## Leidraad

1. **Technische en organisatorische maatregelen**

|  |  |  |
| --- | --- | --- |
| **ALGEMEEN**  **BEVEILIGINGSBELEID EN**  **ORGANISATIE VAN**  **INFORMATIEBEVEILIGING** |  | **Verantwoordelijke voor informatie beveiliging:**  [Naam Verwerker] heeft informatieveiligheidsconsulent aangesteld die verantwoordelijk is voor de data beveiliging   * contactgegevens: … |
|  |  | **Verantwoordelijke voor gegevensbescherming:**  [Naam Verwerker] heeft een Data Protection Security Officer aangewezen die verantwoordelijk is voor het coördineren, opvolgen en controleren van de beveiligingsregels en -procedures.   * Contactgegevens: … |
|  |  | **Verantwoordelijkheden op vlak van informatiebeveiliging en gegevensbescherming:** De verantwoordelijkheden van de medewerkers van [Naam Verwerker] zijn formeel gedocumenteerd en gepubliceerd in een privacy- en security policy |
|  |  | **Risico analyse, beheer en controle**: [Naam Verwerker] voert periodiek risicoanalyses uit van de genomen beveiligingsmaatregelen en doet controles voor wat betreft de naleving van de verschillende informatiebeveiligingsprocedures |

|  |  |  |
| --- | --- | --- |
| **PERSONEEL** | | |
| **VEILIG PERSONEELSBELEID** |  | **Training over belang van beveiliging en omgang met persoonsgegevens:**  [Naam Verwerker] voorziet opleidingen om alle medewerkers te sensibiliseren voor wat betreft de beveiligingsrichtlijnen- en beveiligingsprocedures en hun rol daarbij. |
|  |  | **Toegangsautorisatie**:  [Naam Verwerker] implementeert en handhaaft een autorisatiebeheersysteem dat de toegang controleert tot systemen die persoonsgegevens bevatten. |
|  |  | **Segregatie:**  [Naam Verwerker] heeft een segregatie ingevoerd om te vermijden dat personen toegang krijgen tot gegevens waarvoor ze geen toegang nodig hebben voor de uitoefening van hun taak. |

|  |  |  |
| --- | --- | --- |
| **GEBOUW** | | |
| **FYSIEKE BEVEILIGING** |  | **Fysieke toegang tot productie- en bureauruimtes:**  [Naam Verwerker] beperkt de toegang tot haar ruimtes waar persoonsgegevens verwerkt worden in kader van haar opdracht, strikt tot geïdentificeerde en geautoriseerde personen.  Hiervoor werden badge-lezers geïnstalleerd, werd de lift uitgerust met codes en werden sloten voorzien op deuren waar nog nodig, dit alles om ongeoorloofde toegang te vermijden. |
|  |  | **Beveiliging van de omgeving:**  Naast badge-lezers is het volledige gebouw uitgerust met  - camerabewaking  - een alarm- en branddetectie systeem. |
| **BESCHERMING TEGEN**  **ONGEREGELDHEDEN,**  **PANNES EN INCIDENTEN** |  | **Firewall:**  [Naam Verwerker] is uitgerust met een geavanceerde firewall en controlemechanismen die zijn interne netwerk op gepaste wijze beschermt tegen ongeoorloofde toegang tot zijn interne netwerk. |

|  |  |  |
| --- | --- | --- |
| **DATA CENTER** |  |  |
| **FYSIEKE BEVEILIGING** |  | **Fysieke toegang tot het Data Center:**  [Naam Verwerker] centraliseerde alle data die nodig is in kader van haar opdracht in een beveiligd data center conform de industrienormen. Fysieke toegang tot het data center wordt gecontroleerd / beheerd. |
|  |  | **Noodherstel:**  [Naam Verwerker] beschikt over een noodherstelplan in  geval van calamiteiten met haar servers in het Data Center  waarop persoonsgegevens staan |
|  |  | **Redundantie**:  [Naam Verwerker] bewaart kopieën van persoonsgegevens alsook haar gegevensherstelprocedures welke opgeslagen staan in het primaire data center in een tweede data center. => Deze kopieën zijn extra versleuteld met specifieke encryptie sleutels die enkel nodig zijn indien het primaire data center zou falen. |

|  |  |  |
| --- | --- | --- |
| **DATA** |  |  |
| **DIGITALE GEGEVENS** |  | **Versleuteling van gegevens:**  alle digitale gegevens die verwerkt worden door [Naam Verwerker] in kader van haar opdracht worden centraal in het data center op een versleutelde manier bewaard op de harde schijven |
|  |  | **Anti-virus en beveiligingsupdates:**  [Naam Verwerker] voorziet al zijn systemen van de laatste updates. Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens haar patchmanagementproces |
|  |  | **Kwaadaardige Software**:  [Naam Verwerker] voert anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klantengegevens krijgt. |
|  |  | **Logging van toegangen**.  [Naam Verwerker] voorziet een continue logging op de server van alle toegangen tot haar systemen die persoonsgegevens bevatten met inbegrip van welke gebruiker, de tijd en activiteit. Alle logbestanden worden  gedurende 90 dagen bijgehouden. |

