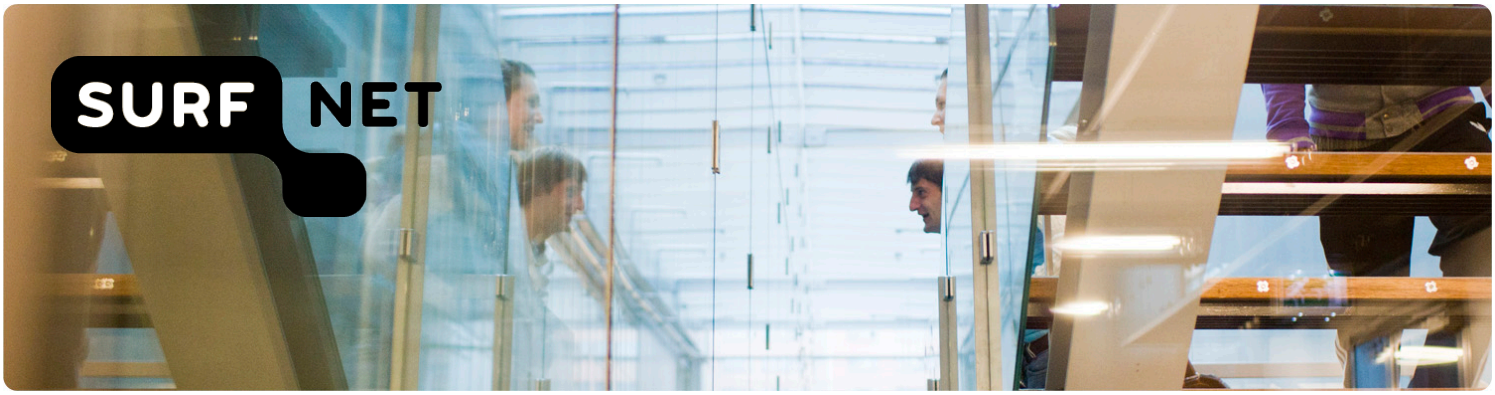

BIV-classificatie veel voorkomende verwerkingen van persoonsgegevens

Auteur(s): Martin Romijn

Versie: 1.0

Datum: 8 mei 2015

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
admin@surfnet.nl
www.surfnet.nl

ING Bank NL54INGB0005936709
KvK Utrecht 30090777
BTW NL 0089.60.173.B01

Inhoud

Inleiding

SURF constateert binnen de community de behoefte aan een BIV-classificatie voor verwerkingen van persoonsgegevens conform de methode voor BIV-classificatie van informatie zoals dat vanuit informatiebeveiliging gebeurt. Uitgangspunt is dat instellingen veelal met dezelfde dreigingen te maken hebben, hetgeen ook blijkt uit het recente door SURF gepubliceerde rapport “Cyberdreigingsbeeld in het Hoger Onderwijs”. Verder zijn de primaire processen binnen het Hoger Onderwijs over het algemeen in grote lijnen identiek.

In opdracht van SURFnet heeft Martin Romijn een tabel met veelvoorkomende verwerkingen van persoonsgegevens inclusief BIV-codes opgesteld. Peter Oost (CISO Erasmus Universiteit) en Chloë Baartmans (Project Manager Voorbereiding Implementatie Algemene Verordening Gegevensbescherming SURFnet) hebben daarbij in de rol van meelezer bijgedragen aan het resultaat.

Veel voorkomende verwerkingen van persoonsgegevens

De Hoger Onderwijs Referentie Architectuur (HORA) biedt onder meer een lijst applicaties en een lijst bedrijfsobjecten. Aan deze objecten is vanuit de HORA een BIV-classificatie toegekend, daarbij is per applicatie aangegeven welke objecten beheerd dan wel benaderd worden. Het Vrijstellingsbesluit Wbp bevat een overzicht van verwerkingen die in de meeste organisaties plaatsvinden. In onderstaande tabel zijn verwerkingen in de het kader van de Wbp gerelateerd aan de applicaties vanuit de HORA. Via de objecten die betrokken zijn bij de meest voorkomende verwerkingen zijn BIV-classificaties afgeleid.

