Informatieveiligheidscomité
Kamer sociale zekerheid en gezondheid

IVC/KSZG/25/034

BERAADSLAGING NR. 25/016 VAN 14 JANUARI 2025 OVER DE MEDEDELING VAN PERSOONSGEGEVENS OVER DE MOGELIJKHEID VAN TEWERKSTELLING MET BIJZONDERE REGELING INZAKE SOCIALEZEKERHEIDSBIJDRAGEN DOOR DE RIJKSDIENST VOOR SOCIALE ZEKERHEID AAN POTENTIËLE WERKGEVERS, SOCIALE MANDATARISSEN EN WERVINGS- EN SELECTIEBUREAUS IN HET KADER VAN EEN PRECONTRACTUELE RELATIE OP BASIS VAN EEN MANDAAT VERSTREKT DOOR DE BETROKKENE

Gelet op de wet van 15 januari 1990 *houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid*, in het bijzonder artikel 15, § 1;

Gelet op de aanvraag van de Rijksdienst voor Sociale Zekerheid;

Gelet op het rapport van de Kruispuntbank van de Sociale Zekerheid;

Gelet op het verslag van de voorzitter.

A. VOORWERP

1. Bij de beraadslaging nr. 24/222 van 3 december 2024 besliste de kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité, naar aanleiding van een vraag van de betrokken instellingen van sociale zekerheid, dat de mededeling van persoonsgegevens uit het netwerk van de sociale zekerheid door een instelling van sociale zekerheid aan een organisatie, een onderneming of een individuele beroepsbeoefenaar, op basis van een mandaat verstrekt door een natuurlijke persoon, steeds moet geschieden volgens de bepalingen van die beraadslaging. Voormelde beraadslaging geldt als een algemeen kader dat steeds moet worden geëerbiedigd maar doet geen afbreuk aan de bevoegdheid van het informatieveiligheidscomité om zich, geval per geval, in concrete situaties over dergelijke verwerkingen van persoonsgegevens uit te spreken.

2. Overeenkomstig de beraadslaging nr. 24/222 van 3 december 2024 gebeurt de mededeling van persoonsgegevens in het kader van een relatie met een gestandaardiseerd mandaat verstrekt door de betrokkene. De draagwijdte van elk (type) mandaat dat kan verstrekt worden, wordt door het informatieveiligheidscomité goedgekeurd.

3. Deze specifieke beraadslaging heeft betrekking op de mededeling van bepaalde persoonsgegevens door de Rijksdienst voor Sociale Zekerheid aan potentiële werkgevers, om in de precontractuele fase, op basis van een mandaat van de betrokkene, te kunnen

nagaan of de betrokkene al dan niet kan worden tewerkgesteld met toepassing van bepaalde regelingen inzake socialezekerheidsbijdragen.

4. De betrokkene kan dit mandaat van het type "precontractuele persoonsgegevens" verlenen aan drie categorieën van mandaatnemers: potentiële werkgevers, door werkgevers in het kader van de sociale administratie aangestelde mandatarissen en wervings- en selectiebureaus.

5. De eerste categorie (potentiële werkgevers) betreft alle entiteiten die over een ondernemingsnummer beschikken. In de precontractuele fase moeten zij nog niet noodzakelijk als werkgever ingeschreven zijn bij de Rijksdienst voor Sociale Zekerheid. Het kan bijvoorbeeld gaan over een zelfstandige (natuurlijke persoon) die een eerste werknemer wil aanwerven. Erkende uitzendbureaus vallen ook onder de categorie van potentiële werkgevers. De erkende uitzendbureaus die op zoek gaan naar geschikt werk voor de personen die bij hen zijn ingeschreven, moeten, mits mandaat van de betrokkene, bijvoorbeeld kunnen nagaan of de betrokkene al dan niet met een bijzondere regeling inzake socialezekerheidsbijdragen kan worden tewerkgesteld. In dit kader stellen partijen hun bedoeling om een arbeidsovereenkomst voor uitzendarbeid te sluiten schriftelijk vast in een intentieverklaring (overeenkomstig artikel 8, § 2, van de wet van 24 juli 1987 *betreffende de tijdelijke arbeid, de uitzendarbeid en het ter beschikking stellen van werknemers ten behoeve van gebruikers*).

