

**Vlaamse Toezichtcommissie voor het
elektronische bestuurlijke
gegevensverkeer**

**Beraadslaging VTC nr. 48/2016 van
7 december 2016**

Betreft: het mededelen van persoonsgegevens van personeelsleden van de Vlaamse Overheid door het Agentschap voor Overheidspersoneel (AgO) aan de Crisiscentrum van de Vlaamse Overheid (CCVO) van het departement Kanselarij en Bestuur (departement KB) in het kader van crisiscommunicatie

I. ELEMENTEN VAN DE AANVRAAG

A. WETTELIJKE, DECRETALE EN REGLEMENTAIRE GRONDSLAGEN

1. De Vlaamse Toezichtcommissie (hierna: "de VTC");
2. Gelet op het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer (hierna: "het e-govdecreet"), inzonderheid de artikelen 8 en 11;
3. Gelet op het besluit van de Vlaamse Regering van 15 mei 2009 betreffende veiligheidsconsulenten;
4. Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna "WVP");
5. Gelet op het Koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna "KB van 13 februari 2001");

B. VERLOOP VAN HET ONDERZOEK

6. Gelet op de aanvraag van AgO enerzijds en het departement KB anderzijds, ontvangen per mail op 1 december 2016;
7. Gelet op de evaluatie van de beveiliging van AgO, van 28 november 2016, ontvangen op 1 december 2016;
8. Gelet op de evaluatie van de beveiliging van het departement KB, van 22 november 2016, ontvangen op 1 december 2016;
9. Beslist op van 7 december 2016, na beraadslaging, als volgt:

II. ONDERWERP EN CONTEXT VAN DE AANVRAAG

10. Op het ogenblik waarop zich een crisis voordoet en waarbij personeelsleden (van meerdere entiteiten) en/of infrastructuur van de Vlaamse Overheid getroffen of bedreigd worden, kan het coördinatie- en crisiscentrum (CCVO) samengeroepen worden. Het CCVO neemt dan de nodige maatregelen met het oog op de veiligheid van de personeelsleden van de Vlaamse Overheid en ter vrijwaring van haar voorzieningen.

11. Deze taak vloeit voort uit de beslissing van de Vlaamse Regering van 6 mei 2011 in het kader van de "Aanpak inzake bedrijfscontinuïteitsplanning binnen de Vlaamse administratie" (in bijlage bij de aanvraag). Om deze taken meer concreet invulling te geven, zal binnenkort een document over de rollen en verantwoordelijkheden van het CCVO ter bekrachtiging voorgelegd worden aan de Vlaamse Regering (in bijlage bij de aanvraag). Op dit ogenblik wordt ook gewerkt aan een update van het crisiscommunicatieplan voor het CCVO.

12. Deze machtigingsaanvraag vloeit voort uit de taak van het CCVO om in crisissituaties¹ de crisiscommunicatie ten aanzien van de personeelsleden van de Vlaamse Overheid te verzorgen.

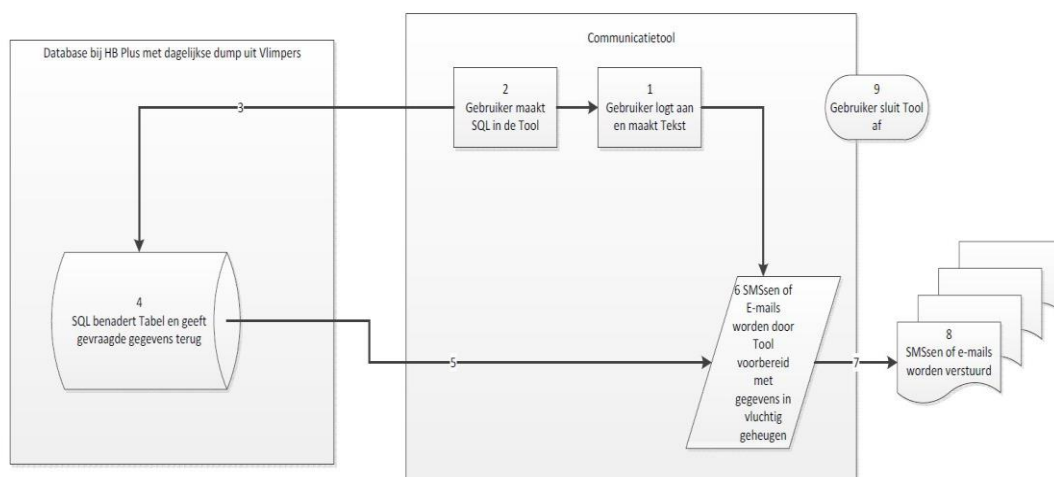
13. Deze machtigingsaanvraag heeft betrekking op de elektronische mededeling van persoonsgegevens die zich in Vlimpers bevinden. Voor deze machtiging worden een aantal vooraf gedefinieerde gegevens (zie verder) uit Vlimpers elke nacht geüpload op een beveiligde dropserver.

