|  |
| --- |
|  |
|  |
|  |
|  |
|  |

**BIV-classificatie 2.0**

***Classificatie van gegevens binnen UWV met het oog op het waarborgen van hun beschikbaarheid, integriteit en vertrouwelijkheid***

***Status: vastgesteld***

**Inhoud**

[1 Versiebeheer 3](#_Toc29758947)

[2 Inleiding 5](#_Toc29758948)

[2.1 Wat is BIV-classificatie 5](#_Toc29758949)

[2.2 Waarom is BIV-classificatie belangrijk? 5](#_Toc29758950)

[2.3 BIV-classificatie, risico’s en maatregelen 6](#_Toc29758951)

[2.4 Beschikbaarheid, Integriteit en Vertrouwelijkheid kennen een eigen dynamiek 6](#_Toc29758952)

[2.5 Doel van dit document 7](#_Toc29758953)

[2.6 Totstandkoming en eigenaarschap van dit document 8](#_Toc29758954)

[3 Beschikbaarheid 9](#_Toc29758955)

[3.1 Wat is beschikbaarheid? 9](#_Toc29758956)

[3.2 Welke beschikbaarheidsniveau onderscheiden we? 9](#_Toc29758957)

[3.3 Wie is verantwoordelijk voor het classificeren en het bepalen van het juiste beschikbaarheidsniveau? 10](#_Toc29758958)

[3.4 Instructie bepalen beschikbaarheidsklasse 10](#_Toc29758959)

[4 Integriteit 12](#_Toc29758960)

[4.1 Wat is integriteit? 12](#_Toc29758961)

[4.2 Welke integriteitsniveaus onderscheiden we? 12](#_Toc29758962)

[4.3 Wie is verantwoordelijk voor het classificeren en bepalen van het juiste integriteitsniveau? 12](#_Toc29758963)

[4.4 Instructie integriteitsclassificatie 13](#_Toc29758964)

[4.4.1 Stroomschema integriteitsclassificatie 14](#_Toc29758965)

[5 Vertrouwelijkheid 15](#_Toc29758966)

[5.1 Wat is vertrouwelijkheid? 15](#_Toc29758967)

[5.2 Welke vertrouwelijkheidsniveaus onderscheiden we? 15](#_Toc29758968)

[5.3 Gezondheidsgegevens en medisch beroepsgeheim 18](#_Toc29758969)

[5.4 Wie is verantwoordelijk voor het classificeren en het bepalen van het juiste vertrouwelijkheidsniveau? 18](#_Toc29758970)

[5.5 Gebruik van vertrouwelijkheidsklassen 19](#_Toc29758971)

[5.6 Instructie vertrouwelijkheidsclassificatie 19](#_Toc29758972)

[5.6.1 Stroomschema’s vertrouwelijkheidsclassificatie 20](#_Toc29758973)

[6 Relatie met andere classificatiesystemen 22](#_Toc29758974)

[6.1 BIO 22](#_Toc29758975)

[6.2 Classificatie indelingen buiten UWV 23](#_Toc29758976)

1. Versiebeheer

**Wijzigingen**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Verandering** |
| 1.00 | 18-04-2016 | Ronald Paans |  |
|  |  | Petra Billekens |  |
| 1.05 | 02-07-2018 | Stef Schinagl  Joseline van Tessel | Introductie V-klasse 2+; Reguliere persoonsgegevens hoger geclassificeerd om aan AVG te voldoen |
| 1.10 | 30-01-2019 | Esther Sloof Anne van de Geijn  Adrienne Boerwinkel | Tekst herzien en afgestemd op UWV Beleidskader Privacy. |
| 1.20  1.30  1.50  1.90 | 27-09-2019  05-11-2019  15-11-2019  10-01-2020 | Esther Sloof  Anne van de Geijn  Adrienne Boerwinkel  Esther Sloof  Anne van de Geijn  Esther Sloof  Esther Sloof | Richtlijn toepassing vertrouwelijheidsclassificaties opgenomen.  Passages mbt gegevensleveringen toegevoegd.  Meer aandacht voor onderscheid classificatie en maatregelen.  Review verwerkt.  Titel aangepast ivm herkenbaarheid.  §2.3: Positionering BIV aangepast obv bespreking met CISO;  §4.2: Integriteitsklasse I-0 verwijderd wegens nvt;  §5.2: Voorbeelden classificatieniveaus toegevoegd na bespreking BSO’s en JZ;  §6.1:Passage mbt BIO aangepast obv bespreking met CISO; meerdere paragrafen: Lokaal gegevensmanager gewijzigd in Gegevensmanager. |

**Distributie en besluitvorming**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Distributie** | **Status en doel** |
| 1.00  1.05  1.20  1.30  1.50 | 18-04-2016  02-07-2018  27-09-2019  05-11-2019  21-11-2019  27-11-2019 | Strategisch overleg coalitie IB&P  Tactisch overleg coalitie IB&P  Data Office: Corine Boersma en Patrick Stolk Gegevensdiensten: Mattheu van Bommel John Berendsen CISO-Office: Erik Kuipers  IS Applicatie-beschikbaarheid  Informeel BSO-overleg Operationeel Gegevensmanagers-overleg  Tactisch overleg van de coalitie IB&P  KOG | **Akkoord**  Geen akkoord  Review  Bespreking  bespreking |
| 1.90 | 16-01-2020  30-01-2020 | Tactisch overleg van de coalitie IB&P  Strategisch overleg van de coalitie IB&P | Ter informatie  Ter akkoord |
|  | 09-04-2020  **15-07-2020** | Strategisch overleg van de coalitie IB&P  **SO akkoord met implementatie 1.9 versie.** 2.0 versie wordt eind 2020 vastgesteld. | Ter akkoord |
| 2.0 | 17-12-2020 | Uitvraag via BSO’s | **Definitief vastgesteld** |
|  |  |  |  |

**Locatie:** <https://digitalewerkplek.sharepoint.uwv.nl/documentcenter/Documenten/Bestuurszaken/Team%20IBP%20BZ/Beleidsdocument>

1. Inleiding
   1. Wat is BIV-classificatie

Het classificeren van gegevens houdt in dat deze aan de hand van een analyse worden ingedeeld in verschillende niveaus van drie informatiebeveiligingsprincipes: beschikbaarheid, integriteit en vertrouwelijkheid. (Deze principes worden in de hoofdstukken 3 t/m 5 nader toegelicht)

Op elk van deze beveiligingsprincipes bepaalt het belang van de gegevens welk classificatieniveau van toepassing is. Het aldus vastgestelde classificatieniveau maakt mede inzichtelijk welk beschermingsniveau geboden is, zodat gerichte maatregelen kunnen worden getroffen om de gegevens adequaat te beschermen tegen onrechtmatige inzage, wijziging, verlies of onbeschikbaarheid.

Wanneer het bij classificatie over gegevens gaat, worden zowel *persoons*gegevens (gegevens met betrekking tot een geïdentificeerde of identificeerbare persoon) als *bedrijfs*gegevens (gegevens over bijvoorbeeld bedrijfsvoering, aanbestedingen of beleid) bedoeld.

Bij het classificeren worden gegevens altijd in context beschouwd. Juist de combinatie van gegevens bepaalt het classificatieniveau. Het gegeven ‘WIA<35’ wordt bijvoorbeeld pas gevoelig als dit door een identificerend gegeven zoals een naam of BSN aan een persoon kan worden gekoppeld.

