**Conformiteitsverklaring inzake het informatieveiligheidssysteem dat het voorwerp uitmaakt van een aanvraag tot beraadslaging bij het Informatieveiligheidscomité**

|  |
| --- |
| ***Aanvragende instelling die verantwoordelijk is voor de verwerking*** |
| Naam |  |
| Officiële afkorting |  |
| Officieel adres |  |
| Ordernemingsnummer (KBO) |  |
| Nummer van de vestigingseenheid (KBO) |  |

|  |
| --- |
|  |

|  |
| --- |
| ***Verantwoordelijke voor het dagelijks beheer van de verwerking*** |
| ***Contactgegevens*** |
| Titel |  |
| Naam en voornaam |  |
| Contactadres |  |
| Telefoon |  |
| e-mail |  |
| Taal  |  |

|  |
| --- |
| Ondergetekende, **verantwoordelijke voor het dagelijks beheer van de verwerking** van persoonsgegevens, die het voorwerp is van de aanvraag voor beraadslaging, hierna "de bedoelde verwerking", **verklaart dat**, overeenkomstig de verplichtingen bepaald in de Algemene Verordening Gegevensbescherming, de Privacywet en andere geldende wetten, de passende technische en organisatorische maatregelen werden genomen voor een toereikende bescherming van de verwerkte persoonsgegevens. Deze maatregelen zullen operationeel zijn ten laatste op de dag dat deze verwerking wordt verricht.Daarbij werd rekening gehouden met : * de aard van de verwerkte persoonsgegevens en de verwerkingen ervan evenals de vereisten inzake vertrouwelijkheid, integriteit en beschikbaarheid;
* de wettelijke of reglementaire verplichtingen die van toepassing zouden zijn;
* de grootte van de instelling (daarbij inbegrepen aantal en profiel van de personen die toegang tot de gegevens kunnen hebben);
* het belang en de complexiteit van de betrokken informatiesystemen, toepassingsprogramma’s en informaticasystemen;
* de mate waarin de instelling openstaat voor de buitenwereld evenals de mate waarin er toegang is vanuit de buitenwereld;
* de risico’s waaraan de instelling zelf of de personen van wie de persoonsgegevens worden verwerkt, blootgesteld worden;
* alsook de stand van de techniek ter zake en de kosten voor het toepassen van de maatregelen,
 |
| **verklaart dat** ten laatste op de dag dat deze verwerking wordt verricht aan de hiernavolgende beveiligingsaspecten is voldaan (aanvinken): 1. een functionaris voor gegevensbescherming (DPO) en/of informatieveiligheidsconsulent werd aangesteld JA NEE 

|  |
| --- |
| **Contactgegevens van de functionaris voor gegevensbescherming (DPO)** |
| Naam |  |
| Voornaam |  |
| Contactadres |  |
| Telefoon |  |
| e-mailadres |  |

 |
|

|  |
| --- |
| **Contactgegevens van de informatieveiligheidsconsulent** |
| Naam |  |
| Voornaam |  |
| Contactadres |  |
| Telefoon |  |
| e-mailadres |  |

 |
| 2. Evaluatie van de risico’s JA  NEE  De risico’s die de verwerkte persoonsgegevens lopen, werden geëvalueerd en de daarmee verbonden beveiligingsbehoeften werden vastgesteld. 3. Een informatiebeveiligingsbeleid JA  NEE  Er werd een geschreven document – het beveiligingsbeleid – opgesteld waarin de strategieën en de weerhouden maatregelen voor gegevensbeveiliging worden omschreven. 4. Identificatie van de dragers JA  NEE  Alle mogelijke dragers die de verwerkte persoonsgegevens bevatten, werden geïdentificeerd. 5. Informatieverstrekking aan het personeel JA  NEE  De interne en externe personeelsleden die bij de verwerking van persoonsgegevens betrokken zijn, werden ten aanzien van de verwerkte gegevens ingelicht over de vertrouwelijkheids- en beveiligingsverplichtingen die zowel voortvloeien uit de verschillende wettelijke vereisten als uit het beveiligingsbeleid. 6. Fysieke beveiliging van de toegang JA  NEE  Er werden passende beveiligingsmaatregelen genomen om een niet-gemachtigde of onnodige fysieke toegang te verhinderen tot de dragers die verwerkte persoonsgegevens bevatten. 7. Fysieke beveiliging van de omgeving JA  NEE  De noodzakelijke maatregelen werden genomen om elke fysieke schade die de verwerkte persoonsgegevens in gevaar zouden kunnen brengen, te verhinderen. 8. Netwerkbeveiliging JA  NEE  De verschillende netwerken gekoppeld aan de apparatuur die de persoonsgegevens verwerkt, zijn beschermd. 9. Lijst met gemachtigde personen JA  NEE   |
| Er werd een actuele lijst opgemaakt van de verschillende bevoegde personen die in het kader van de verwerking toegang hebben tot de persoonsgegevens alsook van hun respectieve toegangsniveau (creatie, raadpleging, wijziging, vernietiging). 10. Logische beveiliging van de toegang JA  NEE  Er werd een mechanisme voor toegangsmachtiging ontworpen zodat de verwerkte persoonsgegevens en de verwerkingen die betrekking hebben op deze gegevens uitsluitend toegankelijk zijn voor personen en toepassingen die daartoe uitdrukkelijk gemachtigd zijn. 11. Logging van toegang JA  NEE  Er werd een informatiesysteem ontworpen dat permanente logging, opsporing en analyse mogelijk maakt van de toegang die personen en logische entiteiten gehad hebben tot de verwerkte persoonsgegevens. Indien nodig werd voldoende aandacht besteed aan de volgende beveiligingsaspecten. 12. Toezicht, aanpassing en onderhoud JA  NEE  Er werd voorzien in toezicht op de geldigheid en doeltreffendheid in de tijd van de ingestelde technische of organisatorische maatregelen. 13. Urgentiebeheer van informatiebeveiligingsincidenten JA  NEE  Er werden urgentieprocedures opgesteld voor beveiligingsincidenten waarbij persoonsgegevens betrokken zijn. 14. Documentatie JA  NEE  Er werd voldoende documentatie samengesteld over de organisatie van de informatiebeveiliging voor de bedoelde verwerking en deze documentatie wordt up-to-date gehouden. **Ik verklaar op eer dat de bovenstaande inlichtingen naar waarheid werden verstrekt[[1]](#footnote-1).** Datum: Handtekening: |
|  |
|  |
|  |
|  |

1. Elke verklaring die niet met de waarheid overeenstemt, kan als valsheid in geschrifte worden beschouwd en stelt de verantwoordelijke voor de verwerking strafrechtelijk aansprakelijk. De documenten worden ter beschikking gehouden van het Informatieveiligheidscomité dat om een kopie kan verzoeken. [↑](#footnote-ref-1)