Reglement tot vaststelling van de criteria voor de toepassing van een cirkel van vertrouwen bij de verwerking van persoonsgegevens in het kader van onderzoeken die nuttig zijn voor de kennis, de conceptie en het beheer van de sociale bescherming

DOEL VAN HET REGLEMENT

De verwerking van gepseudonimiseerde persoonsgegevens die (mede) afkomstig zijn uit het Datawarehouse Arbeidsmarkt en Sociale Bescherming moet steeds geschieden in overeenstemming met de regelgeving, inzonderheid de regelgeving inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer.

Dit reglement heeft tot doel om aan de instanties die dergelijke gespeudonimiseerde persoonsgegevens verwerken in het kader van onderzoeken die nuttig zijn voor de kennis, de conceptie en het beheer van de sociale bescherming een standaardkader te bieden waarbinnen dergelijke verwerking kan plaatsvinden overeenkomstig de geldende regelgeving, inzonderheid de Algemene Verordening Gegevensbescherming. De betrokken instanties kunnen verklaren te voldoen aan dit standaardkader. In dat geval wordt naar dit standaardkader en deze verklaring verwezen in de ontwerpberaadslaging die de Kruispuntbank van de Sociale Zekerheid voorlegt aan het Informatieveiligheidscomité, zodat de te nemen maatregelen niet telkens ad hoc moeten worden beschreven in de beraadslaging. Dit responsabiliseert de instanties die de vermelde gepseudonimiseerde persoonsgegevens verkrijgen en vereenvoudigt de behandeling van het dossier binnen het Informatieveiligheidscomité. De instantie die om de betrokken gegevens verzoekt, wordt uitgenodigd om bij elk verzoek wel nog zelf de maatregelen te beschrijven die waarborgen dat de opgevraagde gegevens anonieme of gepseudonimiseerde persoonsgegevens zijn in de zin van de Algemene Verordening Gegevensbescherming en het principe van gegevensminimalisatie is toegepast.

Belangrijk is het waarborgen dat de persoonsgegevens uitsluitend worden verwerkt voor rechtmatige doeleinden, door personen die daadwerkelijk gepseudonimiseerde persoonsgegevens van de betrokkenen nodig hebben voor het bereiken van die doeleinden. In een systeem van verwerking van persoonsgegevens door tal van actoren – in dit geval de organisaties die als authentieke bron persoonsgegevens ter beschikking stellen, de Kruispuntbank van de Sociale Zekerheid die ze opneemt in haar Datawarehouse Arbeidsmarkt en Sociale Bescherming en de organisaties die ze uiteindelijk gebruiken voor het realiseren van onderzoeken die nuttig zijn voor de kennis, de conceptie en het beheer van de sociale bescherming – vereist het bieden van een dergelijke waarborg een duidelijke vastlegging van de verantwoordelijkheden van elke actor.

Concreet wil dit reglement hiertoe bijdragen door het preciseren van het concept van “cirkel van vertrouwen”. Het betreft een groep gebruikers van een organisatie *(in casu de organisatie die de persoonsgegevens nodig heeft voor het realiseren van onderzoeken die nuttig zijn voor de kennis, de conceptie en het beheer van de sociale bescherming*), waarvoor die organisatie zelf op enkele vlakken informatieveiligheidsmaatregelen organiseert en waakt over de correcte naleving ervan, zodat een andere organisatie (*in casu de Kruispuntbank van de Sociale Zekerheid*) er redelijkerwijze op kan vertrouwen dat deze informatieveiligheidsmaatregelen worden nageleefd en ze die dus niet meer zelf moet organiseren of bewaken.

Opdat andere organisaties dan de organisatie die een cirkel van vertrouwen instelt daarin een rechtmatig vertrouwen zouden kunnen hebben, worden criteria vastgelegd waaraan moet worden voldaan door de organisatie die een cirkel van vertrouwen wil organiseren. Deze criteria

verwijzen maximaal naar bestaande Europese en Belgische regelgeving, zoals de 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* (de Algemene Verordening Gegevensbescherming). Zij doen geen afbreuk aan deze regelgeving, die ten volle blijft gelden, maar preciseren in een aantal gevallen de wijze waarop aan deze regelgeving moet worden voldaan. De criteria nemen de vorm aan van een reglement.

OVERZICHT VAN DE CRITERIA

1. Rechtmatigheid

De ontvangende organisatie baseert de rechtmatigheid van de verwerking van de persoonsgegevens uit het datawarehouse arbeidsmarkt en sociale bescherming op artikel 6, 1, eerste lid, c) of e), van de Algemene Verordening Gegevensbescherming (respectievelijk de noodzaak "*om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust*" en de noodzaak "*voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen*").

