Vlaamse overheid

Aan de verwerkingsverantwoordelijken van de Vlaamse lokale besturen en hun agentschappen

Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens
Autonome dienst met rechtspersoonlijkheid

Koning Albert II-laan 15
1210 Brussel
https://overheid.vlaanderen.be/vlaamse-toezichtcommissie

PER MAIL

uw bericht van	uw kenmerk	ons kenmerk	bijlagen
		VTC/A/2023/09	2

vragen naar / e-mail	telefoonnummer	datum
Anne Teughels contact@toezichtcommissie.be	02 553 20 85	

Betreft: Instrument beoordeling leveranciers:
Vragenlijst voor verificatie adequate beveiligingsmaatregelen leveranciers-verwerkers van Vlaamse (Lokale) Besturen

Geachte algemeen-directeur,
Geachte verwerkingsverantwoordelijke,

De aanleiding voor deze brief zijn enerzijds de conclusies uit het Globaal rapport - thema-audit Beheer van ICT-risico's bij lokale besturen van Audit Vlaanderen van 13 juni 2023 en anderzijds de meldingen van datalekken door de lokale besturen bij de VTC, waarbij regelmatig gemerkt wordt dat de nodige beveiliging niet geregeld werd, niet afgedwongen werd t.o.v. de leverancier of niet geleverd werd/wordt door de leverancier.

De vragenlijst in bijlage is bedoeld als een instrument ter ondersteuning van de verwerkingsverantwoordelijken, en in het bijzonder van de leidinggevenden van de lokale besturen. De rol van de functionarissen voor gegevensbescherming is om hen daarbij te adviseren.

De vragenlijst is bedoeld om na te gaan of leveranciers die persoonsgegevens voor het bestuur verwerken (kunnen) voldoen aan bepaalde minimale beveiligingsverplichtingen en men deze dus kan contracteren in kader van bepaalde diensten of kan blijven contracteren (wat niet het geval is indien de nodige beveiligingsmaatregelen niet (meer) gegarandeerd kunnen worden).

Dit zou normaal geen extra werk mogen betekenen aan uw zijde of leverancierszijde:

a) normaal gezien beschikt u al over de beperkte door u in te vullen informatie voor uw verwerkingen,
b) leveranciers zouden voor al hun diensten de gevraagde informatie "off-the-shelf" moeten kunnen halen (en deze zou overigens hetzelfde moeten zijn voor elk van de besturen waaraan zij gelijkaardige diensten leveren[1]).

De vragenlijst helpt u ook in het kader van de verantwoordingsplicht van de AVG aangezien die u vraagt om de conformiteit met de AVG, in het bijzonder met artikel 28, 29 en 32, AVG, ook te kunnen aantonen en dus te documenteren.

Het gebruik van deze vragenlijst is niet verplicht, maar u wordt wel geacht op al deze vragen te kunnen antwoorden. De VTC wil wel ten sterkste aanraden om deze tool te gebruiken.

Hoe aanpakken?

A. Verwerkingen

U vult eerst de basisgegevens van de verwerking in en geeft dan de vragenlijst door aan de leverancier.

De vragen moeten gesteld en beantwoord worden per verwerking van persoonsgegevens en dit in principe voor alle verwerkingen die het bestuur laat uitvoeren door een verwerker. De verwerkingen zouden al moeten opgenomen zijn in uw verwerkingsregister.

De vragenlijst is niet bedoeld voor de verwerkingen die u zelf uitvoert.

De vragenlijst geldt zeker ook voor oude toepassingen en systemen die, zoals meermaals werd vastgesteld, te weinig aandacht krijgen wat beveiliging betreft.

U kan de leverancier uitleg vragen als er meerdere verwerkingen aan diezelfde leverancier worden toevertrouwd en er daardoor onduidelijkheid is.

B. De leverancier-verwerker

De leveranciers moeten de vragen in de tabel in verband met de verwerkingen onder uw toezicht beantwoorden en voorzien van het nodige bewijsmateriaal (dat zij in principe dus "off-the-shelf" zouden moeten liggen hebben).

C. Advies

Uw functionaris voor gegevensbescherming en uw security-verantwoordelijke moeten in hun adviesverlenende en toezichtfunctie betrokken worden bij deze oefening.

[1] De VTC suggereert dat voor gelijkaardige diensten afspraken gemaakt worden tussen de besturen.

D. De vragen

De vragen zijn gericht op de basisvereisten van de AVG inzake beveiliging. Beveiliging houdt niet alleen technische beveiliging in, maar heeft ook een organisatorische component die ook aandacht krijgt in de vragen.

De vragen zijn gebaseerd op ISO-standaarden, die vereenvoudigd en waar mogelijk ook samengenomen werden.

E. De antwoorden

Het is in uw belang als verantwoordelijke en zeker in het belang van de burgers dat de relatie met de verwerkers van het bestuur duidelijk wordt en de risico's in kaart worden gebracht en verholpen.

F. De gevolgen

De VTC wijst erop dat verwerkingen die niet of onvoldoende aan deze basisvereisten voldoen moeten geremedieerd worden en zo dat niet kan binnen een redelijke termijn, moeten worden stopgezet. Voor verwerkers en verwerkingen die niet voldoen, moet:

- bij ernstige afwijkingen of zware risico's de verwerking stilgelegd worden;
- bij belangrijke afwijkingen een alternatief worden gezocht binnen een termijn van 6 maanden;
- bij "medium" afwijkingen een alternatief worden gezocht binnen een termijn van 6 maanden.

De VTC zal vanaf 2025 bij meldingen van datalekken opvragen of de vragenlijst gebruikt is.

G. Feedback

We nodigen u uit om feedback te geven op de vragenlijst zodat deze als instrument kan groeien.
U kan dit doen via het secretariaat van de VTC.

Alvast bedankt voor uw medewerking aan een veiligere verwerking van persoonsgegevens,

Hans Graux
Voorzitter VTC