Naam van de Organisatie (derde partij)	**Byteflies NV** Borsbeeksebrug 22, 6de verdieping, 2600 Antwerpen Ondernemingsnummer (KBO) BE0628.669.272
Voornaam, Naam, & email adres van de verantwoordelijke voor informatieveiligheid (CISO) (verplicht)	Tim Bogaert tim.bogaert@byteflies.com
Voornaam, Naam, & email adres van het aanspreekpunt voor informatieveiligheid (CISO) (optioneel)	/
Voornaam, Naam, & email adres van de functionaris voor gegevensbescherming (DPO) (verplicht)	Niels Van Thienen dpo@byteflies.com
Voornaam, Naam, & email adres van het lokale aanspreekpunt voor gegevensbescherming (adjunct DPO of vertegenwoordiger) (optioneel)	/
Voornaam, Naam, & email adres van de persoon belast met het dagelijks bestuur (CEO) (verplicht)	Hans Danneels hans.danneels@byteflies.com

	Vraag	JA of NEEN	Leg uit bij een ´neen` antwoord
1	Beschikt u over een formeel, geactualiseerd en door de verantwoordelijke voor het dagelijks bestuur goedgekeurd beleid voor informatieveiligheid?	**JA**	
2	Heeft u een risicobeoordeling voor elk proces/project rond informatieveiligheid/gegevensbescherming die u gebruikt voor de dienstverlening?	**JA**	
3	Binnen uw organisatie: is er een dienst belast met de informatieveiligheid die onder de directe, functionele leiding staat van de verantwoordelijke voor het dagelijks bestuur van de organisatie?	**JA**	
4	Beschikt u over een informatieveiligheidsplan goedgekeurd door de verantwoordelijke voor het dagelijks bestuur?	**JA**	
5	Hoeveel uren werden gepresteerd door de CISO en diens team? CISO Team	**160u / maand** **4u / maand**	
	Hoeveel uren opleidingen rond informatieveiligheid hebben de DPO en diens team gevolgd? DPO Team	**50u / jaar** **4u / jaar**	
6	Beschikt u over procedures voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen, zodat de projectverantwoordelijke rekening kan houden met de veiligheidsvereisten die in de minimale veiligheidsnormen beschreven worden?	**JA**	
7	Neemt u de gepaste maatregelen opdat de professionele, vertrouwelijke en gevoelige gegevens opgeslagen op mobiele media enkel toegankelijk zijn voor geautoriseerde personen?	**JA**	

	Vraag	JA of NEEN	Leg uit bij een ´neen` antwoord
8	Treft u de gepaste maatregelen, in functie van het toegangsmedium, voor de informatieveiligheid van de toegang van buiten uw organisatie tot de professionele, vertrouwelijke en gevoelige gegevens?	JA	
9	Heeft u de telewerk-voorzieningen zo ingericht dat er op de telewerk-plek (thuis, in een satellietkantoor of in een andere locatie) geen informatie wordt opgeslagen op externe toestellen zonder versleuteling en dat mogelijke bedreigingen vanaf de telewerk-plek niet in de IT-infrastructuur terechtkomen?	JA	
10	Sensibiliseert u jaarlijks iedere medewerker met betrekking tot de informatieveiligheid en gegevensbescherming en voert u jaarlijks een evaluatie uit rond de naleving van dit beleid in de praktijk?	JA	
11	Heeft u de toegang beveiligd door een duidelijke toegangsprocedure en heeft u een (logisch of fysiek) toegangssysteem geïmplementeerd om elke ongeoorloofde toegang te voorkomen?	JA	
12	Beschikt u over een classificatieschema voor persoonsgegevens waarvoor u de diensten levert en past u dit classificatieschema toe?	NEEN	De types van data die worden verwerkt door Byteflies systemen zijn opgelijst, maar geen specifieke classificatie is toegekend. In plaats daarvan is de toegang en beveiligingsniveau afgesteld per applicatie en rol van de gebruiker.
13	Heeft u de regels verwerkt in een beleid voor informatieveiligheid die gespecifieerd zijn in een beleidslijn ‘Email, online communicatie en internet gebruik’?	JA	
14	Heeft u minstens één toegangsbeheerder aangesteld wanneer u gebruik maakt van toegang op afstand tot de zorginstelling?	JA	
15	Heeft u uw medewerkers aangezet tot het lezen en toepassen van extra veiligheidsmaatregelen die de zorgvoorziening oplegt (indien van toepassing)?	JA	
16	Wanneer u ‘cryptografie’ wilt toepassen:		
	beschikt u over een formeel beleid voor het gebruik van cryptografische controles ?	JA	
	beschikt u over een formeel beleid voor het gebruik, bescherming en levensduur van de cryptografische sleutels voor de ganse levenscyclus?	JA	
17	Neemt u de nodige maatregelen om de toegang tot de gebouwen en lokalen te beperken tot de geautoriseerde personen en verricht u een controle erop zowel tijdens als buiten de werkuren?	JA	
18	Neemt u de nodige maatregelingen ter voorkoming van verlies, schade, diefstal of compromitteren van middelen en onderbreking van de activiteiten?	JA	