2. Doelbinding

Het datawarehouse arbeidsmarkt en sociale bescherming werd gecreëerd met toepassing van artikel 5 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, uitsluitend om de Kruispuntbank van de Sociale Zekerheid in staat te stellen om op een efficiënte wijze in te gaan op aanvragen tot verwerking van persoonsgegevens voor het verwezenlijken van onderzoeken die nuttig zijn voor de kennis, de conceptie en het beheer van de sociale bescherming. De ontvangende organisatie kan de persoonsgegevens uitsluitend in dat kader verwerken. Zij respecteert te allen tijde de bepalingen van de toepasselijke beraadslaging(en) van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, verleend met toepassing van artikel 15 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*.

3. Evenredigheid en verwerkingsbeperking

De persoonsgegevens uit het datawarehouse arbeidsmarkt en sociale bescherming kunnen enkel worden verwerkt door de gebruikers binnen de organisatie die ze omwille van hun specifieke functie moeten kunnen verwerken voor de rechtmatige verwerkingsdoeleinden. De organisatie bepaalt de verwerkingsmogelijkheden voldoende fijnmazig zodat elke gebruiker slechts de persoonsgegevens kan verwerken die hij effectief uit hoofde van zijn functie nodig heeft en dit slechts gedurende de periode waarvoor dit uit hoofde van zijn functie nodig is. De organisatie onthoudt zich van iedere poging tot het omzetten van de van de Kruispuntbank van de Sociale Zekerheid ontvangen gepseudonimiseerde persoonsgegevens in niet-gepseudonimiseerde persoonsgegevens.

Het is de organisatie niet toegestaan om de vanwege de Kruispuntbank van de Sociale Zekerheid ontvangen persoonsgegevens geheel of gedeeltelijk mee te delen aan derden of aan de opdrachtgever van het onderzoek. Zij mag de resultaten van haar onderzoek enkel in louter anonieme vorm opnemen in publicaties.

Voor zover de organisatie in het kader van haar onderzoek dat nuttig is voor de kennis, de conceptie en het beheer van de sociale bescherming vooraf zelf niet-gepseudonimiseerde persoonsgegevens aan de Kruispuntbank van de Sociale Zekerheid meedeelt (bij wijze van input) en ze achteraf van de Kruispuntbank van de Sociale Zekerheid (gekoppeld aan andere persoonsgegevens) als gepseudonimiseerde persoonsgegevens ontvangt (bij wijze van output), voorziet zij een strikte organisatorische scheiding van functies tussen de betrokken afdelingen/vakgroepen. De afdeling/vakgroep die de output ontvangt en verwerkt, moet verschillend zijn van de afdeling/vakgroep die de input aanlevert en mag geen toegang hebben tot de input.

De organisatie houdt de meegedeelde gepseudonimiseerde persoonsgegevens bij zolang zij ze nodig heeft voor het realiseren van haar onderzoek dat nuttig is voor de kennis, de conceptie en het beheer van de sociale bescherming en uiterlijk tot de datum die de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité in voorkomend geval vaststelt. Daarna vernietigt zij ze onherroepelijk.

De organisatie neemt bij een gegevensaanvraag alle maatregelen om zelf voorstellen te doen rond gegevensminimalisatie en degelijke pseudonimisering.

4. <u>Authenticatie van de identiteit van de gebruiker</u>

De organisatie authentiseert de identiteit van de natuurlijke persoon die de persoonsgegevens verwerkt (de ‘gebruiker’).

Deze authenticatie geschiedt

- hetzij met een middel geïntegreerd in de Federal Authentication Service (FAS) van een niveau dat gelijk is aan of hoger is dan 400
- hetzij door een authenticatiesysteem eigen aan de organisatie
    - mits een registratie van de identiteit geschiedt aan de hand van een eenmalig gebruik van een authenticatiemiddel geïntegreerd in de FAS van een niveau dat gelijk is aan of hoger is dan het niveau 400
    - mits het authenticatiesysteem eigen aan de aanbieder voldoet aan de voorwaarden voor een betrouwbaarheidsniveau ‘substantieel’ zoals gepreciseerd in de punten 2.1., 2.2.1. element 2, 2.2.3., 2.2.4., 2.3.1. (met uitzondering van element 1) en 2.4. van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening[1] en
    - mits het authenticatiemiddel gebruikt in het authenticatiesysteem eigen aan de aanbieder en het activeringsproces ervan voldoet aan de voorwaarden voor een betrouwbaarheidsniveau ‘laag’ in punt 2.2.1. element 1 en punt 2.2.2. van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDASverordening, en het zodanig is ontworpen dat het kan worden verondersteld slechts te worden gebruikt door de persoon aan wie het toebehoort.