6. Een tweede categorie van mandaatnemers betreft de sociale mandatarissen die door een werkgever worden aangesteld in het kader van zijn sociale administratie, bedoeld in artikel 31ter van de wet van 29 juni 1981 *betreffende de algemene beginselen van de sociale zekerheid der werknemers*. Deze categorie omvat twee types sociale mandatarissen: enerzijds de erkende sociale secretariaten, anderzijds de niet-erkende sociale dienstverrichters die bij de Rijksdienst voor Sociale Zekerheid geregistreerd zijn.

7. De derde categorie betreft wervings- en selectiebureaus die betrokkenen bijstaan bij het zoeken van een tewerkstelling en/of werkgevers bijstaan bij het zoeken naar geschikte werknemers. Media die vacatures verspreiden, ICT-dienstverleners van wervings- en selectiebureaus,… vallen hier niet onder.

B. BEHANDELING

8. Het informatieveiligheidscomité acht het opportuun om de essentie van het mandaat van de betrokkene, verleend overeenkomstig het algemeen kader van de beraadslaging nr. 24/222 van 3 december 2024, te onderstrepen: de mededeling van persoonsgegevens door een instelling van sociale zekerheid met mandaat van de betrokkene in het kader van een relatie gebeurt op basis van de geïnformeerde toestemming van de betrokkene met de voorwaarden van een dergelijk mandaat.

9. Het informatieveiligheidscomité stelt vast dat de hem voorgelegde vier documenten over de mededeling van de set "precontractuele persoonsgegevens", door de Rijksdienst voor Sociale Zekerheid op basis van een mandaat van de betrokkene, de voorwaarden inzake de toegang tot deze persoonsgegevens vastleggen waardoor de gemandateerde potentiële werkgevers, sociale mandatarissen en wervings- en selectiebureaus louter toegang krijgen

tot de persoonsgegevens die noodzakelijk zijn voor de realisatie van de hogervermelde finaliteit. Hiermee wordt tevens een minimale gegevensdeling vooropgesteld.

C. BESLUIT

De kamer sociale zekerheid en gezondheid van het informatieveiligheidscomité verleent zijn goedkeuring aan de volgende documenten, die als bijlage gaan en integraal deel uitmaken van deze beraadslaging:

- het document met de voorwaarden waaronder de betrokkene een mandaat met betrekking tot de toegang tot de "precontractuele persoonsgegevens" verschaft;

- het document met de voorwaarden waaronder de mandaathouder een toegang tot de "precontractuele persoonsgegevens" heeft;

- het gebruikersreglement voor de toegang via onlinedienst tot sociale gegevens van persoonlijke aard op basis van een mandaat verstrekt door een natuurlijke persoon;

- het reglement tot vaststelling van de criteria voor de toepassing van een cirkel van vertrouwen door een organisatie, een onderneming of een individuele beroepsbeoefenaar in het kader van de uitwisseling van sociale gegevens van persoonlijke aard op basis van een mandaat verstrekt door een natuurlijke persoon.

Aldus geeft het informatieveiligheidscomité zijn goedkeuring aan de beschreven voorwaarden inzake de toegang tot bepaalde persoonsgegevens van de Rijksdienst voor Sociale Zekerheid (over de mogelijkheid van tewerkstelling met een bijzondere regeling inzake socialezekerheidsbijdragen) door potentiële werkgevers, sociale mandatarissen en wervings- en selectiebureaus, op basis van een mandaat verstrekt door de betrokkene, via een *application programming interface* (API).

Deze beraadslaging treedt in werking op 29 januari 2025.

Michel DENEYER
Voorzitter

Bijlage 1

Voorwaarden mandaat toegang tot precontractuele gegevens

U stemt ermee in dat de door u goedkeurde ontvangers (mandaathouders) in het kader van een sollicitatie volgens de hieronder bepaalde voorwaarden op basis van uw mandaat bepaalde gegevens kunnen raadplegen.

Voor uw studentencontingent is uw mandaat geldig voor maximaal 3 maanden vanaf de datum van registratie van uw toestemming. Voor flexi-jobs is uw mandaat geldig voor maximaal 1 maand vanaf de datum van registratie van uw mandaat.

U kan uw mandaat steeds intrekken via: https://toegangtotmijndata.fgov.be/XXXX.

Het verstrekken of intrekken van een mandaat wordt elektronisch geregistreerd. Een overzicht van uw actieve mandaten vindt u hier.