Uit ervaring blijkt dat het Hoger Onderwijs 25 meest voorkomende verwerkingen kent. Deze zijn, met de afgeleide BIV-classificatie, in onderstaande tabel opgenomen. De BIV-classificatie is niet altijd uit de HORA af te leiden, dan wordt een suggestie gedaan. Er zijn situaties denkbaar waarin de BIV-classificatie kan afwijken van de suggestie, dan wordt dat in de kolom “Applicatie” vermeld. Ook zullen specifieke situaties per instelling leiden tot een andere BIV-classificatie. De uiteindelijke classificatie is een besluit van de instelling.

Nr.	Verwerking	Applicatie	Beheert objecten	BIV object	BIV verwerking
1.	Alumni gegevens	Bedrijfsvoering Komt voor als verwerking van instelling zelf en ook bij alumnivereenigingen.	Alumnus	MHM/ MHH	MHM
2.	Betaalsystemen	Betaalsystemen	Als financieel systeem		MMM
3.	Camera toezicht	Onderwijs Facilitair systeem	Leermateriaal ”Persoonsbeelden” (beveiliging)	MMM -	HMH
4.	Deelnemers sportfaciliteiten	Niet in HORA aanwezig	Deels naar analogie toegangssysteem.		MMM
5.	Digitaal toetssysteem	Onderwijs	Toetsmateriaal	HHH	HHH
6.	Diverse onderzoeks-bestanden	Generieke onderzoeksgegevens Verzwarende omstandigheid: Patiëntenadministratie, bijzondere persoonsgegevens	Onderzoeksgegevens	LMM HHH	LMM tot HHH
7.	Dossier juridische procedures	Niet als zodanig in HORA aanwezig.	Naar analogie CRM		MHH
8.	Dossiers onafhankelijke colleges en commissies (zoals College beroep voor de examens, adviescommissie bezwaarschriften, Commissie seksuele intimidatie, Ombudsman etc.)	Niet als zodanig in HORA aanwezig.	- Naar analogie CRM; allemaal afzonderlijke verwerkingen - Mogen niet met andere verwerkingen worden samengevoegd - Vaak **bijzondere gegevens** (klasse 2 persoonsgegevens >		MHH

Nr.	Verwerking	Applicatie	Beheert objecten	BIV object	BIV verwerking
			I=H V=H)		
9.	Examen register	Niet als zodanig in HORA	Als Toetsresultaat, Beoordeling, Studieresultaat	LHO	LHM
10.	Financiële administratie	Financieel systeem	Kostenplaats Vordering Verplichting Journaalpost Activum Inkomende betaling Uitgaande betaling	LML LML LML LML LLL MML LML	MMM
11.	Gebruikersadministratie bibliotheek	Bibliotheeksysteem Vertrouwelijkheid **hoog** indien de betaal- en leenhistorie wordt bewaard.	Uitleen Werk Manifestatie Expressie Item	LLL LHO LLO LLO LLO	LHM/ LHH
12.	Identity management systeem	Applicatieplatform	Beheert in HORA geen elementen		HHM
13.	Inkoop systeem	Bedrijfsvoering	Leverancier Inkoopcontract	LLL LML	LML
14.	IT management systeem	Bedrijfsvoering	Applicatie Apparaat Systeemsoftware	LLL LLH LLL	LMH
15.	Kiesgerechtigden	Niet als zodanig in HORA aanwezig. Goed voorbeeld van **niet-bron** systeem: bevat informatie uit andere bronsystemen.	Bevat meer of minder elementen van Deelnemer en Medewerker		MHM
16.	Nevenwerk openbaar register (conform gedragscode NSVU)	Samenwerkingssysteem			LHO
17.	Onderzoeks administratie en -gegevensbeheer	Onderzoeksgegevensbeheerssysteem	Onderzoeksinformatiesysteem	LHM	LHM
18.	Personeelsinformatie systeem - Adressen en smoelenboek	Personeelssysteem	Onderwijsinstelling Organisatieonderdeel Medewerker Dienstbetrekking	LLL LLL MHH LMM	MHH

