Informatieveiligheid bij <leveranciersnaam>

<Contactpersoon>

Deze toelichting heeft betrekking op het product/dienst <invullen naam toepassing of dienst>. Voor verdere toelichting kan u zich wenden tot <contactpersoon leverancier> via <contactmogelijkheid en gegevens van de leverancier>. Meer informatie over de toepassing is te verkrijgen via <publieke weblink naar het product/dienst waar meer info te vinden is>

[Adres van het bedrijf]

1 Waarom deze vragenlijst?

Het WZC heeft de wettelijke verplichting om een informatieveiligheidsbeleid en –plan op te stellen om gevoelige persoonsgegevens adequaat te beschermen. Wanneer een bedrijf toegang heeft tot gegevens van medewerkers of bewoners van het WZC in het kader van het leveren van een product of dienst, dan dienen de veiligheidscriteria voor informatieveiligheid in kaart te worden gebracht. Dit is een wettelijke verplichting die voortvloeit uit artikel 16 van de wet van 8/12/1992 bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

2 Wat verwacht het WZC van haar leveranciers?

Het WZC werkt voor wat betreft informatieveiligheid aan de hand van de ISO 27000 methodologie, zoals aanbevolen door de Privacycommissie (Aanbeveling nr 01/2013 van 21 januari 2013). De leverancier verbindt zich er toe een informatieveiligheidsbeleid uit te werken volgens dezelfde of gelijkaardige principes, meer in het bijzonder de methodologie die beschreven staat in ISO 27001:2013 en de maatregelen zoals opgelijst in ISO 27002:2013 en ISO 27799:2008.

3 Een leverancier die persoonsgegevens bewaart in de cloud?

In haar Advies nr 04/2015 van 25 februari 2015 geeft de Privacycommissie aan dat een WZC, alvorens gebruik te maken van een systeem in de cloud, een analyse maakt van de veiligheidsvoorzieningen. Elke leverancier die aan het WZC dergelijke diensten levert, vult daartoe de SMALS Cloud Security Model evalutatietool[1] in.

[1] https://www.smalsresearch.be/tools/cloud-security-model-nl/

NR	Na te leven norm	Voldoet J/N/NVT[2]	Toelichting van de leverancier	Wanneer zal de leverancier voldoen?
1 Risicobeheer en Organisatie van informatieveiligheid				
1	De leverancier voert op regelmatige basis risicoanalyses uit op de geleverde producten en diensten om na te gaan in welke mate deze voldoen aan de veiligheidsvereisten.			
2	De leverancier engageert zich om elk relevant risico in het product of dienstverlening binnen een zo kort mogelijke periode te melden aan het WZC. Met relevant wordt bedoeld een risico waarbij het veiligheidsniveau van de persoonsgegevens in de toepassing of dienstverlening in het gedrang komt zoals gegevenslekken, hacking, onderbreking van een systeem in productie			
3	De leverancier werkt volgens de ISO 27000 methodologie of gelijkaardig, en heeft een veiligheidsbeleid, veiligheidsplan en veiligheidsverantwoordelijke (veiligheidsconsulent en/of Data Protection Officer) aangesteld.		<Wie is de Security Officer of Data Protection Officer>	
2 Omgang met personeelsleden en onderaannemers				
4	De leverancier heeft informatieveiligheid meegenomen in de overeenkomsten met personeelsleden en contractanten. Ze zijn bij gevolg op de hoogte hoe met gevoelige persoonsgegevens moet worden omgegaan.			
5	De leverancier neemt informatieveiligheid mee in de overeenkomsten met onderaannemers. De leverancier heeft met andere woorden controle over de veiligheidsmaatregelen die de onderaannemers nemen.		<Welke toeleveranciers hebben (direct of indirect) toegang tot de gegevens van het WZC en voor welke taken is deze toegang uitgevaardigd?>	
3 Toegangscontrole van de leverancier tot systemen van het WZC				
6	De leverancier verklaart toegangscodes tot systemen die direct of indirect toegang verlenen tot informatie van het WZC of systemen die over het WZC informatie bevatten, te beheren als een goede huisvader. Dit omvat de nodige beveiligingsvereisten, ook bij beëindiging van contracten met medewerkers			
7	De leverancier verklaart op elk moment te kunnen nagaan wie toegang had tot de informatie van het WZC. Om dit te realiseren, wordt gebruik gemaakt van gepersonaliseerde toegangscodes voor alle identiteiten.		<tot hoe lang kan men teruggaan in de tijd?>	
8	De toegangscodes die worden gebruikt voor het leveren van producten en diensten zijn uniek voor het WZC en worden niet gedeeld in configuraties met andere ziekenhuizen. Voorbeelden van toegangscodes zijn deze voor het			