¹ Telkens in deze aanvraag gesproken wordt over crisissituaties worden hier uitzonderlijke situaties bedoeld waarbij personeelsleden (van meerdere entiteiten) en / of infrastructuur van de Vlaamse Overheid getroffen wordt, en tijdens de welke het CrisisCentrum van de Vlaamse Overheid optreedt.

14. Tijdens een uitzonderlijke crisissituatie zal het CCVO beslissen om de aangeschafte crisiscommunicatietool te gebruiken en in functie van het soort crisis zal het CCVO de inhoud van de boodschap bepalen en welke personeelsleden op welke wijze geïnformeerd zullen worden.

Nadat dit gebeurd is, zal ingelogd worden op de tool en zal de boodschap via de tool met het gekozen communicatiekanaal verstuurd worden.

15. De wijze waarop dit gebeurt, wordt verduidelijkt in onderstaand schema:



1. Een medewerker van het CCVO logt aan op een beveiligde manier in de tool over het internet en selecteert of hij een e-mail of een SMS wil versturen aan een doelgroep. Hij schrijft daarvoor de nodige teksten.
2. Hij definieert een doelgroep adhv een SQL (Sequel statement).
3. Deze SQL wordt door de tool op een beveiligde manier verstuurd naar de database die elke nacht gevoed wordt door Vlimpers (HRM-applicatie van AgO).
4. De database interpreteert de SQL en bouwt een file op met de gevraagde gegevens.
5. Deze gevraagde gegevens worden op een beveiligde manier verzonden naar de tool.
6. De tool opent de file met de gevraagde gegevens in een vluchtig geheugen, zodat de medewerker van het CCVO een controle kan uitvoeren.
7. De medewerker van het CCVO gaat akkoord en geeft de opdracht tot verzenden.
8. De tool bouwt en verzendt de SMSsen en e-mails, waarna de gegevens verdwijnen uit het vluchtige geheugen. De verzending gebeurt over respectievelijk het GSM netwerk of over het internet.
9. De medewerker van het CCVO sluit de tool op een beveiligde manier af. De tool bevat geen gegevens meer.

III. ONDERZOEK VAN DE AANVRAAG

A. ONTVANKELIJKHEID

16. Het betreft identificatiegegevens en contactgegevens van personeelsleden van de entiteiten van de Vlaamse Overheid die gebruik maken van Vlimpers.

17. De personen worden geïdentificeerd aan de hand van naam en voornaam en contactgegevens. In casu betreft het een latere verwerking van gegevens die informatie bevatten omtrent een geïdentificeerde natuurlijke persoon. Deze gegevens kunnen dus als persoonsgegevens in de zin van artikel 1, §1, WVP, gekwalificeerd worden.

18. Aangezien deze persoonsgegevens op een geautomatiseerde wijze worden verwerkt, is de WVP van toepassing².

19. Overeenkomstig artikel 8, eerste lid, van het e-govdecreet vereist elke elektronische mededeling van persoonsgegevens door een instantie³ een machtiging van de VTC, tenzij de elektronische mededeling van gegevens al onderworpen is aan een machtiging van een ander sectoraal comité, opgericht binnen de Commissie voor de Bescherming van de Persoonlijke Levenssfeer.

20. De persoonsgegevens worden in eerste instantie opgevraagd bij AgO. AgO is een intern verzelfstandigd agentschap zonder rechtspersoonlijkheid, behorend tot het beleidsdomein Kanselarij en Bestuur⁴. AgO is dus een instantie, vermeld in artikel 4, §1, 2°, decreet van 26 maart 2004 betreffende openbaarheid van bestuur, en valt dus onder het toepassingsgebied van artikel 8 van het e-govdecreet.