* 1. Waarom is BIV-classificatie belangrijk?

Het classificatieniveau geeft uitdrukking aan het belang van gegevens. Het geeft daarmee inzicht in welke mogelijke schade een dreiging (bijvoorbeeld oneigenlijke toegang tot gegevens of uitval van het systeem waarin de gegevens worden ontsloten) kan toebrengen aan de organisatie of aan andere belanghebbenden, zoals klanten. Het toekennen van classificatieniveaus aan gegevens en informatiesystemen vormt zo een essentiële basis om te bepalen welk beschermingsniveau nodig is en welke beveiligingsmaatregelen daarbij passend zijn.

De classificatieniveaus zijn daarom relevant bij het ontwerpen van processen en systemen. Het helpt de proceseigenaar of systeemeigenaar om risicogericht maatregelen te treffen om de gegevens die in het proces of systeem omgaan adequaat te beschermen.

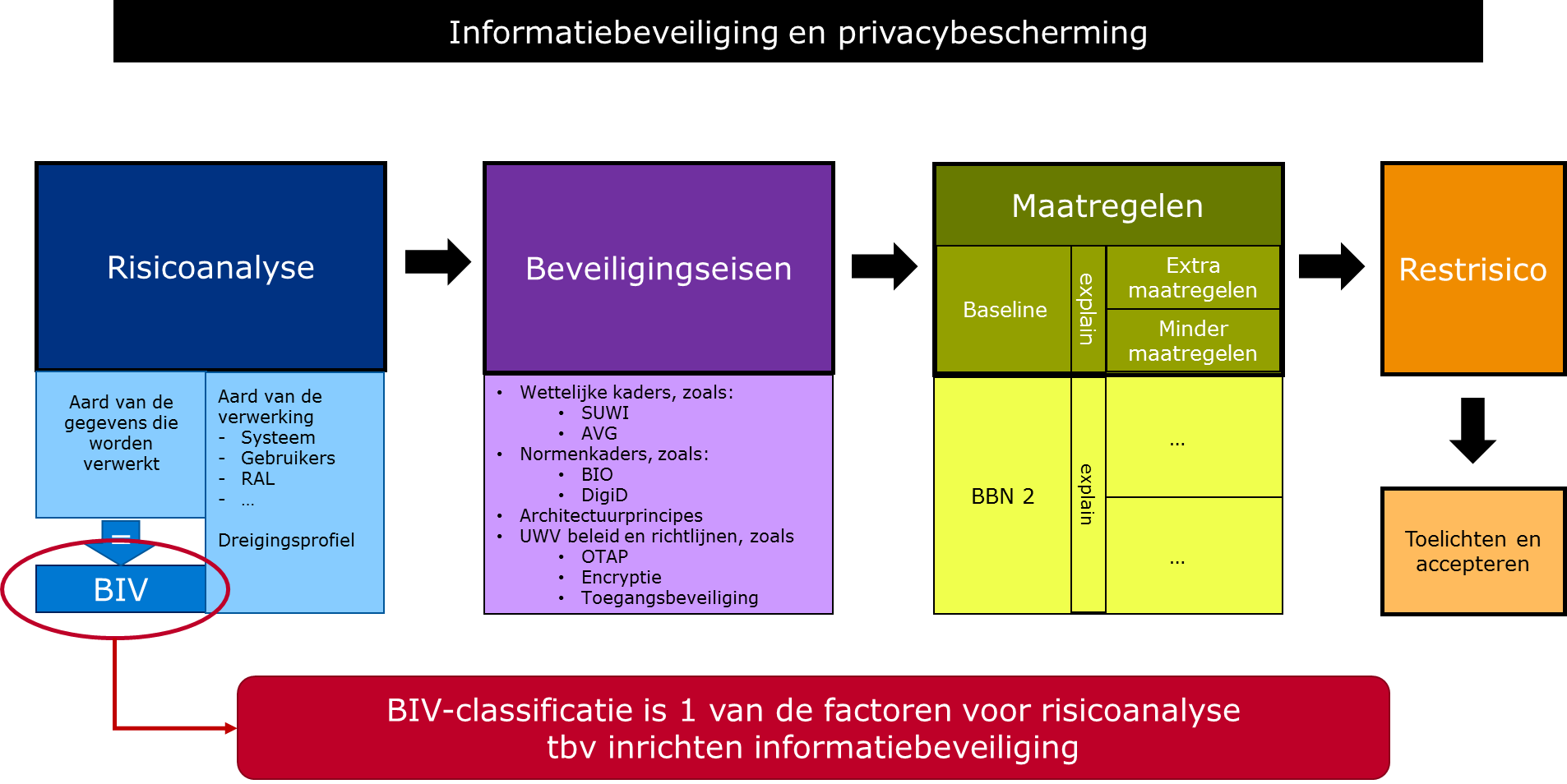
Daarnaast zijn de classificatieniveaus richtinggevend voor de beveiligingsmaatregelen die voor gegevensleveringen moeten worden getroffen.

In het geval van *persoons*gegevens zijn de classificatieniveaus bovendien van belang om te kunnen voldoen aan de Algemene verordening gegevensbescherming (AVG). Deze verplicht namelijk om *passende* beveiligingsmaatregelen te nemen om persoonsgegevens te beschermen. Wat passend is, hangt onder andere af van de aard van de gegevens en de context waarin deze worden verwerkt. Dit komt tot uitdrukking in de BIV-classificatieniveaus.

Het classificeren is daarmee een belangrijke eerste bouwsteen in de doorvertaling van de waarde van gegevens naar een passend beschermingsniveau en concrete maatregelen om inbreuken op de veiligheid te voorkomen.

* 1. BIV-classificatie, risico’s en maatregelen

Het BIV-classificatieniveau geeft een indicatie van het belang en de gevoeligheid van de betreffende gegevens. Om tot de juiste maatregelen te komen om gegevens adequaat te beschermen is alleen het BIV-classificatieniveau echter onvoldoende. In de informatiebeveiliging en privacybescherming maakt de BIV-classificatie onderdeel uit van een bredere risicoanalyse die wordt afgezet tegen beveiligingseisen en de baseline van wat al aan maatregelen is ingericht: het basis beveiligingsniveau (BBN2). Deze bredere analyse bepaalt wat het risico is en welke maatregelen getroffen moeten worden. In het plaatje hieronder wordt dit proces geillustreerd.



Hieruit volgt ook dat de BIV-classificatie niet door factoren als de omvang van een bestand of het aantal externe gebruikers wordt beinvloed. Deze factoren zijn wel van belang voor het bepalen van de maatregelen die moeten worden getroffen, maar hebben een plek in de bredere risicoanalyse; niet in de BIV-classificatie zelf. Als het bijvoorbeeld om een bestand met veel gevoelige gegevens met V-klasse 2+ gaat maakt de omvang van het bestand niet dat de V-klasse wordt bijgesteld naar V-klasse 3. De V-klasse blijft gelijk aan de hoogste V-klasse van de onderliggende gegevens (in dit voorbeeld: V-klasse 2+). Bij de bredere risicoanalyse wordt echter wel meegewogen dat de grote hoeveelheid gegevens het bestand als geheel gevoeliger maakt. Hierdoor zal het totale risicoprofiel hoger uitvallen, wat zal doorwerken in de maatregelen die moeten worden getroffen om het bestand adequaat te beschermen.