	Vraag	JA of NEEN	Leg uit bij een ´neen` antwoord
19	Bij hergebruik van de informatiedrager gebruikt u deze opnieuw in een minstens vergelijkbaar dataclassificatieniveau?	JA	
20	Legt u de gepaste maatregelen voor het wissen van gegevens contractueel vast met de opdrachtgever?	JA	
21	Past u de regels toe in verband met de logging van de toegang zoals vastgelegd door de opdrachtgever?	JA	
22	Zijn regels vastgelegd voor het verwerven, ontwikkelen en onderhouden van systemen tussen de verschillende betrokken partijen?	JA	
23	Werken alle medewerkers met de ICT middelen in het kader van de opdracht op basis van minimale autorisatie voor de uitvoering van hun taak?	JA	
24	Worden de vereisten voor toegangsbeveiliging (identificatie, authenticatie, autorisatie) gedefinieerd, gedocumenteerd, gevalideerd en gecommuniceerd? Worden deze toegangen gelogd?	JA	
25	Worden de veiligheids- en gegevensbeschermingsrisico's contractueel vastgelegd tussen u en eventuele onderaannemers?	JA	
26	Gebruikt u een controlelijst zodat de projectleider er zich kan van vergewissen dat het geheel van de beleidslijnen informatieveiligheid en gegevensbescherming correct geëvalueerd en indien noodzakelijk geïmplementeerd worden tijdens de ontwikkelingsfase van het project?	JA	
27	Voert u bij elke in productiestelling van een project een controle uit of de veiligheids- en gegevensbeschermingsvereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden?	JA	
28	Worden, onder de supervisie van de projectleider, de voorzieningen voor ontwikkeling, test en/of acceptatie en productie gescheiden – inclusief de bijhorende scheiding der verantwoordelijkheden in het kader van het project?	JA	
29	Wordt elke toegang tot persoonlijke en vertrouwelijke gegevens gelogd in overeenstemming met een policy "logging" en de toepasselijke wetgeving en regelgeving?	JA	
30	Wordt in de specificaties van een project opgenomen hoe de toegang tot en het gebruik van systemen en applicaties gelogd zal worden om bij te dragen tot de detectie van afwijkingen inzake informatieveiligheid en gegevensbescherming?	JA	
31	Beantwoordt het logbeheer minimaal aan de volgende doelstellingen? • De informatie om te kunnen bepalen wie, wanneer en op welke manier toegang heeft verkregen tot welke informatie • De identificatie van de aard van de geraadpleegde informatie • De duidelijke identificatie van de persoon	JA	