Verwerkingsverantwoordelijke

De ontvanger van de persoonsgegevens engageert er zich als verwerkingsverantwoordelijke toe om de relevante bepalingen inzake gegevensbescherming, waaronder de algemene verordening gegevensbescherming (AVG of GDPR), na te leven.

Persoonsgegevens

Uw mandaat geldt voor de raadpleging van volgende persoonsgegevens:

- voor studentenarbeid: het aantal beschikbare uren van het contingent studentenarbeid met toepassing van solidariteitsbijdrage,
- voor flexi-jobs: het antwoord op de vraag of u al dan niet voldoet aan de tewerkstellings- of pensioneringsvoorwaarden.

Doeleinde

De ontvanger mag uw persoonsgegevens uitsluitend verwerken om, in het kader van een sollicitatie, na te gaan of u in aanmerking komt voor tewerkstelling als flexi-werknemer of als student met solidariteitsbijdrage, en zo ja, voor hoeveel resterende uren of dagen.

Bewaringstermijn

De ontvanger mag deze gegevens enkel verwerken gedurende de periode die noodzakelijk is om te beslissen of hij u al dan niet zal tewerkstellen via het statuut jobstudent of flexi-job. Wanneer de ontvanger beslist om u niet aan te werven, moet hij uw gegevens onmiddellijk vernietigen.

Informatiebeveiliging

De toegang uw persoonsgegevens verloopt steeds op een beveiligde elektronische manier. De ontvanger moet de door het Informatieveiligheidscomité bepaalde maatregelen inzake informatiebeveiliging naleven:

- bij raadpleging via onlinedienst: volgend gebruikersreglement
- bij raadpleging via API: volgende “cirkel van vertrouwen” (CoT)

Bijlage 2

Voorwaarden mandaathouder toegang tot precontractuele gegevens

U verbindt zich ertoe de hieronder bepaalde voorwaarden na te leven waaronder u toegang krijgt tot bepaalde gegevens van de kandidaat-werknemer (mandaatgever) die u hiertoe in het kader van een sollicitatie een mandaat verleent.

Voor het studentencontingent is uw toegang voor maximaal 3 maanden geldig vanaf de registratie van het mandaat van de kandidaat-werknemer.

Voor flexi-jobs is uw toegang voor maximaal 1 maand geldig vanaf de registratie van het mandaat van de kandidaat-werknemer.

De kandidaat-werknemer kan zijn mandaat steeds intrekken. Een overzicht van de actieve mandaten vindt u hier.

Verwerkingsverantwoordelijke

Als verwerkingsverantwoordelijke engageert u zich ertoe om de relevante bepalingen inzake gegevensbescherming, waaronder de algemene verordening gegevensbescherming (AVG of GDPR), na te leven.

Persoonsgegevens

Het mandaat geldt voor de raadpleging van volgende persoonsgegevens van de kandidaat-werknemer:

- voor studentenarbeid: het aantal beschikbare uren van het contingent studentenarbeid met toepassing van solidariteitsbijdrage,
- voor flexi-jobs: het antwoord op de vraag of de kandidaat-werknemer al dan niet voldoet aan de tewerkstellings- of pensioneringsvoorwaarden.

Doeleinde

U mag deze persoonsgegevens uitsluitend verwerken om, in het kader van een sollicitatie, na te gaan of de kandidaat-werknemer in aanmerking komt voor tewerkstelling als flexi-werknemer of als student met solidariteitsbijdrage, en zo ja, voor hoeveel resterende uren of dagen.

Bewaringstermijn

U mag deze gegevens enkel verwerken gedurende de periode die noodzakelijk is om te beslissen of u deze kandidaat al dan niet zal tewerkstellen via het statuut jobstudent of flexi-job. Zodra wordt beslist om deze kandidaat niet aan te werven, moet u de gegevens onmiddellijk vernietigen.

