

Vragenlijst voor een derde partij die informatie van de openbare instelling sociale zekerheid leest, verwerkt, bewaart, communiceert of ICT infrastructuurcomponenten & diensten aanlevert

Naam van de organisatie (derde partij)	Benaming: Adres: Ondernemingsnummer (KBO): <table border="1" data-bbox="1265 627 1765 683"> <tr> <td>0</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	0									
0											
Voornaam, Naam & email adres van de veiligheidsconsulent (CISO) (verplicht)										
Voornaam, Naam & email adres van de adjunct veiligheidsconsulent (adjunct CISO) (optioneel)										
Voornaam, Naam & email adres van de functionaris voor gegevensbescherming (DPO) (verplicht)										
Voornaam, Naam & email adres van de adjunct functionaris voor gegevensbescherming (adjunct DPO) (verplicht)										
Voornaam, Naam & email adres van de persoon belast met het dagelijks bestuur (verplicht)										

VRAGENLIJST VOOR DERDE PARTIJ v2017

Vraag	<i>Kruis (X) het vak aan dat overeenstemt met uw antwoord</i>	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? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
2	Heeft u een risicobeoordeling voor elk proces en bij elk project rond informatieveiligheid en privacy die u gebruikt voor de dienstverlening? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
3	Binnen uw organisatie: <ul style="list-style-type: none"> • is er een veiligheidsdienst onder leiding van een veiligheidsconsulent? • 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? <input type="checkbox"/> JA <input type="checkbox"/> NEEN <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
4	Beschikt u over een informatieveiligheidsplan goedgekeurd door de verantwoordelijke voor het dagelijks bestuur? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
5	Hoeveel uren werden gepresteerd door de veiligheidsconsulent en diens adjunct(en) voor de uitvoering van de veiligheidstaken? 1) veiligheidsconsulent 2) adjunct-veiligheidsconsulent(en) Hoeveel uren opleidingen rond informatieveiligheid hebben de veiligheidsconsulent diens adjunct(en) gevolgd in het jaar? 1) veiligheidsconsulent 2) adjunct-veiligheidsconsulent(en)	1) uren / maand 2) uren / maand 3) uren / jaar 4) uren / 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? <input type="checkbox"/> JA <input type="checkbox"/> NEEN <input type="checkbox"/> N/A	
7	Neemt u de gepaste maatregelen opdat de professionele, vertrouwelijke en gevoelige gegevens opgeslagen op mobiele media enkel toegankelijk zijn voor geautoriseerde personen? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
8	Treff 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? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	

VRAGENLIJST VOOR DERDE PARTIJ v2017

Vraag	<i>Kruis (X) het vak aan dat overeenstemt met uw antwoord</i>	Leg uit bij een 'neen' antwoord
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? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
10	Sensibiliseert u jaarlijks iedere medewerker met betrekking tot de informatieveiligheid en privacy en voert u jaarlijks een evaluatie uit rond de naleving van dit beleid in de praktijk? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
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 ? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
12	Beschikt u over het intern classificatieschema waarvoor u de diensten levert en past u bijkomende regels in functie van het classificatieschema toe. <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
13	Heeft u de regels verwerkt in een beleid voor informatieveiligheid die gespecificeerd zijn in een beleidslijn 'Email, online communicatie en internet gebruik'? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
14	Heeft u minstens één toegangsbeheerder aangesteld wanneer u gebruik maakt van de diensten en toepassingen van het portaal van de sociale zekerheid ten behoeve van uw gebruikers ? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
15	Heeft u uw medewerkers aangezet tot het lezen en toepassen van de reglementen over het gebruik van de informatiesystemen van de portalen? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
16	Wanneer u 'cryptografie' wilt toepassen : <ul style="list-style-type: none"> • beschikt u over een formeel beleid voor het gebruik van cryptografische controles ? • beschikt u over een formeel beleid voor het gebruik, bescherming en levensduur van de cryptografische sleutels voor de ganse levenscyclus? <input type="checkbox"/> JA <input type="checkbox"/> NEEN <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
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? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
18	Neemt u de nodige maatregelen ter voorkoming van verlies, schade, diefstal of compromitteren van middelen en onderbreking van de activiteiten? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
19	Bij hergebruik van de informatiedrager gebruikt u deze opnieuw in een minstens vergelijkbaar data classificatieniveau? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	

