Bijlage 2. A.
Vragenlijst inzake aanwezigheid en effectiviteit van de Organisatorische en Technische maatregelen voor de bescherming van (persoons)gegevens
<< deel in te vullen door verwerkingsverantwoordelijke >>

A. 1. Identificatie van de verwerking

Naam verwerkingsverantwoordelijke(n):

Naam/aanduiding verwerking persoonsgegevens:

Bv. MijnDossier

Over welk product of dienst gaat het:

Bv. CRM om … te ondersteunen

Welke bijzondere categorieën van persoonsgegevens in de zin van artikel 9 van de AVG of persoonsgegevens van zeer gevoelige aard[1] worden verwerkt?

Bv. Gezondheidsgegevens, inkomensgegevens, geloofsovertuiging, seksuele voorkeur

Van hoeveel personen worden er gegevens verwerkt?

Naam (hoofd)verwerker(s):

Adres hoofdzetel van de (hoofd)verwerker(s):

[1] Zie DPIA-lijst VTC (categorie A.3) https://www.vlaanderen.be/vlaamse-toezichtcommissie/machtigingen-en-adviezen-vlaamse-toezichtcommissie/lijst-vtc-criteria-geb-dpia

A.2. Basisvragen voor de verantwoordelijke over de verwerking

Beantwoord elke vraag en vermeld de naam en vindplaats van het stavingstuk.

De antwoorden op de vragen moeten ook betrekking hebben op de verwerkingen door subverwerker(s).

VRAGEN	NEE	JA	GETEST	STAVINGSSTUKKEN	Korte uitleg
Beheer verwerking					Leg eventueel verder uit in een bijlage
Is de documentatie inzake de verwerking actueel en acuraat?					
Werd u op de hoogte gebracht van eventuele (recente) wijzigingen aan de verwachte verwerking ?					
Werd/wordt er een verwerkingsovereenkomst ondertekend voor de verwerking werd/wordt aangevat?					
Werd uw DPO geraadpleegd?					
Werd(en) de DPO(s) van de verwerker(s) geraadpleegd?					
Worden er (andere) subverwerkers ingeschakeld?				Benoem subverwerkers en verwerkersovereenkomsten met hen	
Bescherming persoonsgegevens					
Wordt de uitoefening van de rechten van de betrokkenen gegarandeerd i.k.v. de toepassing/het platform?					
Is er een PDO/contactpersoon bij de verwerker voor AVG-vragen					

ter ondersteuning van uw DPO?					
Naam en functie verwerkingsverantwoordelijke					
Datum					
Ik verklaar dat de antwoorden juist zijn en geen belangrijke tekortkomingen verhullen. Ik verplicht mij om de stavende stukken te overhandigen.				Handtekening	

Bijlage 2. B.

Vragenlijst inzake aanwezigheid en effectiviteit van de Organisatorische en Technische maatregelen voor de bescherming van (persoons)gegevens

<< deel in te vullen door verwerker >>

In te vullen door de hoofdverwerker/hoofdcontractant:

Beantwoord elke vraag en vermeld de naam en vindplaats van het stavingstuk dat u ter beschikking houdt van de VTC.

De antwoorden op de vragen moeten ook betrekking hebben op de verwerkingen door subverwerker(s).

VRAGEN	NEE	JA	GETEST	STAVINGSSTUKKEN	Korte uitleg
Beschrijving van de dienst					
Is de documentatie inzake de geleverde dienst actueel en accuraat?					
Werd de verwerkings-verantwoordelijke op de hoogte gebracht van eventuele (recente) wijzigingen aan de geleverde dienst?					

Werd/wordt er een verwerkingsovereenkomst ondertekend voor de verwerking werd aangevat? Werd/wordt deze aangepast voor eventuele wijziging?					
Organisatorische Maatregelen					
ISO 5.1 - Is er een duidelijke security policy die alle domeinen van de ISO 27001/27002 afdekt – rekening houdende met beschreven “te beschouwen dimensies”?					
ISO 5.2 - Zijn de rollen en verantwoordelijkheden vastgelegd met name in zake CISO, DPO, operationeel beheer, incidentenbeheer?					
ISO 5.3 - Is functiescheiding toegepast om ongeoorloofde acties onmogelijk te maken?					
ISO 5.12/5.13 - Wordt er een classificatie van data en van systemen toegepast?					