Informatiebeveiliging

De toegang tot persoonsgegevens verloopt steeds op een beveiligde elektronische manier. U moet de door het Informatieveiligheidscomité bepaalde maatregelen inzake informatiebeveiliging naleven:

- bij raadpleging via onlinedienst: volgend gebruikersreglement
- bij raadpleging via API: volgende “cirkel van vertrouwen” (CoT)

Bijlage 3

Gebruikersreglement voor de toegang tot sociale gegevens van persoonlijke aard op basis van een mandaat verstrekt door een natuurlijke persoon

Artikel 1. - Toepassingsgebied

Dit reglement betreft de toegang tot en het verwerken van sociale gegevens van persoonlijke aard, aangeduid als persoonsgegevens, die bekomen werden van een instelling van de sociale zekerheid middels een mandaat verstrekt door een natuurlijke persoon, aan een organisatie, een onderneming of een individuele beroepsbeoefenaar.

Dit reglement betreft bijkomende verplichtingen en doet geen afbreuk aan de verplichtingen die voortkomen uit het Gebruikersreglement voor de toegang tot en het gebruik van het informatiesysteem van de federale overheid en de openbare instellingen van sociale zekerheid door ondernemingen en hun lasthebbers[1].

Artikel 2 - Definities

Betrokkene : een natuurlijke persoon die middels een mandaat, toegang verleent aan een derde instantie tot een bepaalde set van persoonsgegevens die hem betreffen.

Derde instantie : een organisatie, een onderneming of een individuele beroepsbeoefenaar die middels een mandaat, verstrekt door een betrokkene, toegang bekomt tot persoonsgegevens van deze betrokkene.

Artikel 3 – Rechtmatigheid en doelbindingsbeginsel

De derde instantie beschikt voor de verwerkingsactiviteiten m.b.t. betrokkenen die een mandaat hebben verstrekt, over een register van de verwerkingsactiviteiten zoals bedoeld in artikel 30 van de Algemene Verordening Gegevensbescherming (AVG), waarin de rechtmatige verwerkingsdoeleinden van de verwerkingsactiviteiten staan vermeld. Dit betreft dus ook verwerkingen van persoonsgegevens die bekomen werden door middel van een mandaat verstrekt door elke betrokkene.

Artikel 4 – Evenredigheidsbeginsel : beperking van de verwerking

De persoonsgegevens m.b.t. betrokkenen, kunnen enkel worden verwerkt door gebruikers van de derde instantie, die deze in hoofde van hun functie moeten kunnen verwerken voor de rechtmatige verwerkingsdoeleinden beschreven in het register van de verwerkingsactiviteiten en zoals vastgelegd in de specifieke beraadslaging die de draagwijdte van het verstrekte mandaat en de finaliteit ervan bepaalt.

[1] https://www.socialsecurity.be/site_nl/general/rules/rules_employer_N.pdf

Artikel 5 – Informatie, vorming en sensibilisering

De derde instantie stelt de nodige policies op om uitvoering te geven aan de voorwaarden vermeld in dit document, stelt deze op een algemeen toegankelijke wijze ter beschikking van alle gebruikers die toegang hebben tot de verstrekte gegevens, biedt hierover een gepaste permanente vorming aan aan deze gebruikers en sensibiliseert hen voortdurend tot het naleven van de policies

Artikel 6 – Naleving beraadslagingen informatieveiligheidscomité

De derde instantie organisatie bevestigt alle maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer na te leven die zijn voorzien in de toepasselijke beraadslagingen van het Informatieveiligheidscomité

Artikel 7 – Registratie van de aanvaarding en toepassing van dit reglement door de derde instantie

De derde instantie meldt dat zij akkoord gaat met de voorwaarden gesteld in dit document en deze toepast in haar organisatie. De melding gebeurt in het toegangsbeheersysteem van de Sociale Zekerheid door de personen die daartoe gemachtigd zijn door de verantwoordelijken van de organisatie.

Bijlage 4

Reglement tot vaststelling van de criteria voor de toepassing van een cirkel van vertrouwen door een organisatie, een onderneming of een individuele beroepsbeoefenaar in het kader van de uitwisseling van sociale gegevens van persoonlijke aard op basis van een mandaat verstrekt door een natuurlijke persoon

DOEL VAN HET REGLEMENT

Dit reglement betreft het verwerken van sociale gegevens van persoonlijke aard, aangeduid als persoonsgegevens, die bekomen werden van een instelling van de sociale zekerheid middels een mandaat verstrekt door een natuurlijke persoon, hierna de betrokkene genoemd, aan een organisatie, een onderneming of een individuele beroepsbeoefenaar, hierna de derde instantie genoemd.