² Art. 3, §1 WVP.

³ Het begrip 'instantie' wordt gedefinieerd in artikel 2, 10°, van het decreet als: "een instantie, vermeld in artikel 4, §1, van het decreet van 26 maart 2004 betreffende openbaarheid van bestuur".

Art. 4. § 1. Dit decreet is van toepassing op de volgende instanties :

1° het Vlaams Parlement en de eraan verbonden instellingen;

2° de diensten, instellingen en rechtspersonen die afhangen van de Vlaamse Gemeenschap of het Vlaamse Gewest;

3° de gemeenten en de districten;

4° de provincies;

5° de andere gemeentelijke en provinciale instellingen, met inbegrip van de verenigingen zonder winstoogmerk waarin één of meer gemeenten of de provincies minstens de helft van de stemmen in één van de beheersorganen heeft of de helft van de financiering voor haar rekening neemt;

6° de verenigingen van provincies en gemeenten, bedoeld in de wet van 22 december 1986 betreffende intercommunales, en de samenwerkingsvormen zoals geregeld in het decreet van 6 juli 2001 houdende intergemeentelijke samenwerking;

7° de openbare centra voor maatschappelijk welzijn, hierna O.C.M.W.'s te noemen, en de verenigingen, bedoeld in hoofdstuk 12 van de organieke wet van 8 juli 1976 betreffende O.C.M.W.'s;

8° de polders, bedoeld in de wet van 3 juni 1957 betreffende polders, en de wateringens, bedoeld in de wet van 5 juli 1956 betreffende wateringens;

9° de kerkfabrieken en de instellingen die belast zijn met het beheer van de temporalien van de erkende erediensten;

10° alle andere instanties binnen het Vlaamse Gewest en de Vlaamse Gemeenschap.

⁴ Besluit van de Vlaamse regering van 11 juni 2004 tot oprichting van het intern verzelfstandigd agentschap "Agentschap voor Overheidspersoneel".

21. De VTC is derhalve bevoegd om voorliggende machtigingsaanvraag te behandelen.

B. TEN GRONDE

B.1. FINALITEITSBEGINSEL

22. Artikel 4, §1, 1°, WVP, stelt dat iedere verwerking van persoonsgegevens eerlijk en rechtmatig moet zijn. Dit houdt in dat iedere gegevensverwerking dient te gebeuren op een transparante wijze en mits naleving van het recht. Overeenkomstig artikel 4, §1, 2°, WVP, dienen persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en mogen zij niet verder worden verwerkt op een wijze die, rekening houdende met alle relevante factoren, met name de redelijke verwachtingen van de betrokkene en met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden. De VTC onderzoekt hierna de verschillende aspecten van dit finaliteitsbeginsel.

Oorspronkelijk doeleinde van de gegevensverwerking:

23. De personeelsgegevens in Vlimpers worden nu gebruikt voor de verschillende HR-processen.

24. De wettelijke basis hiervoor ligt in artikel 4, §2, 7° van het Besluit van de Vlaamse Regering tot oprichting van het intern verzelfstandigd agentschap "Agentschap Overheidspersoneel"⁵.

Doeleinde van de verdere verwerking:

25. Het toekomstige doeleinde is het doelgericht en snel informeren van personeelsleden van de Vlaamse Overheid in uitzonderlijke crisissituaties, zodat zij snel en accuraat op de hoogte zijn van de laatste stand van zaken en kennis kunnen nemen van de evt. te nemen maatregelen. Enkele voorbeelden illustreren dit:

- binnen blijven in een bepaald gebouw bij een ernstig incident in de directe omgeving (terreur, gaswolk,...)
- vraag om gedurende bepaalde periode niet in een gebouw te werken (omwille van onbeschikbaarheid van een gebouw) en maximaal te telewerken;
- alle personeelsleden inlichten over de verschillende maatregelen nav een lockdown in een stad;
- ...