* 1. Beschikbaarheid, Integriteit en Vertrouwelijkheid kennen een eigen dynamiek

De beveiligingsprincipes beschikbaarheid, integriteit en vertrouwelijkheid zijn met elkaar verbonden omdat zij alle drie gericht zijn op het belang van de geclassificeerde gegevens en daarmee een indicatie geven van het benodigde beschermingsniveau. Toch verloopt het proces van het vaststellen van de classificaties langs verschillende lijnen en kennen zij een eigen ritme.

Het vaststellen van de vertrouwelijkheidsklasse is de verantwoordelijkheid van de gegevenseigenaar (de directie van het betreffende organisatieonderdeel). In de praktijk is deze verantwoordelijkheid meestal gedelegeerd aan de Gegevensmanager. Deze zorgt er voor dat de vertrouwelijkheidsklasse wordt vastgesteld en wordt vastgelegd in het functioneel gegevensmodel (FUGEM) – het overzicht van alle gegevens die door de systemen gaan. Wanneer de BSO of IB&P medewerker in het kader van de RAL de vertrouwelijkheidsklasse van de gegevens in een bepaalde applicatie moet invullen, neemt hij de hoogste classificatie van de onderliggende gegevens uit het betreffende FUGEM over. Ook bij het bepalen van de vertrouwelijkheid van de gegevens die in een gegevenslevering worden gedeeld of van gegevens van een verwerking die het onderwerp is van een GEB wordt het FUGEM geraadpleegd om de vertrouwelijkheid van de onderliggende gegevens vast te stellen. De bescherming van de gegevenslevering moet dan zijn gebaseerd op de hoogste vertrouwelijkheidsklasse van de onderliggende gegevens (waarbij in de bredere risicoanalyse ook andere factoren zoals de omvang van het bestand nog een rol spelen om de uiteindelijk benodigde beveiliging te bepalen).

Het vaststellen van de integriteitsklasse en de beschikbaarheidsklasse is de verantwoordelijkheid van de proceseigenaar. Het belang dat een bepaald gegeven juist, actueel en beschikbaar is hangt immers samen met het proces waarin het gegeven wordt gebruikt. Ten aanzien van processen in ketens is het van belang dat proceseigenaren met elkaar in gesprek gaan over de classificatie voor hun onderdeel van de keten. Indien er wordt uitgewisseld zullen de versturende en de ontvangende partij hun beschermingsniveau op elkaar moeten afstemmen en een van de factoren daarin betreft de BIV-classificatie.  
Bij het inrichten van de beveiliging van informatiesystemen, maken systeemeigenaren gebruik van de BIV-classificaties die voor de processen zijn vastgelegd. Omdat informatiesystemen veelal meerdere processen ondersteunen betekent dit dat de systeemeigenaar met meerdere proceseigenaren om tafel moet om de beveiliging van het betreffende informatiesysteem adequaat in te richten. Ook hier geldt dat de beveiliging op de hoogste klasse wordt gericht. Tegelijkertijd moet voorkomen worden dat informatiesytemen te zwaar beveiligd zijn waardoor het gebruik onevenredig wordt ingeperkt en kosten onnodig worden opgedreven. Het is daarom aan te raden om indien mogelijk het informatiesysteem in compartimenten te beschouwen en gerichte maatregelen te treffen.

* 1. Doel van dit document

Dit document (BIV-classificatie 2.0. *Classificatie van data binnen UWV*) geeft uitleg over welke BIV-classificatieniveaus UWV hanteert en welke gegevens tot welk classificatieniveau behoren. Voor elk van de beveiligingsprincipes (beschikbaarheid, integriteit en vertrouwelijkheid) wordt dit beleid ook vertaald naar een stappenplan van hoe het classificatieniveau wordt vastgesteld.

Het document is opgesteld om UWV medewerkers te helpen bij het vaststellen van de classificatieniveaus. Daarnaast geeft het UWV medewerkers die met classificatieniveaus geconfronteerd worden (bijvoorbeeld bij het uitvoeren van een risicoanalyse of bij het vaststellen van maatregelen) inzicht in waar de verschillende classificatieniveaus voor staan.

Het document is nadrukkelijk bedoeld voor de interne gegevensclassificatie van UWV en sluit aan bij het type gegevens dat UWV verwerkt. Buiten UWV worden diverse andere classificatie indelingen gebruikt. In hoofdstuk 6 wordt hier kort op ingegaan.

Het document voorziet niet in antwoorden op implementatievraagstukken of een vertaling van classificatieniveaus naar maatregelen. Dit laatste is niet wenselijk aangezien de BIV-classificatie slechts één van de facoren is in de analyse van het risicoprofiel van de verwerking (zie ook paragraaf 2.3). Voor meer informatie over welke maatregelen wanneer van toepassing zijn verwijzen we naar de richtlijnen die uit de BIO voortkomen en welke binnen UWV door CISO, BZ, HRM, Data Office en FB worden opgesteld.

* 1. Totstandkoming en eigenaarschap van dit document

Dit document is opgesteld door Bureau Gegevensbescherming in samenwerking met Data Office UWV, JZ en CISO. Bureau Gegevensbescherming is eigenaar van het BIV-beleid en Data Office UWV is eigenaar van de instructie met betrekking tot het vaststellen van de vertrouwelijkheidsclassificatie.

Vaststelling van het document gebeurt via het strategisch overleg van de coalitie IB&P en binnen de Data Governancelijn.

Het document vervangt de documenten BIV-classificatie versie.1.0 van 18 april 2016, BIV-classificatie versie 1.05 van 2 juli 2018 en de Richtlijn toepassing vertrouwelijkheidsclassificatie.

1. Beschikbaarheid
   1. Wat is beschikbaarheid?

Het beveiligingsprincipe ‘beschikbaarheid’ beschrijft hoeveel en wanneer gegevens toegankelijk moeten zijn en kunnen worden gebruikt. Beschikbaarheid is te definiëren als de 'eigenschap van het geheel van ICT-diensten, systemen, componenten en gegevensdragers die van invloed zijn op de tijd dat het product of de dienst (en daarmee informatie) beschikbaar is voor de geautoriseerde gebruiker, op de momenten dat het beschikbaar moet zijn'.

De beschikbaarheidsklasse wordt vastgesteld door de proceseigenaar. Deze weet hoe belangrijk de gegevens zijn om het proces te kunnen uitvoeren en hoe kritiek het proces is. Uit praktische overwegingen is het object van classificatie echter niet de gegevens, maar de informatiesystemen waar deze gegevens in beschikbaar worden gesteld. De maatregelen worden ook op het niveau van systeem genomen. Dit betekent dat de door de proceseigenaar vastgestelde beschikbaarheidsklasse input is voor de systeemeigenaar om maatregelen te nemen om de benodigde beschikbaarheid te kunnen garanderen.

Voor het classificeren van de beschikbaarheid van een informatiesysteem vormt de maximale tolereerbare uitvalsduur, ofwel ‘Recovery Time Objective (RTO)’, van een bedrijfsproces een belangrijk uitgangspunt. De RTO is een belangrijk instrument binnen bedrijfscontinuïteitsmanagement (BCM) en geeft aan hoe lang een bedrijfsproces stil mag liggen, voordat dit onacceptabele consequenties heeft voor klant, partners en eigen organisatie. Dit geeft een goede indicatie voor het gewenste beschikbaarheidsniveau van een informatiesysteem dat het bedrijfsproces mogelijk maakt: bij een lage RTO-score zal hoogstwaarschijnlijk een hoger beschikbaarheidsniveau van het betreffende informatiesysteem noodzakelijk zijn om de gewenste RTO in de praktijk ook daadwerkelijk te kunnen realiseren.