De verwerking van persoonsgegevens dient te geschieden met de nodige maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer. Een belangrijk aspect daarvan is de waarborg dat de persoonsgegevens enkel worden verwerkt

- voor rechtmatige doeleinden en
- door personen die, voor het bereiken van die doeleinden, nood hebben aan de verwerking van persoonsgegevens m.b.t. de betrokkene.

In een systeem waarbij persoonsgegevens bekomen worden middels een mandaat dat een betrokkene verstrekt aan een derde instantie, vereist het bieden van dergelijke waarborg een duidelijke vastlegging van de verantwoordelijkheden van elkeen.

Dit reglement wil hiertoe bijdragen door het preciseren van het concept van ‘cirkels van vertrouwen’. Een ‘cirkel van vertrouwen’ is een groep gebruikers van een organisatie, waarvoor die organisatie zelf op een aantal vlakken informatieveiligheidsmaatregelen organiseert en de correcte naleving ervan bewaakt, zodat andere organisaties en de betrokkene er redelijkerwijze kunnen op betrouwen dat deze informatieveiligheidsmaatregelen worden nageleefd en deze maatregelen dus zelf niet meer moeten organiseren of bewaken.

Opdat andere organisaties dan de organisatie die een cirkel van vertrouwen instelt en de betrokkene, daarin rechtmatig vertrouwen zouden kunnen hebben, worden criteria vastgelegd waaraan elke organisatie die dergelijke cirkel van vertrouwen wenst te organiseren, moet voldoen. Deze criteria verwijzen maximaal naar reeds bestaande Europese en Belgische regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). Zij doen geen afbreuk aan deze regelgeving, die ten volle blijft gelden, maar preciseren in een aantal gevallen de wijze waarop aan deze regelgeving dient te worden voldaan.

De criteria zelf nemen de vorm aan van een reglement. Bij sommige criteria wordt voor een goede verstaanbaarheid toelichting verstrekt. Die toelichting is louter informatief.

OVERZICHT VAN DE CRITERIA

THEMA 1: RECHTMATIGHEIDS- EN DOELBINDINGSBEGINSEL

CRITERIUM 1: REGISTER VAN DE VERWERKINGSACTIVITEITEN

De organisatie beschikt voor de verwerkingsactiviteiten m.b.t. betrokkenen die een mandaat hebben verstrekt over een register van de verwerkingsactiviteiten zoals bedoeld in artikel 30 van de Algemene Verordening Gegevensbescherming (AVG), waarin de rechtmatige verwerkingsdoeleinden van de verwerkingsactiviteiten staan vermeld. Dit betreft dus ook verwerkingen van persoonsgegevens die bekomen werden door middel van een mandaat verstrekt door elke betrokkene.

THEMA 2: EVENREDIGHEIDSBEGINSEL

CRITERIUM 2: VERWERKINGSBEPERKING

De persoonsgegevens m.b.t. betrokkenen kunnen enkel worden verwerkt door gebruikers van de derde instantie, die deze in hoofde van hun functie moeten kunnen verwerken voor de rechtmatige verwerkingsdoeleinden beschreven in het register van de verwerkingsactiviteiten en zoals vastgelegd in de specifieke beraadslaging die de draagwijdte van het mandaat en de finaliteit ervan bepaalt. De verwerkingsmogelijkheden worden voldoende fijnmazig gemoduleerd, zodat elke gebruiker slechts de persoonsgegevens kan verwerken van de betrokkenen waarvoor dit in hoofde van zijn functie nodig is en over de tijdsperiode waarvoor dit in hoofde van zijn functie nodig is.

THEMA 3: GEBRUIKERS- EN TOEGANGSBEHEER

CRITERIUM 3: AUTHENTICATIE VAN DE IDENTITEIT VAN DE GEBRUIKER

De derde instantie authentiseert de identiteit van de natuurlijke persoon die de bekomen 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 het niveau 400;
- hetzij, voor interne toepassingen, 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 vastgesteld door het Beheerscomité van de Kruispuntbank van de Sociale Zekerheid en
    - 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 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.

Toelichting

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 gebruikt maakt van slechts één authenticatiefactor (bvb. gebruikersnummer en paswoord).