⁵ Vervangen bij BVR 13 april 2015, art. 17, in werking: 1 april 2015)⁵

26. De wettelijke basis is de beslissing van de Vlaamse Regering op 6 mei 2011 tot de oprichting van het CCVO (zie bijlage bij de aanvraag). In deze beslissing wordt de rol van het CCVO als volgt verduidelijkt: "Het coördinatie- en crisiscentrum is een virtueel centrum dat geactiveerd wordt bij een incident of een crisis, met impact op meerdere entiteiten en beleidsdomeinen. [...] Het coördinatie- of crisiscentrum kan eveneens in actie treden op vraag van een entiteit of een beleidsdomein."

27. Het CCVO is een virtueel centrum dat geactiveerd wordt bij een incident of crisis. Het is geen operationele entiteit of afdeling, maar een virtueel contactpunt dat in tijden van calamiteiten of crisissen uitgebouwd wordt tot een operationele cel. Het centrum treedt in werking als de voorzitter via het centrale meldnummer een melding krijgt van het incident of calamiteit en beslist dat er tot alarmering dient te worden overgegaan.⁶

28. Crisiscommunicatie maakt hiervan een belangrijk onderdeel uit (zie onder andere: vaste vertegenwoordiging in het CCVO van de toenmalige afdeling communicatie van het departement DAR). Het crisiscommunicatieteam staat bovendien in nauw contact met het crisismanagementteam.

29. Op 23 mei 2014 besliste de Vlaamse Regering onder andere om de taakstelling van het CCVO uit te breiden met crisiscoördinatie gerichte op externe crisissituaties. (zie bijlage bij de aanvraag).

30. Naar aanleiding van de recente gebeurtenissen op het vlak van terreurdreiging en naar aanleiding van de aanslagen in Brussel van 22 maart 2016 heeft het CCVO ervaren dat een gerichte en eenduidige informatiestroom ten aanzien van de personeelsleden aangewezen is via verschillende communicatiekanalen (zie hiervoor ook de verslagen van de bijeenkomsten van het College van Voorzitters van 21 januari 2016 en 19 mei 2016; en de bijhorende documenten in bijlage bij de aanvraag).

31. De VTC is van oordeel dat de doeleinden in randnummer 25 e.v. welbepaald en uitdrukkelijk omschreven zijn in de zin van artikel 4, §1, 2°, WVP.

32. Aangaande vereiste van verenigbaarheid met het oorspronkelijk doeleinde, wijst de VTC erop dat de geplande verwerkingen, bestaan uit latere verwerkingen van gegevens die oorspronkelijk voor andere doeleinden werden verwerkt. De rechtmatigheid van deze latere verwerkingen is aldus afhankelijk van hun verenigbaarheid met de oorspronkelijke verwerking.

33. Overeenkomstig artikel 4, §1, 2°, WVP, mogen persoonsgegevens immers niet verder worden verwerkt op een wijze die, rekening houdende met alle relevante factoren, met name de redelijke verwachtingen van de betrokkene en met de toepasselijke wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden.

⁶ Nota aan de Vlaamse Regering van 6 mei 2011 betreffende de aanpak inzake continuïteitsplanning binnen de Vlaamse administratie.

34. De personeelsleden van wie de persoonsgegevens worden opgenomen in Vlimpers, kunnen verwachten dat hun identificatiegegevens en contactgegevens verder verwerkt worden in het kader van crisiscommunicatie van hun werkgever, de Vlaamse Overheid.

35. Er kan dus geoordeeld worden dat de doeleinden van de latere verwerking verenigbaar zijn met deze van de oorspronkelijke verwerking.

36. Het toekomstige doel is rechtmatig te noemen.

37. Niettemin moet wel rekening worden gehouden met de belangen van de betrokkenen. Vandaar dat de vereisten van transparantie en beveiliging een doorslaggevende rol spelen (zie onder B.3 en B.5)

B.2. PROPORTIONALITEITSBEGINSEL

B.2.1. Aard van de gegevens

38. Overeenkomstig artikel 4, §1, 3°, WVP, moeten persoonsgegevens toereikend, terzake dienend en niet overmatig zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt.

39. Er worden enkel gegevens opgevraagd zolang iemand personeelslid is van de Vlaamse Overheid en het van belang is dat hij/zij geïnformeerd kan worden bij het optreden van een crisis. Zodra hij/zij geen personeelslid meer is, is deze informatiedoorstroom niet langer van toepassing.