De classificatie van beschikbaarheid bepaalt welke maatregelen nodig zijn om de continuïteit van de dienstverlening zo goed mogelijk te borgen. De classificatie heeft daarmee bijvoorbeeld invloed op de Service Level Agreements (SLA) die met leveranciers wordt afgesloten, maar ook op de volgorde waarin informatiesystemen worden hersteld na een grootschalige verstoring.

* 1. Welke beschikbaarheidsniveau onderscheiden we?

Binnen UWV onderscheiden we vier beschikbaarheidsniveaus. Deze zijn hieronder omschreven.

|  |  |  |
| --- | --- | --- |
| **Klasse** | **Omschrijving** | **Toelichting** |
| B-0 | Laag | Het systeem kan zonder gevolgen langere tijd niet beschikbaar zijn. Uitval van het systeem heeft geen tot zeer beperkte negatieve gevolgen voor klanten, partners of eigen organisatie. |
| B-1 | Medium | Uitval van het systeem heeft enige negatieve gevolgen voor klanten, partners of eigen organisatie. De continuïteit zal op redelijke termijn moeten worden hervat. |
| B-2 | Hoog | Uitval van het systeem heeft serieuze negatieve gevolgen voor klanten, partners of eigen organisatie. De continuïteit zal snel moeten worden hervat. |
| B-3 | Kritiek | Uitval van het systeem heeft (zeer) grote negatieve gevolgen voor klanten, partners of eigen organisatie. De continuïteit zal zeer snel moeten worden hervat. |

Het bepalen van het beschikbaarheidsniveau van een informatiesysteem vindt plaats middels een kwalitatieve dialoog tussen betrokken partijen (systeemeigenaar en proceseigenaren). Voor beschikbaarheid wordt naar de volgende zaken gekeken:

* Het aantal bedrijfsprocessen dat het informatiesysteem ondersteunt;
* De bijbehorende RTO-scores (de maximaal toelaatbare uitvalsduur);
* De mate waarin deze bedrijfsprocessen afhankelijk zijn van het informatiesysteem voor continuering;
* Eventuele beschikbaarheidseisen waar aan moet worden voldaan (7x24 uur dienstverlening, kantoortijden etc.).
  1. Wie is verantwoordelijk voor het classificeren en het bepalen van het juiste beschikbaarheidsniveau?

Het bepalen van het juiste beschikbaarheidsniveau van informatiesystemen is een gezamenlijke verantwoordelijkheid van de systeemeigenaar, de proceseigenaren en indien van toeassing de keteneigenaren die van het informatiesysteem gebruik maken. De proceseigenaar geeft het belang van het proces en het belang van het informatiesysteem binnen het betreffende proces aan. De systeemeigenaar vertaalt de beschikbaarheidseisen die de verschillende processen aan het informatiesysteem stellen naar een beschikbaarheidsklasse voor het informatiesysteem.

Vanuit praktische overwegingen draagt de systeemeigenaar daarbij de verantwoordelijkheid voor het initiëren en faciliteren van dit proces. De uitvoering hiervan kan worden gedelegeerd aan de Business Security Officer voor reeds bestaande systemen of projectmanager voor de implementatie van een nieuw systeem of grote systeemwijziging. Bij UWV wordt de beschikbaarheidsklasse vastgelegd in de RAL en minimaal jaarlijks herijkt.

* 1. Instructie bepalen beschikbaarheidsklasse

***Stap 1 – Verzamel de RTO’s van de afnemende bedrijfsprocessen***

Voor het bepalen van het gewenste beschikbaarheidsniveau van een systeem dient als uitgangspunt de Recovery Time Objective (RTO) van de bedrijfsprocessen die door het informatiesysteem worden ondersteund. De RTO geeft de maximale uitvalsduur dat een bedrijfsproces tolereert en wordt middels een business impact analyse (BIA) bepaald op basis van onder andere de impact op de klant, reputatie, financiën. De BIA wordt uitgevoerd door de proceseigenaar. De RTO wordt tevens vastgesteld door de proceseigenaar.

***Stap 2 – Bepaal het beschikbaarheidsniveau o.b.v. de RTO’s***

Bij het bepalen van het beschikbaarheidsniveau dient de onderstaande tabel als richtlijn. De tabel is gebaseerd op het principe dat bij een lagere RTO-score een hoger beschikbaarheidsniveau noodzakelijk is om daadwerkelijk de RTO te kunnen realiseren.

|  |  |  |  |
| --- | --- | --- | --- |
| **RTO** | **Klasse** | **Omschrijving** | **Toelichting** |
| >5 dagen | B-0 | Laag | Het systeem kan zonder gevolgen langere tijd niet beschikbaar zijn. Uitval van het systeem heeft geen tot zeer beperkte negatieve gevolgen voor klanten, partners of eigen organisatie. |
| <5 dagen | B-1 | Medium | Uitval van het systeem heeft enige negatieve gevolgen voor klanten, partners of eigen organisatie. De continuïteit zal op redelijke termijn moeten worden hervat. |
| <24 uur | B-2 | Hoog | Uitval van het systeem heeft serieuze negatieve gevolgen voor klanten, partners of eigen organisatie. De continuïteit zal snel moeten worden hervat. |
| <2 uur | B-3 | Kritiek | Uitval van het systeem heeft (zeer) grote negatieve gevolgen voor klanten, partners of eigen organisatie. De continuïteit zal zeer snel moeten worden hervat. |

***Stap 3 – Stel het beschikbaarheidsniveau bij o.b.v. mate van afhankelijkheid***

De rol van een informatiesysteem in het bedrijfsproces kan verschillen: Het systeem kan cruciaal zijn voor het functioneren van het proces, maar kan ook ondersteunend zijn waarbij uitval van het systeem geen tot geringe impact heeft op het bedrijfsproces. Denk hierbij aan bijvoorbeeld een rapportagesysteem. In dit geval kan er worden afgeweken van het beschikbaarheidsniveau dat de tabel o.b.v. de RTO aangeeft en deze bijgesteld worden naar een lager beschikbaarheidsniveau.

1. Integriteit
   1. Wat is integriteit?

Integriteit betekent dat gegevens juist en volledig zijn en aldus in overeenstemming met de werkelijkheid. Maatregelen gericht op het waarborgen van integriteit zijn erop gericht te voorkomen dat gegevens onbevoegd kunnen worden gewijzigd of gewist. Dit is zowel van belang tijdens de opslag en het gebruik van gegevens, als tijdens transport. Om de integriteit aantoonbaar te kunnen waarborgen, moeten de juiste maatregelen worden ingericht.

Om te kunnen vaststellen dat een gegeven juist en volledig is, moeten ook de eventuele wijzigingen van dat gegeven kunnen worden herleid. Dit houdt in dat zowel de oorsprong als mutaties van gegevens moeten kunnen worden gevolgd zodat de authenticiteit van het gegeven kan worden bewezen.

* 1. Welke integriteitsniveaus onderscheiden we?

