

**Verklaring i.v.m. de technische en organisatorische maatregelen i.k.v. de
aanvraag voor individuele gegevens van de VSA**

|  |
| --- |
| **Technische en organisatorische maatregelen** |
| 1. **Persoonsgegevens van de informatieveiligheidsadviseur, indien aangesteld**
 |
| * 1. Voornaam
 | Klik hier om tekst te typen. |
| * 1. Naam
 | Klik hier om tekst te typen. |
| * 1. Functie
 | Klik hier om tekst te typen. |
| * 1. Adres
 | Straat | Klik hier om tekst te typen. |
| Nummer | Klik hier om tekst te typen. |
| Bus | Klik hier om tekst te typen. |
| Postcode | Klik hier om tekst te typen. |
| Gemeente | Klik hier om tekst te typen. |
| Land | Klik hier om tekst te typen. |
| * 1. E-mailadres
 | Klik hier om tekst te typen. |
| * 1. Telefoonnummer
 | Klik hier om tekst te typen. |
| * 1. Medewerker buiten de instelling
 | [ ]  Ja[ ]  Neen |
| 1. **Meldingsplicht voor inbreuken in verband met persoonsgegevens**

***Overeenkomstig artikel 33 van de algemene verordening gegevensbescherming (AVG) dient de verwerkingsverantwoordelijke indien een inbreuk i.v.m. persoonsgegevens heeft plaatsgevonden, dat zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen aan de bevoegde toezichthoudende autoriteit te melden, tenzij het niet waarschijnlijk is dat de inbreuk i.v.m. persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Afhankelijk van uw instelling is die bevoegde toezichthoudende autoriteit de Vlaamse Toezichtcommissie (VTC) of de Gegevensbeschermingsautoriteit (GBA). Bovendien moet overeenkomstig artikel 34 AVG die inbreuk ook worden gemeld aan de betrokken personen als de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van die personen.******Daarnaast, overeenkomstig onderhavige verbintenis en het protocol voor de elektronische mededeling van individuele gegevens van de VSA, gesloten ter vastlegging van de modaliteiten van gegevensmededeling, verbindt de instelling die de aanvraag doet er zich ook toe elke inbreuk i.v.m. persoonsgegevens die en elk beveiligingsincident of -lek (wat een inbreuk op de beveiliging is die geen betrekking heeft op persoonsgegevens) dat betrekking heeft op individuele gegevens medegedeeld door de VSA, zonder onredelijke vertraging te melden via*** ***dpo.sv@vlaanderen.be*** ***en dit ten laatste binnen 24 uur na de melding van de instelling aan diens bevoegde toezichthoudende autoriteit.******Een inbreuk i.v.m. persoonsgegevens of een beveiligingsincident/-lek kan verschillende vormen aannemen en onder meer bestaan in diefstal van die gegevens voor ongeoorloofd gebruik, van doorsturing naar daarvoor niet-bevoegde instellingen of voor elk ander gebruik dat niet strookt met onderhavige verbintenis en het protocol* *voor de elektronische mededeling van individuele gegevens van de VSA, gesloten ter vastlegging van de modaliteiten van gegevensmededeling. Voorts kan het gaan om een handeling of verzuim met als gevolg beschadiging of foutief geraken van die gegevens, of verder nog om een informatica-aanval waarbij met het oog op latere afpersing de informatie onbruikbaar wordt gemaakt.*** |
| Gelieve uitvoerig de procedures uiteen te zetten die zijn ingevoerd om ervoor te zorgen dat de meldingsplicht voor inbreuken in verband met van persoonsgegevens wordt nageleefd.Klik hier om tekst in te typen. |
| 1. **Oefent uw instelling ook een controle of repressiefunctie uit?**