VRAGENLIJST VOOR DERDE PARTIJ v2017

Vraag	<i>Kruis (X) het vak aan dat overeenstemt met uw antwoord</i>	Leg uit bij een 'neen' antwoord
20	Legt u de gepaste maatregelen voor het wissen van gegevens contractueel vast met de opdrachtgever ? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
21	Past u de regels in verband met de logging van de toegang zoals vastgelegd door de opdrachtgever. <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
22	Is er een constructieve communicatie opgezet bij elke project voor het verwerven, ontwikkelen en onderhouden van systemen tussen de verschillende betrokken partijen en de veiligheidsconsulent(en) ? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
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 ? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
24	Worden de vereisten voor toegangsbeveiliging (identificatie, authenticatie, autorisatie) gedefinieerd, gedocumenteerd, gevalideerd en gecommuniceerd? Worden deze toegangen gelogd? <input type="checkbox"/> JA <input type="checkbox"/> NEEN <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
25	Wordt de veiligheids- en privacy-risico's contractueel vastgelegd tussen u en de opdrachtgever met vertrouwelijkheids- en continuïteitsclausules? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
26	Gebruikt u een controlelijst zodat de projectleider er zich kan van vergewissen dat het geheel van de beleidslijnen informatieveiligheid en privacy correct geëvalueerd en indien noodzakelijk geïmplementeerd worden tijdens de ontwikkelingsfase van het project? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
27	Voert u bij elke in productiestelling van een project een controle uit of de veiligheids- en privacy-vereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
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? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
29	Worden elke toegang tot persoonlijke en vertrouwelijke gegevens die sociaal of medisch van aard zijn, gelogd in overeenstemming met de beleidslijnen "logging" en de toepasselijke wetgeving en regelgeving? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
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 van de beleidslijnen informatieveiligheid en privacy? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	

VRAGENLIJST VOOR DERDE PARTIJ v2017

Vraag	<i>Kruis (X) het vak aan dat overeenstemt met uw antwoord</i>	Leg uit bij een 'neen' antwoord
31	Beantwoordt het logbeheer minimaal aan de volgende doelstellingen? <ul style="list-style-type: none"> • 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 	
32	Zijn de noodzakelijke tools ter beschikking om toe te laten de log gegevens uit te baten door de geautoriseerde personen?	
33	Worden de transactionele/functionele log gegevens minimaal 10 jaar en de technische/infrastructurale log gegevens minimaal 2 jaar bewaard?	
34	Worden de deliverables (gegevens die verwerkt worden, de documentatie (broncode, programma's, technische documenten, ...)) van het project geïntegreerd in het backup beheersysteem zoals opgelegd in de beleidslijnen?	
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?	
36	Wordt uw continuïteitsplan en de bijhorende procedures geactualiseerd in functie van de projectevolutie, met inbegrip van continuïteitstesten ?	
37	Wordt er een risico analyse in het begin van het project uitgevoerd om de noodprocedures te definiëren?.	
38	Worden, in de loop van de ontwikkeling van het project, de procedures met betrekking tot het incidentbeheer geformaliseerd en gevalideerd ?	
39	Wordt de veiligheidsconsulent op de hoogte gesteld van de veiligheids- en privacy-incidenten?	
40	Wordt tijdens de levensloop van het project de documentatie (technisch, procedures, handleidingen, ...) actueel gehouden?	
41	Worden alle middelen inclusief aangekochte of ontwikkelde systemen toegevoegd aan het beheerssysteem van de operationele middelen (inventaris) ?.	
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?	
43	Worden de vereisten rond informatieveiligheid en privacy gedocumenteerd om risico's te reduceren met betrekking tot toegang tot informatiemiddelen?	
45	Worden alle relevante vereisten rond informatieveiligheid en privacy opgesteld en overeengekomen tussen u en derde partijen / toeleveranciers (die informatie van	