We onderscheiden twee niveaus voor integriteit van gegevens. Deze zijn hieronder beschreven.

|  |  |  |
| --- | --- | --- |
| **Klasse** | **Omschrijving** | **Toelichting** |
| I-1 | Beschermd | Het bedrijfsproces dat gebruik maakt van deze gegevens heeft geen directe hinder van (integriteits)fouten. Een basisniveau van beveiliging is noodzakelijk. Schending van de integriteit van gegevens in deze classificatie kan enige (in-)directe schade toebrengen.  Voorbeelden:   * Nieuwsberichten op DWU * Verslaglegging van teamvergaderingen |
| I-2 | Hoog | Het bedrijfsproces dat gebruik maakt van deze gegevens staat zeer weinig tot geen (integriteits)fouten toe. Schending van de integriteit en fouten in deze gegevens kan (zeer) grote schade toebrengen. **Deze integriteitsklasse geldt voor de meeste verwerkingen bij UWV.**  Voorbeelden:   * Alle persoonsgegevens van klanten en medewerkers van UWV * Financiële transacties * Gegevens in de Polisadministratie * Beschikkingen |

* 1. Wie is verantwoordelijk voor het classificeren en bepalen van het juiste integriteitsniveau?

De proceseigenaar is verantwoordelijk voor het vaststellen van het vereiste integriteitsniveau voor de gegevens. Aangezien de maatregelen om integriteit te waarborgen vooral op het niveau van informatiesystemen en transport liggen, heeft de systeemeigenaar een belangrijke rol om de integriteitsklassen te vertalen naar de juiste bescherming. Net als bij het vaststellen van de beschikbaarheidsklasse wordt daarom uit praktische overwegingen er veelal voor gekozen om de integriteitsklasse van gegevens per informatiesysteem vast te leggen. De systeemeigenaar is hierbij de initiatiefnemer. Binnen UWV wordt de integriteitsklasse in de RAL vastgelegd en minimaal jaarlijks herijkt.

* 1. Instructie integriteitsclassificatie

Binnen UWV is in de meeste gevallen I-klasse 2 van toepassing, omdat voor vrijwel alle gegevens die in de dienstverlening van UWV worden gebruikt geldt dat deze onweerlegbaar en aantoonbaar juist dienen te zijn.

De snelste manier om vast te stellen welk integriteitsniveau van toepassing is, is dan ook om deze I-klasse 2 als uitgangspunt te hanteren en te kijken of het object van classificatie van de daarbij gegeven omschrijving afwijkt.

Een andere methode neemt juist de gegevens en het gebruik van deze gegevens als startpunt van de analyse. Dit ziet er als volgt uit:

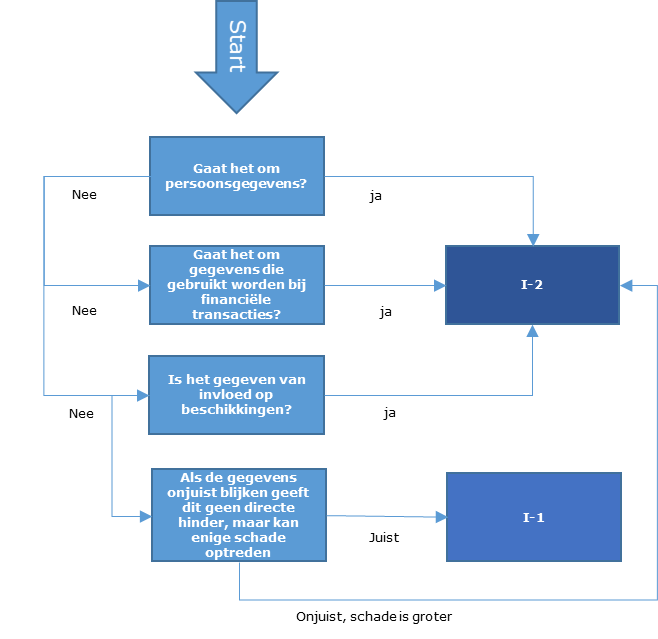
***Stap 1 – In kaart brengen van de afnemende bedrijfsprocessen***

De eerste stap is het inzichtelijk maken van de bedrijfsprocessen die gebruik maken van de gegevens in het systeem. Hiermee zijn tevens de belanghebbende partijen in kaart gebracht die bij het classificatieproces moeten worden betrokken.

***Stap 2 – Bepalen van de mate van afhankelijkheid van de integriteit***

Vervolgens is het wenselijk om per bedrijfsproces te bepalen wat de mate van afhankelijkheid is van de juistheid van het betreffende gegeven. Vragen die hierbij kunnen helpen zijn de volgende:

* Hoe erg is het als er fouten of ongeautoriseerde wijziging van de gegevens plaats heeft gevonden?
  + Kunnen er datalekken optreden door fouten in de gegevens (bv fouten in adresgegevens)?
* Kunnen personen negatieve gevolgen ondervinden wanneer de gegevens niet correct zijn?
* Kan er fraude plaatsvinden (denk aan onterechte toekenning van uitkering, ongeautoriseerde financiële transactie) door fouten in de gegevens of ongeautoriseerde wijziging van de gegevens?
* Leiden fouten of ongeautoriseerde wijzigingen tot imagoverlies? Wordt de minister van SZW daarop door de politiek/media aangesproken?
* Zijn er contractuele of wettelijke verplichtingen voor de integriteit van de gegevens? Als het om persoonsgegevens gaat, denk dan aan de eisen van de AVG.
  + 1. Stroomschema integriteitsclassificatie



1. Vertrouwelijkheid
   1. Wat is vertrouwelijkheid?

Het principe van vertrouwelijkheid wordt gebaseerd op de mogelijke gevolgen wanneer de gegevens in handen komt van onbevoegde derden (derden die hiervoor niet zijn geautoriseerd). Hoe gevoeliger de gegevens, hoe groter de gevolgen kunnen zijn. Deze gevoeligheid kan betrekking hebben op privacybelangen (dit is het geval bij persoonsgegevens) of op organisatiebelangen.

Door te classificeren wordt een onderscheid gemaakt in de mate van vertrouwelijkheid. De vertrouwelijkheidsklasse is daarmee één van de factoren om te bepalen wat de juiste technische en organisatorische maatregelen zijn om gegevens te beschermen. Passende beveiliging betekent in de context van vertrouwelijkheid dat deze waarborgt dat alleen personen die daarvoor zijn geautoriseerd toegang krijgen tot de gegevens.

Voor een aantal categorieën van gegevens hangt de classificatie nauw samen met toepasselijke wetgeving. Zo geldt dat de AVG een duidelijk onderscheid maakt tussen ‘gewone’ persoonsgegevens en persoonsgegevens die extra gevoelig zijn en daarom extra beschermd moeten worden. Deze extra gevoelige persoonsgegevens zijn

1. bijzondere persoonsgegevens genoemd in artikel 9 AVG[[1]](#footnote-1);
2. persoonsgegevens van strafrechtelijke aard genoemd in artikel 10 AVG[[2]](#footnote-2);
3. het BSN.

Maar ook wetgeving op het terrein van het medisch beroepsgeheim (Wet BIG) leidt ertoe dat bijvoorbeeld gezondheidsgegevens over een patiënt die verwerkt worden door een arts, onder de hoogste vertrouwelijkheidsklasse vallen.

De vertrouwelijkheidsklasse is context gebonden. Ten aanzien van persoonsgegevens zegt een enkel gegeven bijvoorbeeld meestal niet zoveel over een persoon. Echter, wanneer gegevens worden gecombineerd kunnen deze niet alleen de herleidbaarheid tot een individuele persoon vergroten, maar ook een grotere inbreuk op de privacy van die betrokkene betekenen. Een postcode en een geboortedatum zeggen op zichzelf niet veel, maar kunnen in een kleine gemeente al leiden naar een individu, gecombineerd met een ziekmelding of een afspraak met een arts wordt dit zeer privacygevoelig. Hetzelfde geldt voor andere gevoelige gegevens zoals bepaalde bedrijfsgegevens en bijvoorbeeld securitygegevens. Daarom bepalen we de vertrouwelijkheidsklasse niet op het niveau van een enkel gegeven, maar op het niveau van een groep gegevens (ook wel ‘entiteit’ genoemd).