40. Het betreft de volgende persoonsgegevens van de personeelsleden van de entiteiten van de Vlaamse Overheid die gebruik maken van Vlimpers.

Exacte behoefte	Proportionaliteit
<i>Basisidentificatiegegevens</i> <i>Naam en voornaam</i>	Nodig om het personeelslid gericht te kunnen informeren.
<i>Contactgegevens van de gebruiker</i> <i>Werkadres (waar het personeelslid zijn/haar standplaats heeft):</i> straat nummer gemeente naam gebouw	Deze gegevens zijn nodig om met de gebruiker in contact te kunnen komen, zowel wanneer hij of zij op kantoor werkt, van thuis uit, op verplaatsing of onderweg. Door deze gegevens beschikbaar te stellen wordt de gebruiker beter bereikbaar zowel rechtstreeks via telefoon, gsm, thuiswerknummer als onrechtstreeks via e-mail of fax. Deze communicatiemiddelen zijn onontbeerlijk in de dagelijkse werking van de Vlaamse Overheid-medewerker. Nodig om betrokken personeelsleden te kunnen bereiken via hun werkcoördinaten.

<p>Indien beschikbaar: <i>vast telefoon nummer werk</i> <i>gsm-nummer werk</i> <i>mailadres werk</i></p> <p>Indien beschikbaar: <i>vast telefoon nummer privé</i> <i>gsm-nummer privé</i> <i>mailadres privé</i></p>	<p>Nodig om betrokken personeelsleden te kunnen bereiken via hun privécoördinaten. Deze gegevens zullen steeds als eerste gebruikt worden</p> <p>Deze gegevens zullen pas gebruikt worden als het personeelslid niet bereikbaar is via zijn/haar werk-coördinaten De communicatietool geeft de mogelijkheid aan de geadresseerde om te antwoorden. Na 10 min zonder antwoorden kan het CCVO beslissen om naar hen die niet hebben geantwoord een voicebericht of SMS bericht te sturen naar een privé-nummer)</p>
--	--

41. Op dit ogenblik bevinden de gegevens zich in Vlimpers beheerd door het Agentschap Overheidspersoneel (AgO). Het CCVO heeft op dit ogenblik nog geen toegang tot deze gegevens.

42. Bij het optreden van een crisis bepaalt het CCVO/entiteit van de Vlaamse Overheid de inhoud van de boodschap, welke personeelsleden geïnformeerd zullen worden en welke communicatiekanalen (sms, e-mail, voicemailbericht) hiervoor gebruikt zullen worden. Elke nacht zullen personeelsgegevens uit het personeelssysteem (Vlimpers) op een beveiligde dropserver geüpload worden.

43. De medewerkers van DKB/entiteit van de Vlaamse Overheid zullen – op het ogenblik dat er zich een crisis voordoet en in functie van de opgetreden crisis - op deze gegevens een bevraging uitvoeren zodat de te verwittigen doelgroep exact zal afgelijnd worden.

44. Nadat dit gebeurd is, zal ingelogd worden op de tool en zal de boodschap via de tool met het gekozen communicatiekanaal verstuurd worden.

45. Op basis van de hierboven geanalyseerde elementen kunnen de gegevens worden beschouwd als relevant, evenredig en niet overmatig voor de doeleinden vermeld in randnummer 25 e.v.

B.2.2. Bewaringstermijn van de gegevens

46. Artikel 4, §1, 5°, WVP voorziet dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen of verder worden verwerkt.

47. Er werd gevraagd om de gegevens te bewaren afhankelijk van de tewerkstellingsperiode van het personeelslid. Bij de behandeling van het dossier werd verduidelijkt dat het wel degelijk de bedoeling is om elk etmaal de gegevens opnieuw uit Vlimpers te halen en dus niet langer dan een dag te bewaren.

48. De VTC kan akkoord gaan met de aangepaste bewaringstermijn.

B.2.3. Frequentie van de toegang

49. De toegang tot de gevraagde gegevens zou permanent zijn. Elke nacht worden de personeelsgegevens uit Vlimpers geüpload. Dit is nodig om steeds over de meest actuele gegevens te beschikken. Het betreft dus eigenlijk een periodieke opvraging.