**☐ Ja. Gelieve onderstaand kader in te vullen.****☐ Neen** |
| Maatregelen om de vertrouwelijkheid van de meegedeelde individuele gegevens te garanderen (interne organisatie, functiescheiding) | Klik hier om tekst in te typen. |
| 1. **Welke technische en organisatorische maatregelen worden genomen om de individuele gegevens te beschermen?**
 |
| Gelieve hier uitvoerig de technische en organisatorische maatregelen uiteen te zetten die de individuele gegevens maximaal dienen te beschermen om zo te vermijden dat: 1) de individuele gegevens toegankelijk zijn voor personen die niet betrokken zijn bij deze verwerking, 2) de individuele gegevens gebruikt zouden worden voor een andere finaliteit en 3) er een identificatie zou kunnen plaatsvinden van de betrokken personen / ondernemingen. Klik hier om tekst in te typen. |
| 1. **Verklaring dat ten laatste op de datum van uitvoering van de gegevensverwerking de volgende informatieveiligheidsaspecten de nodige aandacht zullen hebben gekregen:**
 |
| 1. Voor de verwerkte individuele gegevens is een risico-evaluatie doorgevoerd en de informatieveiligheidsbehoeften zijn daarbij opgespoord en vastgelegd.
 | [ ]  Ja[ ]  Neen |
| 1. Er is een schriftelijk document uitgewerkt – het beleid inzake informatieveiligheid – waarin de strategieën en maatregelen bedoeld om de verwerkte individuele gegevens te beveiligen omschreven worden.
 | [ ]  Ja[ ]  Neen |
| 1. Er is een lijst opgemaakt van alle informatiedragers, van welke aard ook, die met de verwerkte individuele gegevens in betrekking staan.
 | [ ]  Ja[ ]  Neen |
| 1. De bij de gegevensverwerking betrokken interne en externe personeelsleden werden voorgelicht omtrent hun vertrouwelijkheids- en informatieveiligheidsplichten t.a.v. de verwerkte individuele gegevens, zoals die voortvloeien uit zowel de verschillende wettelijke vereisten als uit het gevoerde beleid inzake informatieveiligheid.
 | [ ]  Ja[ ]  Neen |
| 1. Er zijn gepaste informatieveiligheidsmaatregelen getroffen om onnodige of onbevoegde fysieke toegang tot de dragers waarop de verwerkte individuele gegevens staan opgeslagen te beletten.
 | [ ]  Ja[ ]  Neen |
| 1. Er zijn gepaste informatieveiligheidsmaatregelen getroffen om fysieke schade die de verwerkte individuele gegevens in gevaar zou kunnen brengen te beletten.
 | [ ]  Ja[ ]  Neen |
| 1. Er is adequate bescherming voor de verschillende netwerken waaraan de gegevensverwerkende apparatuur gekoppeld is.
 | [ ]  Ja[ ]  Neen |
| 1. Er is een lijst opgemaakt van de verschillende personen die in het kader van de bedoelde gegevensverwerking toegangsbevoegdheid hebben tot de individuele gegevens, met opgave van hun graad van toegangsbevoegdheid (aanmaak, inzage, bewerking, wissen), en die lijst wordt regelmatig bijgewerkt.
 | [ ]  Ja[ ]  Neen |
| 1. Er is een toelatingsmechanisme voor gegevenstoegang ingebouwd waardoor de verwerkte individuele gegevens en de verwerkingen verricht op die gegevens slechts toegankelijk zijn voor daartoe uitdrukkelijk bevoegd verklaarde personen en applicaties.
 | [ ]  Ja[ ]  Neen |
| 1. Het informatiesysteem is zo opgebouwd dat de toegang van personen en logische eenheden tot individuele gegevens onafgebroken kan worden geregistreerd, getraceerd en geanalyseerd.
 | [ ]  Ja[ ]  Neen |
| 1. Er is voorzien in een controlesysteem op geldigheid en onverminderde doeltreffendheid van de ingevoerde technische of organisatorische maatregelen.
 | [ ]  Ja[ ]  Neen |
| 1. Er zijn procedures uitgewerkt voor urgentiebeheer van informatieveiligheidsincidenten waarbij verwerkte individuele gegevens betrokken zijn.
 | [ ]  Ja[ ]  Neen |
| 1. In het kader van de bedoelde gegevensverwerking is over informatieveiligheid en de organisatie ervan toereikend documentatiemateriaal opgesteld, dat regelmatig zal worden bijgewerkt.
 | [ ]  Ja[ ]  Neen |
| 1. **Handtekening van de informatieveiligheidsadviseur, de verwerkingsverantwoordelijke of de wettelijke vertegenwoordiger van de instelling**
 |
| [ ]  Ik verklaar op erewoord dat de hierboven verstrekte informatie oprecht, volledig en juist is.[ ]  Ik ga ermee akkoord dat de VSA de vermelde gegevens mag gebruiken om mijn verklaring i.v.m. de technische en organisatorische maatregelen te verwerken en ik verklaar dat ik de uitdrukkelijke toestemming heb verkregen van de daarin vermelde informatieveiligheidsadviseur, indien aangesteld, voor het gebruik van zijn/haar persoonsgegevens. |
| * 1. Datum
 | Klik hier om een datum in te voeren. |
| * 1. Voornaam
 | Klik hier om tekst te typen. |
| * 1. Naam
 | Klik hier om tekst te typen. |
| * 1. Functie
 | Klik hier om tekst te typen. |
| HandtekeningBij voorkeur een (met eID) gekwalificeerde elektronische handtekening |  |