Vraag		JA of NEEN	Leg uit bij een ´neen` antwoord
32	Zijn de noodzakelijke tools ter beschikking om toe te laten de log gegevens uit te baten door de geautoriseerde personen?	JA	
33	Worden de transactionele/functionele log gegevens overeenkomstig de bewaard overeenkomstig de gegevens zelf (vb 30 jaar voor medische gegevens)?	JA	
34	Worden de deliverables (gegevens die verwerkt worden, de documentatie (broncode, programma's, technische documenten, ...)) van het project geïntegreerd in het back-up beheersysteem?	JA	
35	Worden, in de loop van de ontwikkeling van het project, de behoeften met betrekking tot continuïteit van de dienstverlening geformaliseerd, conform met uw verwachtingen?	JA	
36	Wordt uw continuïteitsplan en de bijhorende procedures geactualiseerd in functie van de projectevolutie, met inbegrip van continuïteitstesten?	JA	
37	Wordt er een risico analyse in het begin van het project uitgevoerd om de noodprocedures te definiëren?	JA	
38	Worden, in de loop van de ontwikkeling van het project, de procedures met betrekking tot het incidentbeheer geformaliseerd en gevalideerd?	JA	
39	Wordt de CISO op de hoogte gesteld van de veiligheidsincidenten en de DPO voor incidenten inzake gegevensbescherming?	JA	
40	Wordt tijdens de levensloop van het project de documentatie (technisch, procedures, handleidingen, ...) actueel gehouden?	JA	
41	Worden alle middelen inclusief aangekochte of ontwikkelde systemen toegevoegd aan de inventaris van de operationele middelen?	JA	
42	Wordt de gepaste medewerking verleend aan audits uitgevoerd onder de vorm van het ter beschikking stellen van personeel, documentatie, logbeheer en andere informatie die redelijkerwijze beschikbaar is?	JA	
43	Worden vereisten rond informatieveiligheid en gegevensbescherming gedocumenteerd om risico's te reduceren mbt toegang informatiemiddelen?	JA	
44	Worden alle relevante vereisten rond informatieveiligheid en privacy opgesteld en overeengekomen tussen u en derde partijen/toeleveranciers (die informatie van de organisatie lezen, verwerken, stockeren, communiceren of ICT infrastructuurcomponenten en ICT diensten aanleveren)?	JA	
45	Wordt regelmatig de dienstverlening aan u door derde partijen / toeleveranciers gemonitord, geëvalueerd en geauditeerd ?	JA	
46	Worden de wijzigingen in de dienstverlening aan u door de derde partij / toeleverancier beheerd, waaronder het bijhouden van bestaande beleidslijnen, procedures/maatregelen voor informatieveiligheid en gegevensbescherming ?	JA	

	Vraag	JA of NEEN	Leg uit bij een ´neen` antwoord
47	Beschikt u over een beleidslijn ‘Cloud computing’ wanneer u een beroep doet op clouddiensten?	JA	
48	Wanneer u professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een cloud voldoet u aan de minimale contractuele waarborgen?	JA	
49	Heeft u procedures voor het vastleggen en beheren van incidenten over informatieveiligheid of gegevensbescherming met de bijhorende verantwoordelijkheden en heeft u deze procedures intern bekend gemaakt?	JA	
50	Heeft u een overeenkomst met alle medewerkers dat elke medewerker (zowel vast of tijdelijk, intern of extern) verplicht is melding te maken van ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen?	JA	
51	Worden de gebeurtenissen en zwakheden over informatieveiligheid of gegevensbescherming die verband houden met informatie en informatiesystemen zodanig kenbaar gemaakt aan de opdrachtgever zodat u en de opdrachtgever tijdig en adequaat corrigerende maatregelen kunnen nemen?	JA	
52	Beschikt BYTEFLIES over een procedure om zo snel als mogelijk intern incidenten inzake informatieveiligheid/gegevensbescherming te communiceren/rapporteren?	JA	
53	Worden bij incidenten over informatieveiligheid of gegevensbescherming het bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften correct verzameld?	JA	
54	Wordt elk incident over informatieveiligheid of gegevensbescherming formeel gevalideerd opdat procedures en controlemaatregelen verbeterd kunnen worden en worden de lessen die getrokken worden uit een incident gecommuniceerd naar uw directie voor validatie en goedkeuring van verdere acties?	JA	
55	Heeft u een continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen?	JA	
56	Is informatieveiligheid en gegevensbescherming een integraal onderdeel van uw continuïteitsbeheer?	JA	
57	Heeft u een eigen continuïteitsplan? Wordt dit plan regelmatig getest en aangepast met de nodige communicatie naar uw directie voor validatie en goedkeuring?	JA	
58	Voert u periodiek een conformiteitsaudit uit met betrekking tot de situatie rond informatieveiligheid en gegevensbescherming?	JA	
59	Heeft u een formeel disciplinair proces voor werknemers die inbreuk op de informatieveiligheid of gegevensbescherming hebben gepleegd?	JA	

	Vraag	JA of NEEN	Leg uit bij een ´neen` antwoord
60	Brengt u regelmatig alle informatie samen om de risico's in kaart te brengen in verband met de conformiteit met GDPR en voert u de nodige acties uit als gevolg van een hoog "residueel" risico op non-conformiteit?	JA	
61	Heeft u een up-to-date centrale register van de verwerkingsverantwoordelijke of van de verwerker en heeft u een formele verantwoording voor het niet realiseren van controlemaatregelen gericht op de naleving van de Europese verordening voor de specifieke verwerking?	JA	