VRAGENLIJST VOOR DERDE PARTIJ v2017

Vraag	<i>Kruis (X) het vak aan dat overeenstemt met uw antwoord</i>	Leg uit bij een 'neen' antwoord
	de organisatie lezen, verwerken, stockeren, communiceren of ICT infrastructuurcomponenten en ICT diensten aanleveren)?	
46	Wordt regelmatig de dienstverlening aan u door derde partijen / toeleverancier gemonitord, geëvalueerd en geauditeerd ?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
47	Worden de wijzigingen in de dienstverlening aan u door de derde partij / toeleverancier beheerd, waaronder het bijhouden van bestaande beleidslijnen, procedures en maatregelen voor informatieveiligheid en privacy ?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
48	Bent u conform met punt 2.1 van de beleidslijn 'Cloud computing' wanneer u een beroep doet op cloud-diensten ?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
49	Wanneer u professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een cloud voldoet u aan de minimale contractuele waarborgen en de beleidslijnen zoals beschreven in punt 2.2, 2.3 en 2.4 van de beleidslijn 'Cloud computing' ?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
50	Heeft u procedures voor het vastleggen en beheren van incidenten over informatieveiligheid of privacy met de bijhorende verantwoordelijkheden en heeft u deze procedures bekend gemaakt aan uw medewerkers ?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
51	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 ?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
52	Worden de gebeurtenissen en zwakheden over informatieveiligheid of privacy die verband houden met informatie en informatiesystemen zodanig kenbaar gemaakt aan de opdrachtgever zodat u en de opdrachtgever tijdig en adequaat corrigerende maatregelen kan nemen?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
53	Worden de incidenten over informatieveiligheid en privacy zo snel als mogelijk via de leidinggevende, de helpdesk, de informatieveiligheidsconsulent (CISO) of functionaris van gegevensbescherming (DPO) gerapporteerd?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
54	Worden bij incidenten over informatieveiligheid of privacy het bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften correct verzameld?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN
55	Wordt elk incident over informatieveiligheid of privacy 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?	<input type="checkbox"/> JA <input type="checkbox"/> NEEN

VRAGENLIJST VOOR DERDE PARTIJ v2017

Vraag	<i>Kruis (X) het vak aan dat overeenstemt met uw antwoord</i>	Leg uit bij een 'neen' antwoord
56	Heeft u een continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
57	Is informatieveiligheid en privacy een integraal onderdeel van uw continuïteitsbeheer? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
58	Heeft u een eigen continuïteitsplan met de minimale informatie zoals beschreven in de beleidslijn 'Continuïteitsbeheer'? Wordt dit plan regelmatig getest en aangepast met de nodige communicatie naar uw directie voor validatie en goedkeuring ? <input type="checkbox"/> JA <input type="checkbox"/> NEEN <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
59	Voert u periodiek een conformiteitsaudit uit met betrekking tot de situatie rond informatieveiligheid en privacy zoals beschreven in de beleidslijnen? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
60	Heeft u een formeel disciplinair proces voor werknemers die inbreuk op de informatieveiligheid of privacy hebben gepleegd? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
61	Brengt u regelmatig alle informatie samen om de risico's in kaart te brengen in verband met de conformiteit met de Europese verordening en voert u de nodige acties uit als gevolg van een hoog "residueel" risico op non-conformiteit ? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	
62	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? <input type="checkbox"/> JA <input type="checkbox"/> NEEN	

VRAGENLIJST VOOR DERDE PARTIJ v2017

Gelieve de ingevulde vragenlijst terug te sturen naar de dienst Informatieveiligheid en Interne Audit van de Kruispuntbank van de Sociale Zekerheid.

<p>Datum en handtekening van de veiligheidsconsulent (CISO) of functionaris voor gegevensbeheer (DPO) van de organisatie (derde partij) (optioneel)</p>	<p>.....</p> <p>Datum Handtekening</p>
<p>Datum en handtekening van de persoon belast met het dagelijks bestuur van de organisatie (derde partij) (verplicht)</p>	<p>.....</p> <p>Datum Handtekening</p>

***** EINDE VAN DIT DOCUMENT *****