* 1. Welke vertrouwelijkheidsniveaus onderscheiden we?

Binnen UWV onderscheiden we vijf niveaus van vertrouwelijkheid. Deze zijn:

|  |  |  |
| --- | --- | --- |
| **Klasse** | **Omschrijving** | **Toelichting** |
| V-0 | Openbaar | Alle gegevens die algemeen toegankelijk zijn voor iedereen. Schending van de vertrouwelijkheid van de gegevens in deze classificatie is niet mogelijk.  Voorbeelden:   * Brochures die voor het brede publiek beschikbaar zijn. * Informatie op het openbare gedeelte van UWV.nl en Werk.nl. * Informatie die UWV deelt op de openbare sociaal media accounts van UWV. |
| V-1 | Bedrijfsvertrouwelijk | Gegevens die niet bedoeld zijn voor het brede publiek, maar wel toegankelijk mogen of moeten voor alle of een zeer brede groep medewerkers van UWV. De vertrouwelijkheid is gering. Schending van de vertrouwelijkheid van de gegevens in deze classificatie kan enige (in)directe schade toebrengen.  Voorbeelden:   * UWV interne richtlijnen, procedures en werkinstructies. * Informatie op de Digitale Werkplek UWV. * Verslagen van interne overleggen, zoals van een afdelingsoverleg. |
| V-2 | Vertrouwelijk | Gegevens die vertrouwelijk zijn en in principe alleen beschikbaar worden gesteld aan medewerkers die deze nodig hebben voor hun taken. Schending van de vertrouwelijkheid van de gegevens in deze classificatie kan schade opleveren voor UWV en voor betrokkene. Wanneer het om persoonsgegevens gaat, kan schending leiden tot een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens en mogelijk ook aan de betrokkene. **Deze vertrouwelijkheidsklasse geldt voor de meeste gegevens die UWV verwerkt.**  Hieronder vallen:   * Alle reguliere persoonsgegevens (geen bijzondere persoonsgegevens zoals beschreven in art 9 AVG of strafrechtelijke gegevens zoals beschreven in art 10 AVG). Waaronder onder andere:   + Personeelsdossiers van UWV, salarisstroken en personeelsbeoordelingen   + NAW, puikcodes, op naam gestelde e-mailadressen en telefoonnummers van medewerkers UWV * BSN * Interne vertrouwelijke stukken, zoals verslagen van de RvB * Aanbestedingsdocumentatie * Strategische beleidsdocumenten * Securitygegevens |
| V-2+ | Extra vertrouwelijk | Gevoelige gegevens die alleen toegankelijk mogen zijn voor een (zeer) beperkte groep gebruikers. Gaat o.a. om persoonsgegevens die op grond van de AVG extra moeten worden beschermd. Schending van de vertrouwelijkheid van de gegevens in deze classificatie kan serieuze (in)directe schade toebrengen aan UWV en de betrokkene.  Hieronder vallen:   * Gezondheidsgegevens die geen medische gegevens betreffen, zoals (niet limitatief)   + De indicatie WIA, Wajong, WGA, WAO, WAZO;   + AO-klasse of arbeidsgeschiktheidspercentage;   + Arbeidshandicap;   + Joboach (irt een klant);   + Verstandelijke beperking;   + Auditieve beperking;   + Sociale beperking;   + Motorieke beperking;   + Voorziening;   + Banenafspraak (in de context van UWV);   + gegevens betreffende ziekteverzuim en ziektedagen (als deze niets over de aandoening prijsgeven). * Alle andere bijzondere persoonsgegevens (zie artikel 9 AVG), zoals bijvoorbeeld   + persoonsgegevens betreffende seksuele geaardheid, etnische achtergrond, politieke voorkeur etc.   + foto’s als deze worden gebruikt voor unieke identificatie. * Persoonsgegevens van strafrechtelijke aard (zie artikel 10 AVG), zoals bijvoorbeeld   + Indicatie detentie   + Contact met politie/justitie   + Afwijzing VOG * Persoonsgegevens over opgelegde maatregelen n.a.v. bestuursrechtelijke overtredingen, zoals   + Opgelegde maatregelen en boetes (ihkv) de uitkering. * Persoonsgegevens m.b.t. eigen personeel die in de dienstverlening worden gebruikt (situatie personeel wordt klant), voor zover het geen medische gegevens betreft en geen gegevens betreft mbt een ingesteld onderzoek door HH, BI, een toezichthouder, de politie of de Belastingdienst (in die gevallen is V-3 van toepassing). |
| V-3 | Strikt vertrouwelijk | Dit betreft zeer gevoelige gegevens die alleen toegankelijk mogen zijn voor de direct geadresseerde of een zeer kleine, vooraf gedefinieerde groep gebruikers. Schending van de vertrouwelijkheid van de gegevens in deze classificatie kan (in)direct zeer grote (politieke) schade toebrengen.  Hieronder vallen:   * Medische gegevens, waaronder medische gegevens die vallen onder het medisch beroepsgeheim, zoals   + diagnoses en rapporten van behandelend artsen en andere zorgverleners;   + Aard van een aandoening/ziektebeeld. * Biometrische gegevens voor unieke identificatie, zoals   + Vingerafdruk;   + Irisscan. * Genetische gegevens, zoals   + DNA-profiel * Gegevens met betrekking tot een onderzoek dat naar een persoon is ingesteld - bijvoorbeeld in verband met mogelijke fraude - door de directie Handhaving, Bureau Integriteit, een andere toezichthouder, de politie of de Belastingdienst. * Reden van een veroordeling. * De indicatiestelling VIP. |

* 1. Gezondheidsgegevens en medisch beroepsgeheim

Het begrip ‘gezondheidsgegevens’ is een breed begrip en omvat alle gegevens die verband houden met de lichamelijke of geestelijke gezondheid van een persoon. Het gaat daarbij zowel om echt medische gegevens zoals een diagnose van een arts of de uitslag van een bloedonderzoek, als om meer administratieve gegevens zoals het feit dat iemand een WIA-uitkering heeft of een afspraak heeft met een verloskundige. Alle gezondheidsgegevens gelden onder de AVG als ‘bijzondere persoonsgegevens’ (artikel 9 AVG) en worden daarom minimaal in Vertrouwelijkheidsklasse 2+ ingedeeld. Sommige gezondheidsgegevens zijn echter gevoeliger dan andere gezondheidsgegevens en moeten vanwege hun gevoelige aard extra beschermd worden. Deze kunnen daarom in klasse 3 vallen. Onder de zwaardere klasse 3 vallen bijvoorbeeld gezondheidsgegevens die aan een arts uit hoofde van zijn beroep zijn toevertrouwd. Deze gezondheidsgegevens vallen onder het medisch beroepsgeheim en worden binnen UWV vaak ‘medische gegevens’ genoemd. Dit geldt ook voor gegevens die weliswaar niet aan de arts zelf zijn toevertrouwd (de klant beschikt er bijvoorbeeld zelf over en is bereid deze gegevens zelf te verstrekken) maar die vanwege hun aard normaliter onderdeel uitmaken van een medisch dossier. Denk hierbij aan een diagnoserapport of röntgenfoto’s.