[1] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015R1502&from=NL

Het eenmalig gebruik van een authenticatiemiddel geïntegreerd in de FAS om de identiteit van de gebruiker te registreren houdt niet in dat de FAS zelf daartoe moet worden gebruikt. De elektronische identiteitskaart kan bijvoorbeeld ook gewoon worden opgevraagd om de foto visueel te vergelijken met de houder van de kaart, of uitgelezen aan de hand van een eigen implementatie van de betrokken organisatie. Het authenticatiesysteem eigen aan de organisatie moet voldoen aan de voorwaarden voor het betrouwbaarheidsniveau 'substantieel' van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening, met dien verstande dat het authenticatiemiddel wel een authenticatiemiddel mag zijn dat gebruik maakt van slechts één authenticatiefactor (bvb. gebruikersnummer en paswoord).).

5. Logging

De elektronische toegang tot de persoonsgegevens wordt door de organisatie gelogd. Het systeem van logbeheer moet de organisatie minstens de mogelijkheid bieden om snel en eenvoudig te kunnen bepalen welke natuurlijke persoon op welk tijdstip en op welke wijze toegang heeft verkregen tot welke persoonsgegevens van de Kruispuntbank van de Sociale Zekerheid en om de persoon die de persoonsgegevens heeft verwerkt eenduidig te kunnen identificeren. De organisatie beschikt over de noodzakelijke tools om de geautoriseerde personen in staat te stellen de loggegevens uit te baten en bewaart de loggegevens minstens tien jaar (gedurende 6 maanden online en gedurende 9 jaar en 6 maanden in een archief).

6. Audittrail

De organisatie zorgt ervoor dat, naar aanleiding van een klacht, in geval van een onderzoek, op initiatief van de Kruispuntbank van de Sociale Zekerheid of van een toezichtsorgaan, een volledige reconstructie kan worden geboden met het oog op het vaststellen welke natuurlijke persoon toegang heeft gehad tot welke soorten persoonsgegevens, wanneer en op welke manier. Voorts stemt de organisatie er uitdrukkelijk mee in dat vertegenwoordigers van de Kruispuntbank van de Sociale Zekerheid te allen tijde toegang hebben tot de lokalen waar de door haar meegedeelde persoonsgegevens worden bewaard, om toe te zien op de uitvoering van de bepalingen van de geldende regelgeving en in voorkomend geval de toepasselijke beraadslaging(en) die werd(en) verleend door de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité.

7. Informatie, vorming en sensibilisering

De organisatie stelt de nodige gedragslijnen op om uitvoering te geven aan de criteria die vermeld zijn in dit document, stelt deze op een algemeen toegankelijke wijze ter beschikking van alle gebruikers die deel uitmaken van de cirkel van vertrouwen, biedt daarover aan deze gebruikers een gepaste permanente vorming aan en sensibiliseert hen voortdurend tot het naleven van de gedragslijnen.

8. Interne controle

De organisatie organiseert een regelmatige interne controle op de naleving van de criteria vervat in dit document en de gedragslijnen die er uitvoering aan geven. Ze bewaart de resultaten van die interne controle gedurende twee jaar. Ze voorziet ook afschrikwekkende sancties ten aanzien van de gebruikers die deel uitmaken van de cirkel van vertrouwen en de criteria niet naleven.

9. Naleving van de beraadslagingen van het informatieveiligheidscomité

De organisatie bevestigt alle maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer na te leven die zijn vermeld in de toepasselijke beraadslaging(en) van de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, verleend met toepassing van artikel 15 van de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*.

10. Openbare documentatie

De organisatie publiceert op haar website op een begrijpelijke wijze de doeleinden waarvoor ze persoonsgegevens uit het datawarehouse arbeidsmarkt en sociale bescherming verwerkt alsook de gedragslijnen waarmee uitvoering wordt gegeven aan het evenredigheidsbeginsel.

11. Externe controle

De organisatie houdt de documenten en gedragslijnen die ze voor de naleving van deze voorwaarden uitwerkt evenals de resultaten van de interne controle ter beschikking van de toezichtsorganen.