken verstrekt persoonsgegevens aan een groot aantal stichtingen en andere organisaties die deze gegevens gebruiken voor hun dienstverlening of andere doelen.

10(2)g

10(2)g, 11(1)



Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat een verwerkingsverantwoordelijke en een verwerker passende technische en organisatorische maatregelen nemen ter beveiliging van persoonsgegevens. Daarnaast dienen incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld te worden aan de AP en/of de betrokkene(n).

Inbreuken op de privacy

Medewerkers, managers en externe partijen, waarmee wordt samengewerkt en persoonsgegevens mee worden gedeeld of in applicaties wordt opgeslagen, dienen te onderkennen wanneer er een inbreuk of een incident voordoet. Een datalek zit per slot van rekening in een klein hoekje maar kan grote gevolgen hebben voor betrokkenen. Belangrijk is dat iedereen zich bewust is van de verplichting om datalekken te melden. Hiervoor is een protocol beschikbaar waarin duidelijk wordt gemaakt hoe te handelen bij een datalek.

Vast is gesteld dat er een duidelijk beleidsdocument aanwezig is dat voldoet aan de AVG-verplichtingen. Medewerkers en managers zijn in het verleden bij de invoering van de AVG geïnformeerd^{10(2)g}

6.0

^{10(2)g}

Logging van verwerking van gegevens

In het kader van de beveiliging van verwerkingen dient een organisatie maatregelen te nemen waartoe de toegang tot gegevens wordt beperkt tot bepaalde medewerkers (Art. 32 AVG). Hiernaast dient de rechtmatigheid (Art.24 AVG) van verwerkingen binnen geautomatiseerde systemen aangetoond te worden door handelingen van geautoriseerde medewerkers te registreren (tijdstip, handeling, welk bestand). Hierdoor kunnen vragen beantwoord worden wie, welke persoonsgegevens, wanneer en op welke locatie verwerkt heeft.

Er zijn steeds meer situaties waarin het nodig is om loggegevens te kunnen raadplegen. In het kader van de AVG kan de rechtmatigheid worden aangetoond (transparantie) waardoor er verantwoording wordt afgelegd aan betrokkenen en de toezichthouder. Maar ook bij onderzoek naar hacks, een datalek of ongewenste inzage zijn loggegevens relevant.

^{10(2)g, 11(1)}

^{10(2)g}

11(1)



Inrichting van verwerkingen

Verwerkingen dienen zodanig te worden ingericht dat er rekening wordt gehouden met de privacy van betrokkenen (Art.25 lid 1 en 2).

Procesverantwoordelijke dragen er zorg voor dat bij het inrichten van verwerkingen de beginselen vanuit de AVG worden meegenomen. Om dit en de naleving van de AVG aan te kunnen tonen dienen er interne beleidsmaatregelen genomen te worden die ervoor zorgen dat er gegevensbescherming wordt toegepast in conceptfase (privacy by Design) en door standaardinstellingen bij het ontwerp (Privacy by Default).

10(2)g

Bij het verwerken van persoonsgegevens dienen er niet meer gegevens verwerkt worden dat strikt noodzakelijk zijn voor het specifieke doel. Het bovenmatig verzamelen en verwerken (b.v. op meerdere locaties dezelfde persoonsgegevens opslaan) leidt tot doorbreking van doelbinding en ongewenste inbreuken voor betrokkenen. Daarnaast dient de termijn dat de gegevens bewaard en toegankelijk zijn niet langer dan noodzakelijk te zijn. Het beleid t.a.v. het laatste punt kan het beste aansluiten bij de Archiefwet.

11(1)



Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. De organisatie dient aan te kunnen tonen dat de verwerkingen voldoen aan de belangrijkste beginselen van de AVG: rechtmatigheid, behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.

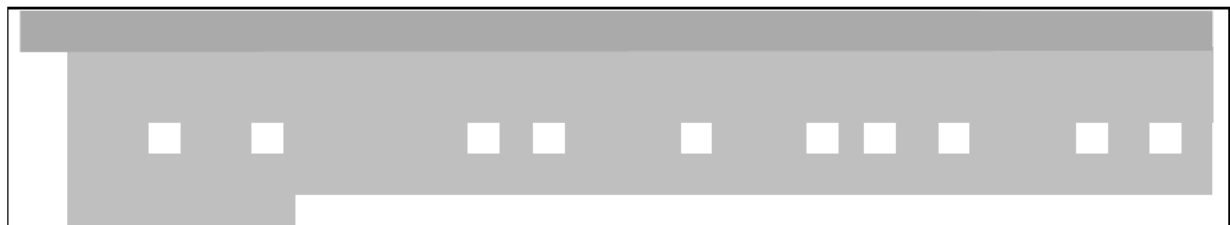
Verwerking van persoonsgegevens op basis van toestemming

Een gemeentelijke organisatie voert over het algemeen taken en wetten uit waarbij het doel en de grondslag voor de verwerking van persoonsgegevens gevonden worden in de diverse wetten. Burgers hoeven daarvoor geen toestemming te geven en kunnen vaak, indien zij dit wel dienen te verstrekken, onvoldoende vrijelijk hun toestemming geven gezien hun afhankelijke positie. De grondslag van toestemming heeft verder als nadeel voor de verwerkingsverantwoordelijke dat betrokkene deze zonder opgave van reden op elk moment kan intrekken.

Indien de organisatie geen andere mogelijkheid heeft dan op basis van deze grondslag persoonsgegevens te verwerken, dan dient zij aan te tonen dat de betrokkene een volwaardige toestemming heeft gegeven en welke informatie is verstrekt. Om dit aan te tonen dient zij b.v. over een register te beschikken waarin wordt bijgehouden wanneer een toestemmingsverklaring is ontvangen en wanneer deze is ingetrokken. Een andere mogelijkheid is om in het proces de toestemmingsverklaring op te nemen, die op elk gewenst moment kan worden verantwoord. Tevens dient het proces zodanig te zijn ingericht dat betrokkene op eenvoudige wijze zijn of haar toestemming kan intrekken en dat de gegevens gelijktijdig worden verwijderd.

De betrokkene dient dan specifiek geïnformeerd te worden waarvoor er toestemming wordt gegeven. Zonder deze specifieke uitleg kan er geen verwerking worden uitgevoerd.

De FG heeft vastgesteld dat er beleid is indien persoonsgegevens worden verwerkt op basis van deze grondslag. Het toepassen van dit beleid dient per verwerkingsproces ingeregeld te zijn zodat kan worden aangetoond dat er vrijelijk toestemming is gegeven door de betrokken burger. ^{10(2)g, 11(1)}





11(1)