Nr.	Verwerking	Applicatie	Beheert objecten	BIV object	BIV verwerking
	- Promovendi (medewerkers die proefschrift schrijven) - Stagiaires		Competentie Beoordeling Formatieplaats	LLO LMM LLL	
19.	Relatiebeheer - Abonnementen magazines - Verzendlijst elektronische nieuwsbrief	Bedrijfsvoering	Campagne Contact Organisatie Individu (is in HORA meta-element) Prospect Alumnus	LLL LLL LLL nvt MHH MHH	MHH
20.	Roosters	Onderwijsondersteuning	Rooster	HML	HML
21.	Salarisadministratie	Salaris verwerkingssysteem	Beheert niets, dus geen HORA BIV. Benadert Financieel en Personeel		MHH
22.	Sollicitanten	Als Personeel		MHH	MHH
23.	Studenten (inclusief deelnemers aan cursussen en post academisch onderwijs) - Inzicht studievoortgang - Organisatie onderwijs - Onderhouden contacten - Inschrijven onderwijs - Resultaten - Studenten advies en begeleiding - Lijsten en smoelenboeken - Visa/internationalisering - Adressen en smoelenboek	Studenteninformatiesysteem Document Management Systeem Email Stage en afstudeer system	Opleiding Minor Onderwijsprogramma Onderwijseenheiduitvoering Onderwijseenheiddeelname Examenprogramma Toetsresultaat Onderwijseenheidresultaat Onderwijsovereenkomst Deelnemer Waardedocument Lesgroep Leergroep Competentie Onderwijsactiviteit Deelnemeractiviteit	MHO MHO MHL MHO MML MHL LHM LHM LML MHH LHL MML LML LLO MML MMH	MHH
24.	Toegang en beheersysteem	Facilitair systeem	Gebouw Ruimte Voorwerp (Medewerker)	MML MML LLL (MHH)	MMM
25.	Web content management	Generiek	Beheert in HORA geen elementen		MMH

Toelichting

Vanuit de HORA bezien “benadert” een applicatie bedrijfsobjecten. In sommige organisaties zullen de applicaties objecten niet “benaderen” maar “beheren”. Als dat het geval is dan kan opschaling van de BIV-classificatie nodig zijn. Soms is een vastlegging de bron voor een vervolgproces, dan moet de integriteit opgewaardeerd worden. Dat kan onder meer het geval zijn bij registraties in het kader van toekomstige juridische procedures.

Studentbegeleiding kan plaatsvinden door studieloopbaanbegeleiders en psychologen. De ervaring is dat sommige instellingen de dienstverlening door psychologen uitbesteden. Betreft dit een formele uitbesteding dan valt het beheer (en de beveiliging) van de psychologische dossiers niet onder de verantwoordelijkheid van de instelling.

Iedere instelling beschikt over een archief. Volgens de HORA beheert het Document Management Systeem tevens gearchiveerde documenten. Mocht een instelling verschillende “archieven” onderscheiden dan bepaalt de BIV-classificatie van de in dat archief opgeslagen type documenten de code voor beschikbaarheid, integriteit en vertrouwelijkheid. Om die reden is Archief niet als aparte verwerking opgenomen.

Bijlage: Definities

Verwerking (van persoonsgegevens): elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
(Bron: Wet bescherming persoonsgegevens.)

Beschikbaarheid: het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante voorzieningen.

Integriteit: het waarborgen van de correctheid en de volledigheid van informatie en verwerking.

Vertrouwelijkheid: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

Beveiligingsklasse: het niveau van gewenste beveiliging, waaraan informatie en informatiesystemen behoren te voldoen. Vaak wordt onderscheid gemaakt naar de klassen ‘standaard’, ‘gevoelig’ en ‘kritiek’, of ‘openbaar’, ‘intern’ en ‘vertrouwelijk”.
(Bron: SURfibo leidraad classificatie)

Vanwege de aansluiting bij de HORA is in de tabel met BIV-classificaties per verwerking gebruik gemaakt van de indeling Openbaar/Laag/Midden/Hoog.