THEMA 4: LOGGING

CRITERIUM 4: INTERNE LOGGING

De elektronische toegang tot persoonsgegevens wordt gelogd. Het logbeheer moet minimaal beantwoorden aan de volgende doelstellingen

- toelaten snel en eenvoudig te kunnen bepalen welke natuurlijke persoon, wanneer en op welke manier toegang heeft verkregen tot welke persoonsgegevens m.b.t. welke persoon;
- de persoon die persoonsgegevens heeft verwerkt en de persoon waarover persoonsgegevens zijn verwerkt eenduidig kunnen identificeren;
- de noodzakelijke tools ter beschikking hebben om toe te laten de loggegevens uit te baten door de geautoriseerde personen;
- de loggegevens minstens 10 jaar bewaren.

CRITERIUM 5: AUDITTRAIL

Omdat de elektronische verwerking van persoonsgegevens de toegang inhoudt tot persoonsgegevens, wordt ervoor gezorgd dat bij onderzoek, op initiatief van de Kruispuntbank van de Sociale Zekerheid, of van een toezichtsorgaan, naar aanleiding van een klacht, een volledige reconstructie kan geschieden die ertoe strekt te bepalen welke natuurlijke persoon toegang heeft gehad tot welke soorten persoonsgegevens m.b.t. welke personen, wanneer en op welke manier.

Indien voor de logging, die in uitvoering van criterium 4 wordt bijgehouden, alle in dat criterium vermelde informatie beschikbaar is in één loggingbestand, kan deze reconstructie geschieden overeenkomstig dat loggingbestand.

Onder coördinatie van de Kruispuntbank van de Sociale Zekerheid worden methoden afgesproken die deze volledige reconstructie mogelijk maken.

THEMA 5: INFORMATIE, VORMING, SENSIBILISERING, CONTROLE EN SANCTIES

CRITERIUM 6: INFORMATIE, VORMING EN SENSIBILISERING

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

CRITERIUM 7: INTERNE CONTROLE

De organisatie organiseert een regelmatig intern toezicht op de naleving van de criteria vervat in dit document en de policies die er uitvoering aan geven. Bij organisaties waar meer dan [10] personen zijn tewerkgesteld die toegang hebben tot persoonsgegevens verwerkt door derden, neemt dit regelmatig toezicht de vorm aan van een formele interne controle. De organisatie bewaart de resultaten van dit intern toezicht of van deze interne controle gedurende 2 jaar. De organisatie voorziet in afschrikwekkende sancties t.a.v. gebruikers die deel uitmaken van de cirkel van vertrouwen die de criteria of de policies die eraan uitvoering geven niet naleven.

THEMA 6: NALEVING BERAADSLAGINGEN INFORMATIEVEILIGHEIDSCOMITE

CRITERIUM 8: NALEVING BERAADSLAGINGEN INFORMATIEVEILIGHEIDSCOMITE

De derde instantie bevestigt alle maatregelen inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer na te leven die zijn voorzien in de toepasselijke beraadslagingen van het Informatieveiligheidscomité.

THEMA 7: HANDHAVING

CRITERIUM 9: OPNAME VAN DE TOETREDING VAN DE DERDE INSTANTIE ALS ORGANISATIE DIE EEN CIRKEL VAN VERTROUWEN ORGANISEERT IN HET TOEGANGSBEHEERSYSTEEM VAN DE SOCIALE ZEKERHEID

De derde instantie meldt dat zij een cirkel van vertrouwen instelt overeenkomstig de voorwaarden vermeld in dit document, en bevestigt daarbij te voldoen aan elk van deze voorwaarden. De melding gebeurt in het toegangsbeheersysteem van de Sociale Zekerheid door de personen die daartoe gemachtigd zijn door de verantwoordelijken van de organisatie.

CRITERIUM 10: EXTERNE CONTROLE

De derde instantie houdt het verwerkingsregister en de documenten en policies die ze voor de naleving van deze voorwaarden uitwerkt, evenals de resultaten van het intern toezicht of de interne controle, ter beschikking van de toezichtsorganen.

BIJLAGE: GLOSSARIUM

ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

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.

Zie https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679

AUTHENTICATIE VAN DE IDENTITEIT

Het proces waarbij wordt nagegaan of de identiteit die een entiteit beweert te hebben om gebruik te kunnen maken van een elektronische dienst, de juiste identiteit is. De authenticatie van de identiteit kan geschieden op basis van een controle van

- kennis (vb. een paswoord);
- bezit (vb. een certificaat op een elektronisch leesbare kaart);
- biometrische eigenschap(pen);
- een combinatie van één of meerdere van deze middelen.