|  |  |  |
| --- | --- | --- |
| **COMMUNICATIE** |  |  |
| **BEVEILIGDE**  **VERBINDINGEN** |  | **Versleuteling van verbindingen:**  [Naam Verwerker] maakt gebruikt van beveiligde verbindingen voor de toegang tot haar gegevens in het datacenter. Alle data die verzonden wordt over publieke netwerken gebeurt dan ook aan de hand van encryptie mechanismen.   * https * VPN |
| **AUTHENTICATIE** |  | **Two-factor authenticatie:**  [Naam Verwerker] maakt gebruik van een combinatie van gebruikers/wachtwoord en een dynamisch token waarvan de geldigheid iedere 30 second vervalt. Wachtwoorden dienen steeds te bestaan uit minimaal acht tekens en zowel uit minimaal één hoofdletter, letter, cijfer. |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **INFORMATIESYSTEMEN** |  |  |
| **ONDERHOUD EN**  **EVOLUTIE VAN**  **INFORMATIESYSTEMEN** |  | **Controle over systeem updates en evoluties**:  [Naam Verwerker] heeft een formeel wijzigingsbeheerproces geïmplementeerd om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze. |
|  |  | **Beveiligingsvereisten**:  De vereisten voor de bescherming van gegevens en systemen worden geanalyseerd en gespecificeerd in samenwerking met onze IT leverancier(s). |
| **INCIDENTEN** |  | **Incident response:** [Naam Verwerker] houdt een register van beveiligingsinbreuken bij met een beschrijving van de inbreuk, het tijdstip, de gevolgen van de inbreuk, de naam van de melder en van degene aan wie de inbreuk werd gemeld. |
|  |  | **Notificatie van incidenten:**  In geval van eengegevensbeveiligingsincident dat impact heeft op de vertrouwelijkheid of integriteit van persoonsgegevens van klanten, zal [Naam Verwerker], zonder onredelijke vertraging, de verwerkingsverantoordeljke hiervan informeren. |

1. **Vertrouwelijksheidscontract**

Mevrouw / De heer ……………………………………………………………………...[naam en voornaam], ……………………………………………………………. [functie], hierna “de *Werknemer*” genoemd, heeft, in het raam van de missie die haar/hem door ………… [naam bedrijf, adres, bedrijfsnummer]werd toevertrouwd (hierna “de *Verwerker*” genoemd), toegang tot (bepaalde) persoonsgegevens (hierna “de *Gegevens*” genoemd).

De *Werknemer* verbindt er zich hiermee toe:

* + - zich alleen toegang te verschaffen tot de *Gegevens* die noodzakelijk zijn voor het uitvoeren van de haar/hem toevertrouwde opdracht in het kader van de verwerking van persoonsgegevens;
    - de *Gegevens* waarvan zij/hij kennis heeft genomen, alleen toe te vertrouwen aan anderen in de mate dat dit voor de uitvoering van haar/zijn opdracht in het kader van de verwerking van persoonsgegevens noodzakelijk is en op voorwaarde dat de persoon aan wie deze *Gegevens* kenbaar worden gemaakt gemachtigd is er kennis van te nemen;
    - de toegangscodes en/of wachtwoorden om zich toegang tot de *Gegevens* te verschaffen niet kenbaar te maken;
    - haar/zijn wachtwoord dat toegang biedt tot de *Gegevens* regelmatig te wijzigen.

De *Werknemer* erkent (\*schrappen wat niet past):

* + - van de *Verwerker* alle informatie te hebben gekregen voor het uitvoeren van de haar/hem toevertrouwde opdracht in het kader van de verwerking van persoonsgegevens;
    - zich ingeschreven te hebben en de bedoeling te hebben om de opleiding die door de *Verwerker* georganiseerd wordt van …………… [datum invoegen] te [Schrappen: volgen / hebben gevolgd] m.b.t. de verbintenissen die zij/hij moet nakomen in overeenstemming met de vigerende wetgeving en normering, zijnde:
  1. *VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn* 95/46/EG (“*algemene verordening gegevensbescherming”*);
  2. de *Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens* die door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer worden opgelegd;
  3. de *Minimale normen informatieveiligheid en privacy* voor sociale zekerheidsinstellingen die toegang willen bekomen en behouden tot het netwerk van de Kruispuntbank;
  4. de *Wet tot regeling van een Rijksregister van de natuurlijke personen* van 8 augustus 1983;
  5. de *Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* van 8 december 1992 (hierna *Privacywet* te noemen), zolang deze wet van kracht blijft.

Deze vertrouwelijkheidsplicht blijft ook na beëindiging van het contract tussen de *Verantwoordelijke voor de Verwerking* en de *Verwerker* voortbestaan, en ook na het verstrijken van het contract tussen de *Werknemer* en de *Verwerker*.

Opgemaakt te ………………………………………., op ……………………………………… in evenveel exemplaren als er Partijen zijn. Elke Partij verklaart haar exemplaar te hebben ontvangen.

*De Werknemer Voor de Verwerker*