* 1. Wie is verantwoordelijk voor het classificeren en het bepalen van het juiste vertrouwelijkheidsniveau?

De verantwoordelijkheid voor het classificeren van de vertrouwelijkheid ligt bij de gegevenseigenaar. Dit is de directie van het organisatieonderdeel dat verantwoordelijk is voor de bepaling en het beheer van de gegevensbeschrijving (gegevens en gegevensgroepen/entiteiten) en/of het beheer van en de sturing op de gegevenswaarde. De uitvoering van de classificatie gebeurt (door verschillende functionarissen) onder regie van de Gegevensmanager.

De vertrouwelijkheidsklasse wordt vastgelegd in het Functioneel Gegevens Model (FUGEM). Dit is een overzicht van alle gegevens die door een informatiesysteem gaan. Het is daarmee een belangrijke bron van informatie voor (risico) analyses in het voortbrengingsproces.

Naast de vastlegging van vertrouwelijkheidsklasse op het niveau van entiteiten in de FUGEM, wordt bij UWV ook op het niveau van informatiesystemen een vertrouwelijkheidsklasse vastgelegd. Dit gebeurt in de RAL, die minimaal jaarlijks wordt herijkt.

* 1. Gebruik van vertrouwelijkheidsklassen

Wanneer voor een bepaald bestand of systeem een uitspraak moet worden gedaan over de vertrouwelijkheid van het geheel aan gegevens van dat bestand of systeem (bijvoorbeeld bij een gegevenslevering, bij het vaststellen van de Risico Applicatie Lijst of bij een Gegevensbeschermingseffectbeoordeling), dan wordt het FUGEM geraadpleegd. De vertrouwelijkheid is dan gelijk aan de hoogste vertrouwelijkheidsklasse van de onderliggende entiteiten.

Het is daarbij van belang om een onderscheid te maken tussen classificatie, risico’s en maatregelen. In een bredere risicoanalyse kan blijken dat vanwege andere factoren (zoals de omvang van het betreffende bestand of een externe koppeling) een groter risico bestaat dan de vertrouwelijkheidsklasse van de onderliggende gegevens lijkt te suggereren. Het is dan niet de bedoeling om de vertrouwelijkheidsklasse bij te stellen, maar uiteraard wel om de maatregelen op de feitelijke situatie te baseren zodat het bestand voldoende is beveiligd.

Bij vragen over de juiste vertrouwelijkheidsklasse van gegevens is het aan te raden om de Gegevensmanager en BSO van het eigen organisatieonderdeel te raadplegen.

* 1. Instructie vertrouwelijkheidsclassificatie

Binnen UWV wordt veel met persoonsgegevens gewerkt en voor de meeste gegevensgroepen geldt dan ook minimaal V-klasse 2. Een snelle manier om de vertrouwelijkheidsklasse te bepalen is dan ook om uit te gaan van deze baseline en te kijken of de gegevensgroep hier van afwijkt. Dit kan een afwijking naar een lager niveau inhouden (er zijn bijvoorbeeld geen persoonsgegevens in opgenomen) of naar een hoger niveau (er zijn extra gevoelige gegevens zoals gezondheidsgegevens of strafrechtelijke gegevens in opgenomen). Omdat er sprake is van twee classificatieniveaus voor extra gevoelige gegevens, moet in dit laatste geval daarna nog een zorgvuldige afweging worden gemaakt van welke V-klasse aan de orde is.

Aanvullende richtlijnen:

* Vertrouwelijkheidsklasse 3 zal voornamelijk van toepassing zijn bij gegevens van SMZ, die onder het beroepsgeheim van de arts vallen en bij personen naar wie een strafrechtelijk onderzoek loopt.
* Bij twijfel over de juiste vertrouwelijkheidsklasse raadpleeg de Gegevensmanager en/of de BSO of coördinator IB&P.
* Neem bij wijzigingen in het proces of systeem die mogelijk gevolgen hebben voor de gegevensgroepen en hun vertrouwelijkheidsklasse contact op met de Gegevensmanager zodat de FUGEM en de indeling in vertrouwelijkheidsklassen juist en actueel blijft.
  + 1. Stroomschema’s vertrouwelijkheidsclassificatie

Start

ja

**Gaat het om persoonsgegevens?**

nee

**V-2+**

**Gaat het om zeer gevoelige gegevens zoals medische gegevens, gegevens van VIPs of gegevens over personen naar wie een onderzoek is afgesteld?**

**Gaat het om bijzondere persoonsgegevens (art. 9 AVG) of gegevens van strafrechtelijke aard (art. 10 AVG)?**

**Gaat het om bedrijfsgegevens?**

ja

**Gegevens worden niet geclassificeerd.**

Voorbeeld:

* Parameters

**V-2**

nee

ja

nee

ja

**V-3**

Voorbeelden V-2:

* Uitkeringsgegevens van een klant in het kader van een wet die niet is gerelateerd aan gezondheid (bijvoorbeeld WW)
* Gegevens over arbeidsbemiddeling van klanten (waar het geen bijzondere persoonsgegevens betreft)
* BSN
* Personeelsdossiers van UWV (waar het geen bijzondere persoonsgegevens betreft)

Voorbeeld V-2+:

* AO-klasse
* Gegevens betreffende ziekteverzuim en ziektedagen
* Persoonsgegevens over boetes of schorsing van de uitkering.

Voorbeeld V-3:

* Medische gegevens, waaronder medische gegevens die vallen onder het medisch beroepsgeheim, zoals diagnoses en rapporten van behandelend artsen en andere zorgverleners.
* Gegevens over personen naar wie een onderzoek is ingesteld - bijvoorbeeld in verband met mogelijke fraude - door de directie Handhaving, Bureau Integriteit, een andere toezichthouder, de politie of de Belastingdienst.
* Gegevens van personen met de indicatiestelling VIP

nee

**Gaat het om openbare bedrijfsgegevens?**

**V-0**

Voorbeelden V-0:

* Brochures die voor het brede publiek beschikbaar zijn.
* Informatie op het openbare gedeelte van UWV.nl en Werk.nl.
* Informatie die UWV deelt op de openbare social media accounts van UWV.

ja

**Leidt ongeautoriseerde onthulling tot noemenswaardige schade?**

nee

**V-1**

Voorbeelden V-1:

* UWV interne richtlijnen, procedures en werkinstructies.
* Informatie op de Digitale Werkplek UWV.
* Verslagen van interne overleggen, zoals van een afdelingsoverleg.

nee

**Gaat het om gegevens die onderdeel uitmaken van fraudemeldingen**

ja

**V-2**

Voorbeelden V-2:

* Interne vertrouwelijke stukken, zoals verslagen van de RvB
* Aanbestedingsdocumentatie
* Strategische beleidsdocumenten
* Securitygegevens

nee

**Gaat het om strikt vertrouwelijke gegevens of zeer gevoelige gegevens waar geheimhouding op rust of om gegevens van bedrijven waar een onderzoek naar is ingesteld in verband met een mogelijke wetsovertreding.**

ja

**V-3**

nee

Voorbeelden V-3:

* Bedrijfsgegevens in verband met onderzoeken naar mogelijke fraude - door de directie Handhaving, Bureau Integriteit, een andere toezichthouder, de politie of de Belastingdienst.

ja

1. Relatie met andere classificatiesystemen

De BIV-classificatie die UWV hanteert is niet universeel. De indeling sluit aan bij het soort gegevens dat UWV verwerkt en is op de interne bedrijfsvoering gericht. Buiten UWV zijn diverse andere BIV-classificatie indelingen in omloop.

