**Risicoanalyse en beheersmaatregelen privacy en security aspecten doorstroommonitor**

1. **Doelstelling doorstroommonitor**

Het doel van de uitwisseling van gegevens over doorstroom naar vervolgonderwijs is om:

* 1. sectororganisaties en onderwijsinstellingen in staat te stellen de kwaliteit van het onderwijs op sectoraal- en instellingsniveau te verbeteren;
	2. instellingen in staat te stellen zich op een efficiënte wijze te kunnen verantwoorden over de kwaliteit van het onderwijs naar het ministerie van OCW (Inspectie) en/of andere stakeholders.
1. **Uitgangspunt borging privacy**

Uitgangspunt voor de gegevensverwerking in het kader van de doorstroommonitor is dat deze geen persoonsgegevens bevat.

1. **Risico’s en beheersmaatregelen in de keten**

Onderstaande inventarisatie van risico’s en beheersmaatregelen zijn gebaseerd op het eerder uitgevoerde onderzoek *Doorstroominformatie georganiseerd, juridische aspecten van de doorstroommonitor, januari 2013* en op het privacybeleid van het ministerie van OCW.

De keten van gegevensuitwisseling in het kader van de doorstroommonitor bestaat uit een aantal (mogelijke) schakels:

I. DUO

II. Sectororganisatie

II. Sectororganisatie

III. Bewerker

IV. Derden

(openbaar)

V. Onderwijsinstelling (niet openbaar)

V. Onderwijsinstelling (niet openbaar)

IV. Derden (openbaar)

Toelichting:

1. Op basis van het Specificatierapport en het 1Cijferbestand stelt DUO per sectorovergang een gegevensbestand (kubus) op. Dit bestand bevat geen persoonsgevens. De kubus is opgebouwd uit cohorten: het aantal studenten met dezelfde doorstroomkenmerken (voorbeeld: het aantal studenten dat twee jaar geleden van opleiding A van instelling B is doorgestroomd naar opleiding X van instelling Y). Op dit niveau is er geen risico dat gegevens verwerkt worden tot persoonsgegevens. DUO stelt (de) kubus(sen), via een beveiligde website en onder voorwaarden, enkel beschikbaar aan specifieke medewerker(s) van de betreffende sectororganisatie, zodat derden geen toegang hebben tot gegevens. De voorwaarden zien er op dat sectororganisaties de kubus(sen) op een beveiligde omgeving bewaren die enkel toegankelijk is voor aangewezen medewerkers en dat gegevens enkel gebruikt worden voor het aangegeven doel.
2. Sectororganisaties ontvangen de kubus(sen) voor zover deze betrekking heeft/hebben op overgangen van hun sector naar vervolgonderwijs en verwerken deze. Deze bestanden bevatten geen persoonsgegevens. Het risico dat sectororganisaties de gegevens zonder onevenredige inspanning kunnen verwerken tot persoonsgegevens is zeer klein. Ook de impact is zeer klein. Door gegevens te verwerken op een beveiligde omgeving door enkel aangewezen medewerkers hebben derden geen toegang tot de doorstroomgegevens.
3. Enkele sectororganisaties besteden de verwerking van de Kubus(sen) tot openbare informatieproducten en/of niet openbare informatieproducten voor individuele onderwijsinstellingen uit aan een bewerker. Als beheersmaatregel sluiten sectororganisatie en bewerker een bewerkersovereenkomst af met voorwaarden waaronder de bewerker de kubus(sen) mag verwerken, zodat gegevens niet verwerkt worden tot persoonsgegevens en derden geen toegang hebben tot gegevens. Voor het opstellen van informatieproducten door de bewerker zijn dezelfde beheersmaatregelen van toepassing zoals onder II aangegeven.
4. Een aantal sectororganisaties verwerken doorstroomgegevens zelf tot openbare informatieproducten om op sectorniveau trends in de overgang naar vervolgonderwijs voor derden inzichtelijk te maken. De kans dat derden gegevens uit deze publicaties zonder onevenredige inspanning kunnen verwerken tot persoonsgegevens is zeer klein. De mogelijke impact van herkenning is wel groter. Daarom wordt, als beheersmaatregel om evt. herkenning te voorkómen, in het informatieproduct een ondergrens gehanteerd voor het aantal studenten dat behoort tot een cohort met bepaalde doorstroomkenmerken. Als dit aantal kleiner is dan 5, wordt het symbool ‘<5’ vermeld.
5. Een aantal sectororganisaties verwerken de van DUO ontvangen kubus(sen) tot niet openbare informatieproducten om deze vervolgens aan individuele onderwijsinstellingen te leveren c.g. voor individuele onderwijsinstellingen te ontsluiten. De kans dat onderwijsinstellingen gegevens uit deze informatieproducten zonder onevenredige inspanning kunnen verwerken tot persoonsgegevens is groot. De mogelijke impact van herkenning is klein (de onderwijsinstelling heeft geen reden het belang van de oud-leerling te schaden). Gelet echter op de kans op verwerking tot persoonsgegevens, wordt ook hier de beheersmaatregel gehanteerd dat de sectororganisatie voor het samenstellen van het informatieproduct een ondergrens hanteert voor het aantal studenten dat behoort tot een cohort met bepaalde doorstroomkenmerken. Als dit aantal kleiner is dan 5, wordt het symbool ‘<5’ vermeld.

Ministerie van OCW en sectororganisaties stellen vast dat voorgaande beheersmaatregel er toe kan leiden dat een aanzienlijk deel van de gegevens uit de doorstroommonitor niet ontsloten kunnen worden voor individuele onderwijsinstellingen, omdat deze anders aangemerkt kunnen worden als persoonsgegevens.