ISO 5.16/5.17/5.18 - Is er een strikt gebruikers- en toegangsbeheer? Met name voor geprivilegieerde beheerders?					
ISO 5.19 - Worden de contractuele verplichtingen 1-op-1 doorgezet naar uw subverwerkers en houdt u daar minimaal jaarlijks toezicht op?					
ISO 5.20 - Worden alle belangrijke activiteiten (met name van beheerders) in onwijzigbare audittrails vastgelegd die toegankelijk zijn voor de verwerkings-verantwoordelijke?					
ISO 5.21/5.22/5.23 - Hebt u duidelijke regels inzake levering en gebruik van software en hardware en (security) testing – toepasselijk voor elke wijziging?					
ISO 5.24 – Zijn er duidelijke systemen en processen voor het beheren (en coördineren) van veiligheidsincidenten?					

ISO 5.34 – Kent u de regels inzake privacybescherming en de bescherming van persoonsgegevens en past u die toe?					
Personele Maatregelen					
ISO 6.1 / 6.2 /6.3 – Zijn er duidelijke regels en is er toezicht op gedrag van geprivilegieerde beheerders? En worden veiligheidsregels jaarlijks herhaald in hun training?					
ISO 6.4/6.5/6.6 - Zijn er duidelijke regels in geval van non-compliant gedrag? Bij het veranderen van functie of verlaten van de firma? Zijn al uw medewerkers gebonden door een geheimhoudings-clausule?					
ISO 6.7 / 6.8 – Zijn er duidelijke regels inzake werken op afstand (enkel middels systemen van de verwerker) + het rapporteren van					

eventuele/mogelijke veiligheidsincidenten?					
Fysieke Maatregelen					
ISO 7.1/7.2/7.3/7.4 - Zijn de toegang tot de systemen en de systemen die gebruikt worden bij beheer op niveau?					
ISO 7.5/7.6/7.7/7.8/7.10/7.11 - Zijn adequate maatregelen getroffen die ongeauthoriseerde toegang tot systemen en dragers van data in principe onmogelijk maken?					
Technologische Maatregelen					
ISO 8.1 – Beschikken beheerders over adequate en beveiligde systemen?					
ISO 8.2 / ISO 8.3 / ISO 8.4 - Hebt u een aparte priviliged access management omgeving (PAM)? Wordt voor (beheers)toegang op afstand gebruik gemaakt van een VPN?					

En is toegang beperkt tot een need-to-know?					
ISO 8.5 - Past u sterke authenticatie toe op al uw processen en MFA voor alle geprivilegieerde toegangen?					
ISO 8.7 / 8.8 – Zijn uw systemen maximaal beschermd tegen malware? Test u uw systemen adequaat tegen kwestbaarheden?					
ISO 8.10 / 8.11 / 8.12 / 8.13 – Beschermt u data adequaat en conform hun CIA-classificatie-niveaus?					
ISO 8.14 – Beschikt u conform de CIA-classificatie over de nodig back-up en disaster recovery systemen?					
ISO 8.15/8.16 - Beschikt u over adequate logging en monitoring om security incidenten te kunnen detecteren?					
ISO 8.20 / 8.21 / 8.22 – Is uw infrastructuur opgezet volgens					

de regels van de kunst om data en systemen adequaat genoeg te scheiden?					
ISO 8.24 – Past u waar nodig adequate cryptografische maatregelen toe zoals signing of encryptie?					
ISO 8.25 / 8.26 / 8.27 / 8.28 / 8.29 – Heeft u een software delivery pipeline die elke code-/config-wijziging valideert op fouten/non-compliancies …?					

* mits naleving van de richtlijnen van de VTC i.v.m. cloud

** met logging wordt in dit geval bedoeld: veiligheidslogging (artikel 24, AVG)

De verwerker,	
Naam en functie van de persoon die tekent namens de verwerker *(wettelijke vertegenwoordiger – NIET de DPO)*	
Datum	

Ik verklaar dat de antwoorden juist zijn en geen belangrijke tekortkomingen verhullen. Ik verplicht mij om de stavende stukken te overhandigen.	Handtekening