UWV kiest bewust voor een eigen indeling van de BIV-classificatie omdat daarmee kan worden aangesloten bij de praktijk van UWV en het type gegevens dat daar in wordt verwerkt. UWV verwerkt bijvoorbeeld veel gevoelige (persoons)gegevens. Door de vertrouwelijkheidsklasse verder te differentiëren wordt het mogelijk om nog gerichter inzicht te hebben in de waarde van deze gegevens en kunnen maatregelen nog gerichter op deze te beschermen waarde worden afgestemd.

Dit wordt ook in het kader van de AVG van UWV verlangd – de AVG vraagt om *passende* beveiliging van persoonsgegevens waarbij bijzondere persoonsgegevens extra worden beschermd. Door de vertrouwelijkheidsklasse van gegevens verder te differentiëren kunnen bijzondere persoonsgegevens met een hogere vertrouwelijkheidsklasse geoormerkt worden zodat duidelijk is waar deze zich bevinden en kan de beveiliging hier op worden afgestemd.

Hoewel de classificatie van UWV niet universeel is, sluit deze wel aan bij de omgeving. In de handreiking *‘Betrouwbaarheidsniveaus voor digitale dienstverlening’* van Forum Standaardisatie (versie 4) wordt bij de uitsplitsing van betrouwbaarheidsniveau op basis van de aard van de gegevens eveneens een onderscheid gemaakt tussen persoonsgegevens met een verhoogd risico, waaronder bijzondere persoonsgegevens worden geschaard, en persoonsgegevens met een hoog risico, waaronder wordt gerefereerd aan gegevens waar een wettelijk bepaalde geheimhoudingsplicht op rust, zoals medische gegevens. Ook de *‘Concept Ministriele Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening’* ziet dit onderscheid. In de tabel ‘criteria betrouwbaarheidsniveaus’ wordt onderscheid gemaakt tussen bijzondere en strafrechtelijke gegevens enerzijds (niveau ‘substantieel’) en persoonsgegevens die nog gevoeliger zijn omdat zij stigmatiserend kunnen werken (niveau ‘hoog’).

* 1. BIO

De Baseline Informatiebeveiliging Overheid (BIO) betreft een gemeenschappelijk

normenkader voor de beveiliging van de informatie en informatiesystemen van de overheid. Ook UWV is aan de BIO gehouden. De normen van de BIO, en het beleid en de richtlijnen waar deze normen in zijn uitgewerkt, maken daarom onderdeel uit van de beveiligingseisen die aan verwerkingen bij UWV worden gesteld.

Ook het BIO normenkader kent een onderscheid in klassen. Het gaat hier echter niet om de classificatie van gegevens, maar om een onderscheid in de mate waarin informatiesystemen moeten worden beschermd. De BIO onderscheidt drie basis beveiligingsniveaus (BBN). Elk beveiligingsniveau geeft een indicatie van welke maatregelen voor een bepaald informatiesysteem minimaal zouden moeten worden getroffen.

Elk beveiligingsniveau geeft daartoe een aantal verplichte overheidsmaatregelen en een aantal controls (beveiligingsnormen) weer, als ook een verantwoordings- en toezichtregime[[3]](#footnote-3).

* BBN 1 geldt voor die informatiesystemen waarvoor BBN 2 als te zwaar wordt gezien. Het is het niveau waar alle overheidssystemen minimaal aan moeten voldoen, een ‘bare minimum’.
* BBN 2 is de baseline voor informatiesystemen binnen de overheid. Deze baseline geldt voor alle informatiesystemen die vertrouwelijke informatie verwerken. Ook voor UWV geldt dat vrijwel alle informatiesystemen van UWV binnen de kaders van de BIO in BBN 2 vallen.
* BBN 3 geldt voor informatiesystemen met Departementaal vertrouwelijke informatie (of vergelijkbaar vertrouwelijk) die beschermd moeten worden tegen statelijke actoren en beroepscriminelen. Dit is niet hetzelfde als systemen waarin gegevens worden verwerkt die in vertrouwelijkheidsklasse 3 worden ingedeeld. Het gaat hier om informatie die door statelijke actoren worden bedreigd.

De BIO gaat uit van risicogebaseerd beveiligen en betrekt hierin het gewicht van de te beschermen belangen in combinatie met relevante dreigingen. Het gewicht van de te beschermen belangen heeft een relatie met BIV-classificatie: een hogere BIV-classificatie betekent een groter te beschermen belang. De BIV-classificatie heeft daarom invloed op welk beveiligingsniveau van de BIO van toepassing is. De BIV-classificatie kan echter niet één op één vertaald worden naar BBN omdat de BIV-classificatie slechts één onderdeel is van het gehele stelsel van risicoanalyse, beveiligingseisen en maatregelen (zie ook paragraaf 2.3). In de praktijk komt het er op neer dat vrijwel alle verwerkingen met persoonsgegevens bij UWV onder BBN 2 vallen – dit is dan ook de baseline bij UWV en andere overheidsorganisaties.

* 1. Classificatie indelingen buiten UWV

Omdat buiten UWV andere BIV-classificatie indelingen worden gehanteerd is het van belang om hier in de samenwerking met andere partijen (ketenpartners, partijen aan wie UWV gegevens levert of van wie UWV gegevens ontvangt of bij andere samenwerkingsvormen) alert op te zijn.

In de praktijk zal het in het gesprek met partners eerder over de beveiligingseisen gaan die aan de verwerking worden gesteld en de maatregelen die daartoe moeten worden getroffen, dan over de BIV-classificatie an sich. Dit bepaalt immers wat er feitelijk gedaan moet worden en welke waarborgen moeten worden geboden. Deze beveiligigingseisen worden breder toegepast en vormen daarmee een gemeenschappelijke taal met ketenpartners. Het is voldoende om intern de relatie te kunnen leggen tussen de BIV-classificatie en de classificatieniveaus van verschillende beveiligingseisen.

K&S heeft in het document *Instructie toekennen betrouwbaarheidsniveaus voor digitale diensten op basis van eIdas[[4]](#footnote-4)* bijvoorbeeld een vertaling gemaakt van BIV-classificatie UWV naar de eIdas betrouwbaarheidsniveaus die worden toegepast bij de beveiliging van digitale diensten.

In dit document is ook te lezen dat stelsels als eIdas, eHerkenning en DigiD elk hun eigen classificatie van betrouwbaarheidsniveaus kennen. Ook deze zijn dus niet universeel, maar via transponeringstabellen wel op elkaar te laten aansluiten.

1. Dit zijn bijvoorbeeld gezondheidsgegevens of gegevens over iemands levensovertuiging of religie. Zie voor een volledig overzicht van bijzondere persoonsgegevens het UWV Beleidskader Privacy. [↑](#footnote-ref-1)
2. Dit zijn bijvoorbeeld gegevens dat een persoon in detentie zit of strafrechtelijk is veroordeeld. [↑](#footnote-ref-2)
3. BIO versie 1.03 [↑](#footnote-ref-3)
4. Instructie toekennen betrouwbaarheidsniveaus voor digitale diensten op basis van eIdas. Versie 2.02 dd 12-02-2019 [↑](#footnote-ref-4)