[2] J=Ja, N=Neen, NVT=niet van toepassing

	aanspreken van een databank, voor toegang tot de applicatie, voor de configuratie van geplande taken en services, voor het maken van verbindingen met externe informatiesystemen, voor de koppeling met medische apparatuur.			
9	De leverancier verklaart toegangscodes, cryptografische sleutels en andere gevoelige informatie op een veilige manier te bewaren. Dit omvat het gebruik van beveiligde informatiecontainers die enkel toegankelijk zijn voor gemachtigde medewerkers.			
4 Beveiliging van de gegevens van het WZC in de geleverde toepassing				
10	De toepassingen die de leverancier levert zijn voorzien van een systeem van toegangsbeveiliging voor de eindgebruiker dat geïntegreerd kan worden in het gebruikersbeheerssysteem van het WZC.		<Indien dit niet het geval is, geef aan in welke mate de toepassing voldoet aan volgende eisen: - De toegang is nominatief in te stellen (gebruikersnaam per gebruiker) - De toegangscode (wachtwoord) is vrij te kiezen door de eindgebruiker en er is een mogelijkheid om deze zelf te wijzigen - De toegangscodes van de applicatie worden op een veilige manier (i.e. geëncrypteerd) uitgewisseld tussen de systeemcomponenten - De toegangscodes worden in een niet leesbaar formaat bewaard in de toepassing>	
11	Handelingen van de gebruiker in de toepassing kunnen worden opgespoord via de logging. Het omvat de logging op leesactiviteiten, wijzigingen die worden doorgevoerd, nieuwe dataelementen die worden aangemaakt of informatie die wordt verwijderd. De logging is beveiligd tegen wijzigingen door de eindgebruiker zelf.			
12	De leverancier dupliceert nooit gegevens zonder toelating van het WZC van GZA VZW. Wanneer gegevens de toepassing verlaten, bijvoorbeeld via een USB stick, door een kopij op afstand of in het kader van een klassieke uitwisseling tussen systeemcomponenten, dan neemt de leverancier veiligheidsmaatregelen om de gegevens te beveiligen. Dit is minstens encryptie van de gegevens zelf en het transportkanaal waarover de gegevens worden getransporteerd.			

5 Ontwikkeling van veilige systemen en producten				
13	De door de leverancier geleverde of gebruikte toepassing voldoet aan de veiligheidsstandaarden zoals deze van de OWASP top 10. De toepassing wordt op regelmatige tijdstippen hierop gescreend door eigen medewerkers én door een derde, onafhankelijke partij. De resultaten hiervan zijn opvraagbaar door het WZC van GZA VZW.			
14	Wanneer de leverancier systemen voorziet of gebruikt waarop gegevens van het WZC worden bewaard (in test, demo of productie), dan zijn deze systemen beveiligd. Hieronder verstaan we dat de systemencomponenten permanent bijgewerkt zijn met de laatste bijwerkingen (vb updates van het besturingssysteem en toepassingen), dat er beveiliging is tegen malware en dat het systeem voorzien is van een backup.		<Wanneer het WZC zelf instaat voor de veiligheid van de ICT omgeving van het product of dienst kan dit hier te worden aangegeven>	
15	Bij een beëindiging van de overeenkomst met de leverancier, al dan niet op een vooraf bepaald moment, behoudt het WZC het recht om de gegevens te kunnen exporteren in een leesbaar formaat.		<Niet van toepassing als het WZC zelf instaat voor de veiligheid van de ICT omgeving van de toepassing>	