In onderstaande tabel zijn alle beheersmaatregelen uitgewerkt:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr. | (Mogelijke) verwerkingsmomenten in de keten | Risico op verwerking (tot) persoonsgegevens | Kans | Impact | Beheersmaatregelen |
| 1 | Opstellen specificatierapport | nihil | nihil | nihil | Uitgangspunt voor Specificatierapport is dat kubussen geen (bijzondere) persoonsgegevens of nummer ter identificatie omvat. |
| 2 | Verwerking gegevens tot kubussen door DUO | nihil | nihil | nihil | Kubussen bevatten geen (bijzondere) persoonsgegevens of nummer ter identificatie. Ook geen om-nummer. Gegevens geaggregeerd per cohort doorstromers met bepaalde kenmerken. |
| 3 | Levering van kubussen door DUO aan sectororganisaties | Identificatie van individu door sectororganisatie zonder onevenredige inspanning | Zeer klein | Zeer klein | Kubussen worden door DUO aan sectororganisaties beschikbaar gesteld onder voorwaarde dat:* deze enkel voor het aangegeven doel verwerkt worden.
* verwerking plaatsvindt op afgeschermde server door aangewezen personen.
 |
|  |  | Identificatie van individu door derde zonder onevenredige inspanning | Zeer klein | Middel | Kubussen worden door DUO via een beveiligde website enkel aan aangewezen personen van betreffende sectororganisaties (met inlogcode) beschikbaar gesteld, waardoor derden geen toegang hebben tot kubussen.  |
| 4 | Verwerken van kubussen door sectororganisaties  | Identificatie van individu door sectororganisatie zonder onevenredige inspanning | Zeer klein | Zeer klein | Verwerking van gegevens door sectorraad vindt plaats op afgeschermde server door aangewezen personen. |
|  |  | Identificatie van individu door derde zonder onevenredige inspanning | Zeer klein | Middel | Verwerking van gegevens door sectorraad vindt plaats op afgeschermde server door aangewezen personen, waardoor derden geen toegang hebben tot kubussen.  |
| 5 | Openbaar maken van informatieproducten door sectororganisaties | Identificatie van individu door onderwijsinstelling zonder onevenredige inspanning | Zeer klein | Klein | Indien bepaald doorstroomcohort bestaat uit minder dan 5 leerlingen wordt in het informatieproduct ‘<5’ vermeld. |
|  |  | Identificatie van individu door derde zonder onevenredige inspanning | Zeer klein | Middel | Indien bepaald doorstroomcohort bestaat uit minder dan 5 leerlingen wordt in het informatieproduct ‘<5’ vermeld. |
| 6 | Levering/ontsluiting van niet openbare informatieproducten door sectororganisaties aan/voor onderwijsinstellingen | Identificatie van individu door onderwijsinstelling zonder onevenredige inspanning | Groot | Klein | Indien bepaald doorstroomcohort bestaat uit minder dan 5 leerlingen wordt in het informatieproduct ‘<5’ vermeld. |
|  |  | Identificatie van individu door derde zonder onevenredige inspanning | Zeer klein | Middel | Indien bepaald doorstroomcohort bestaat uit minder dan 5 leerlingen wordt in het informatieproduct ‘<5’ vermeld. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 7 | Uitbesteding en levering van kubussen door sectororganisatie aan bewerker  | Identificatie van individu door verwerker zonder onevenredige inspanning | Klein | Klein | Sectororganisatie sluit met bewerker overeenkomst met o.a. de volgende voorwaarden:Kubussen:* worden enkel voor het aangegeven doel verwerkt.
* verwerking vindt plaats op afgeschermde server door aangewezen personen
 |
|  |  | Identificatie van individu door derde zonder onevenredige inspanning | Zeer klein | Middel | Kubussen worden door sectororganisatie via een beveiligde wijze enkel aan aangewezen personen van betreffende bewerker beschikbaar gesteld. (Derden hebben zo geen toegang tot kubussen). |
| 8 | Verwerken van kubussen door bewerker tot openbare informatieproducten | Identificatie van individu door onderwijsinstelling zonder onevenredige inspanning | Middel | Klein | Indien bepaald doorstroomcohort bestaat uit minder dan 5 leerlingen wordt in het informatieproduct ‘<5’ vermeld. |
|  |  | Identificatie van individu door derde zonder onevenredige inspanning | Zeer klein | Middel | Indien bepaald doorstroomcohort bestaat uit minder dan 5 leerlingen wordt in het informatieproduct ‘<5’ vermeld. |
| 9 | Verwerken van kubussen door bewerker voor levering/ontsluiting van niet openbare informatieproducten voor onderwijsinstellingen. | Identificatie van individu door onderwijsinstelling zonder onevenredige inspanning | Groot | Klein | Indien bepaald doorstroomcohort bestaat uit minder dan 5 leerlingen wordt in het informatieproduct ‘<5’ vermeld. |
|  |  | Identificatie van individu door derde zonder onevenredige inspanning | Zeer klein | Middel | Indien bepaald doorstroomcohort bestaat uit minder dan 5 leerlingen wordt in het informatieproduct ‘<5’ vermeld. |
| 10 | Gebruik van niet openbare gegevens door onderwijsinstellingen | Identificatie van individu door onderwijsinstelling zonder onevenredige inspanning | Groot | Klein | Onderwijsinstellingen krijgen enkel de beschikking over informatieproducten waarin doorstroomcohorten die bestaan uit minder dan 5 leerlingen zijn aangeduid met het symbool ‘<5’. |