CIRKEL VAN VERTROUWEN

Een cirkel van vertrouwen is een groep gebruikers van een organisatie waarvoor de organisatie zelf op een aantal vlakken informatieveiligheidsmaatregelen organiseert en de correcte naleving ervan bewaakt, zodat andere organisaties er redelijkerwijze kunnen op betrouwen dat deze informatieveiligheidsmaatregelen worden nageleefd en deze maatregelen dus zelf niet meer moeten organiseren of bewaken.

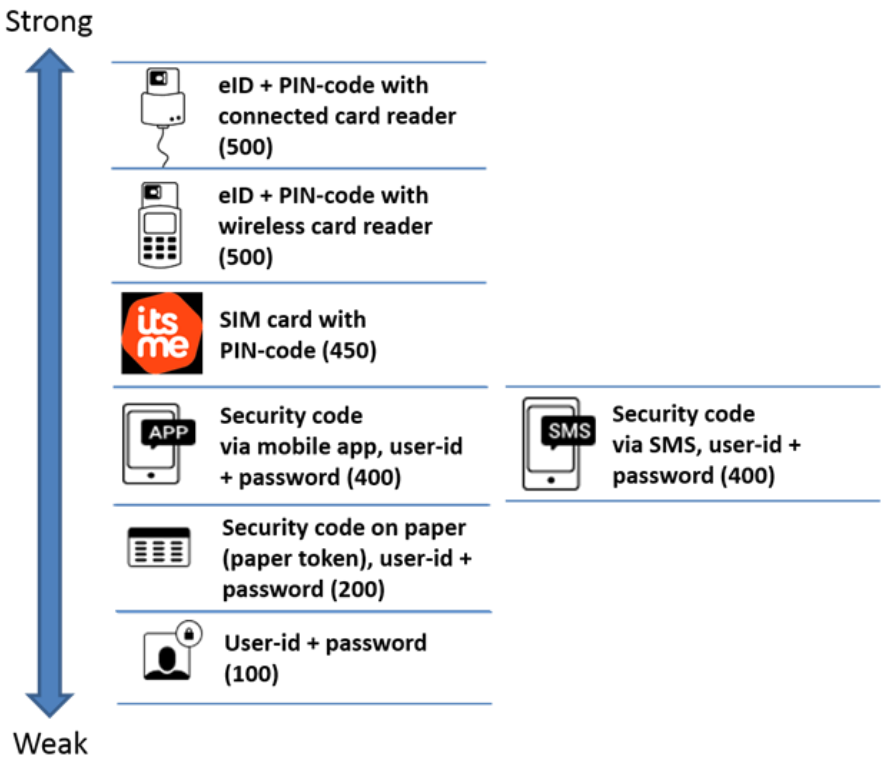
EIDAS - VERORDENING

Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG en de Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

Zie https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:32014R0910

FEDERAL AUTHENTICATION SERVICE (FAS)

Een dienst aangeboden door de FOD BOSA aan de hand waarvan gebruikers van elektronische diensten hun identiteit kunnen authentiseren via verschillende middelen met stijgend veiligheidsniveau. De FAS is een onderdeel van CSAM, een dienst die een algemene oplossing biedt voor alle aspecten van gebruikers- en toegangsbeheer voor online overheidsdiensten. Zie https://iamapps.belgium.be/sma/generalinfo?view=home



GEBRUIKER

De gebruiker is de persoon die persoonsgegevens verwerkt.

IDENTIFICATIENUMMER SOCIALE ZEKERHEID (INSZ)

Unieke identificatiesleutel per natuurlijk persoon die wordt gebruikt in de overheids-, sociale- en gezondheidssector. Voor de personen opgenomen in het Rijksregister is dit het rijksregisternummer dat vermeld staat op de elektronische identiteitskaart. Voor de andere personen is dit een nummer dat de Kruispuntbank van de Sociale Zekerheid toekent en beheert in een gegevensbank, de KSZ-registers.

UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE EIDAS-VERORDENING

Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

Zie https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ%3AJOL_2015_235_R_0002

INFORMATIEVEILIGHEIDSCOMITE

Het Informatieveiligheidscomité ingesteld bij wet van 5 september 2018.