50. De VTC kan akkoord gaan met de gevraagde frequentie.

B.2.4. Duur van de machtiging

51. De toegang en het gebruik wordt voor onbepaalde duur gevraagd, om de reden dat crisiscommunicatie steeds nodig zal zijn.

52. De VTC kan akkoord gaan met de gevraagde duur.

B.2.5. Bestemmingen en/of derden waaraan gegevens worden meegedeeld

53. Interne medewerkers: medewerkers van het departement KB die het virtuele team van het CCVO vormen.

54. Externe medewerkers:

- de gegevens van de externe verwerker zijn nog mee te delen van zodra het raamcontract gegund zal zijn. De externe gebruiker zal deze gegevens nodig hebben om de door het CCVO bezorgde boodschap via de/het gekozen communicatiekana(a)l(en) te kunnen bezorgen;
- aangezien elke leidend ambtenaar van een entiteit van de Vlaamse Overheid (VO) verantwoordelijk is voor de interne communicatie binnen diens entiteit, kan deze ook beslissen om bij het optreden van een crisis binnen de eigen entiteit gericht te communiceren t.a.v. de personeelsleden (of een deelgroep ervan). In dat geval kunnen zij afnemen van het raamcontract. Die entiteiten van de VO duiden dan een beperkt aantal personen aan die ook kunnen inloggen.

B.3. TRANSPARANTIEBEGINSEL

(artikelen 4, §1, 1°, en 9 tot 15bis, WVP)

55. Artikel 9 WVP voorziet in een verplichting tot informatie van de betrokken personen van wie persoonsgegevens worden gebruikt.

56. Indien de verantwoordelijke voor de verwerking de gegevens niet rechtstreeks bij de betrokkene heeft verkregen, kan evenwel op deze informatieverplichting een uitzondering worden gemaakt indien de registratie of de verstrekking van de persoonsgegevens verricht wordt met het oog op de toepassing van een bepaling voorgeschreven

door of krachtens een wet, een decreet of een ordonnantie. Op grond van artikel 9, §2, 2^e lid, b), WVP is in een dergelijke situatie een vrijstelling van informatieplicht van kracht.

57. Deze vrijstelling neemt echt niet weg dat de VTC er zich kan van vergewissen of er passende waarborgen worden voorzien voor de bescherming van de rechten van de betrokkenen.

58. Zodra de communicatietool zal aangekocht worden zullen personeelsleden hiervan persoonlijk op de hoogte gebracht worden via verschillende interne communicatiekanalen (mailing op entiteitsniveau, intranet, "13", nieuwsbrieven, ...).

59. De VTC kan akkoord gaan met deze wijzen van informatieverstrekking.

B.4. EXTERNE VERWERKERS EN DIENSTENINTEGRATOR

60. De externe verwerker, die in opdracht van de gevende organisatie werkt, is HBplus. HBplus voert het beheer uit van de toepassingen Vlimpers, incl. het beheer van alle daaraan gerelateerde besturingssystemen, middleware en hardware.

61. De externe verwerker van de ontvanger (nog niet aangewezen) stelt een tool ter beschikking voor crisiscommunicatie door het CCVO van het departement Kanselarij & Bestuur (DKB) t.a.v. personeelsleden van de VO (doelgroep te bepalen in functie van de crisis, zie verder). Een beperkt aantal medewerkers van DKB kunnen inloggen op deze tool.

62. HBplus biedt een nachtelijke 'databump' aan met de personeelsgegevens via een beveiligd platform. Er zijn georganiseerde gestructureerde overlegmomenten tussen HBplus en de Vlaamse overheidsdiensten waarin HBplus aan de betrokken Vlaamse overheidsdiensten rekenschap aflegt van onder andere de maatregelen die hij neemt opdat hij conform de privacywetgeving handelt. Ook ondertekenen alle HBplus-personeelsleden die persoonsgegevens verwerken in opdracht van Vlaamse overheidsdiensten een geheimhoudingsverklaring.

63. De VTC herinnert er aan dat ingeval van onderaanneming, de privacywet aan iedere verantwoordelijke voor de verwerking oplegt om zijn relatie met externe verwerker te omkaderen met een overeenkomst die voldoet aan de voorschriften van artikel 16, §1, WVP.

B.5. BEVEILIGING

64. De VTC wijst de verantwoordelijke voor de verwerking op de verplichtingen van artikel 16 WVP en op de richtsnoeren informatieveiligheid⁷.

65. Identificatiegegevens en contactgegevens van overheidspersoneel moeten ondermeer beschermd worden omwille van de mogelijkheid van *social engineering* en identiteitsdiefstal.

66. Elke nacht zullen de specifieke persoonsgegevens uit Vlimpers geüpload worden op een beveiligde dropservers in een xml- of csv-bestand. Dit bestand wordt de daarop volgende nacht overschreven zodat het CCVO steeds over de meest up to date gegevens zal kunnen beschikken. Dit xml-bestand zal door de tool die de dump uit Vlimpers voorziet geëncrypteerd worden zodat HBplus er geen inzage in kan hebben.

67. Tijdens een uitzonderlijke crisissituatie zal het CCVO beslissen om de aangeschafte crisiscommunicatietool te gebruiken en in functie van het soort crisis zal het CCVO de inhoud van de boodschap bepalen en welke personeelsleden op welke wijze geïnformeerd zullen worden. Hiertoe kan (enkel) de crisiscommunicatietool het geëncrypteerde Excelbestand decrypteren. Voor het bepalen van de doelgroep zal het CCVO een specifieke query op dit gedecrypteerde bestand uitvoeren. Tevens zal het CCVO de inhoud van de boodschap samenstellen. Na het verzenden van de boodschap verlaat het CCVO de communicatietool, dat alle banden verbreekt met het Excelbestand en de gedecrypteerde gegevens niet onthoudt.

68. Via een beveiligde procedure (ACM-IDM) zal het CCVO inloggen op het systeem van de externe verwerker, zodat de boodschap aan de gedefinieerde doelgroep bezorgd kan worden via het gekozen communicatiekanaal.

B.5.1. Op het niveau van de aanvrager

69. De veiligheidsconsulent van het departement KB is gekend bij het sectoraal comité van het Rijksregister.

70. Het departement is bezig met de opmaak van een geactualiseerd veiligheidsbeleid. De definitieve versie is gepland tegen 28 februari 2017.

⁷ http://www.privacycommission.be/sites/privacycommission/files/documents/richtsnoeren_informatiebeveiliging_0.pdf

B.5.2. Op het niveau van de instantie die de gegevens zal doorgeven

71. De veiligheidsconsulent van AgO is gekend bij het Sectoraal Comité van het Rijksregister (RR nr. 21/2013 (RN-MA-2013-001)).

72. Er werd nog geen veiligheidsplan of veiligheidsbeleid aan de VTC bezorgd. Gezien de ingrijpende reorganisatie binnen de Vlaamse Overheid en de wijzigingen waarmee Ago werd geconfronteerd, nam het uitwerken van dit informatiebeveiligingsbeleid in de lijn met de ISO 27002 meer tijd in beslag dan initieel werd vooropgesteld. In het najaar 2016 zou een eerste versie van een geschreven informatieveiligheidsbeleid voor de Vlimpersdata en ook bijhorende verdere actieplanning aan de VTC en Audit Vlaanderen worden bezorgd. In het formulier evaluatie beveiliging wordt gesteld dat het veiligheidsbeleid tegen januari 2017 zal uitgewerkt zijn en dat een aantal concrete realisaties (lijst van gemachtigde personen, logische beveiliging van de toegang en urgentiebeheer van informatiebeveiliging) tegen eind april 2017.

IV. BESLUIT

73. De VTC **machtigt** het Agentschap Overheidspersoneel om de gevraagde persoonsgegevens mee te delen aan het departement Kanselarij & Bestuur, CCVO, in het kader van crisiscommunicatie zoals beschreven in randnummer 25 e.v., onder de voorwaarden vermeld in deze machtiging.

74. De VTC vraagt dat AgO haar het veiligheidsbeleid bezorgt tegen 31 januari 2017 en dat AgO haar op de hoogte brengt van de tegen eind april 2017 geplande maatregelen.

75. De VTC vraagt dat het departement KB haar het aangepaste veiligheidsbeleid bezorgt tegen 31 maart 2017.

De voorzitter,

Willem Debeuckelaere