HORA: de referentie architectuur voor het hoger onderwijs, te vinden op :
http://www.wikixl.nl/wiki/hora/index.php/BIV_classificaties

Bijlage: Voorstel basisniveaus

Aspect	Toelichting	Basis BIV
Beschikbaarheid	Beschikbaarheid heeft twee componenten: beschikbaarheid in geval van calamiteiten (compleetheid en snelheid van herstel) en beschikbaarheid voor de gebruiker. Veel systemen krijgen in HORA een laag of midden, uitzondering is een Hoog voor toetsmaterialen. De Wet bescherming persoonsgegevens (Wbp) beperkt zich tot herstelbaarheid bij calamiteiten, spreekt daarbij van “beveiliging tegen verlies”. Voorstel: basisniveau beschikbaarheid voor het hoger onderwijs is Midden, tenzij instelling hoger niveau wenst. Dat zou het geval kunnen zijn voor applicaties die via het web aangeboden worden. Deze krijgen Hoog.	M
Integriteit	Binnen HORA krijgen systemen die gegevens ten behoeve van het primaire proces verwerken een Hoog. Dat geldt voor persoonsgegevens (alumnus, deelnemer, medewerker) en ook voor toetsen, toetsresultaten, werkproducten (zoals scripties) en waardedocumenten. Financiële objecten (zoals vorderingen en betalingen) binnen HORA krijgen Midden. Voorstel: niveau is Midden tenzij persoon of toets/toetsresultaat. In dat geval Hoog. De Wet bescherming persoonsgegevens geeft over integriteit geen advies, gebruikt daarvoor “aantasting van de gegevens [of onbevoegde wijziging]”.	M
Vertrouwelijkheid	Binnen HORA wordt openbaar, laag, midden en hoog gebruikt. Hoog bij verwerking van persoonsgegevens en bij toetsmaterialen, ongeacht de hoeveelheid verwerkte gegevens en al dan niet bijzondere gegevens. De Wbp stelt de mate van vertrouwelijk afhankelijk van de risicoklasse. Opvallend binnen HORA is dat systemen die gegevens van apparaten een Hoog krijgen als het IP-adres van een apparaat wordt verwerkt. Voorstel: hoewel veel informatie openbaar is (zoals alles wat gepubliceerd is op websites), is het basisniveau Midden. Hoog wordt – conform HORA – dan systemen met persoons- en toetsgegevens.	M
Controleerbaarheid	Controleerbaarheid wordt niet uitgewerkt in de HORA en alleen geïntroduceerd in de Wpb. Daarom ook hier niet verder uitgewerkt. Bij maatregelen voor controleerbaarheid kan gedacht worden aan encryptie van berichten (digitale handtekening, non-repudiation), logging en introductie van telling- en verbandcontroles (debet/credit, inkomend/uitgaand, inkoop/verkoop) en drill-down.	-

Bijlage: Vrijstellingen bij de Wbp

In aansluiting op de Wet bescherming persoonsgegevens heeft de wetgever het Vrijstellingenbesluit opgesteld. Deze vrijstellingen beschrijven verwerkingen (administraties met persoonsgegevens) die in de meeste organisaties voorkomen. Verwerken conform een vrijstelling betekent dat de verwerking niet gemeld hoeft te worden aan het Cbp, Alle andere privacy-eisen (zoals toegestane bewaartermijnen) blijven van kracht. Het vrijstellingenbesluit doet geen uitspraken over BIV-codes.

Onderstaande tabel somt de voor het hoger onderwijs meest relevante van melding vrijgestelde verwerkingen op.

Artikel	Vrijstelling voor melding van verwerking
3	Verenigingen, stichtingen en publiekrechtelijke beroepsorganisaties
5	Sollicitanten
7	Personeelsadministratie
8	Salarisadministratie
11	Abonnementen
12	Debiteuren en crediteuren
13	Afnemers en leveranciers van goederen en diensten en cliënten- en gastenadministraties
14	Huur en verhuur
15	Individuele gezondheidszorg (w.o. psychologen)
19	Leerlingen, deelnemers en studenten
29	Archiefbestemming
30	Wetenschappelijk onderzoek en statistiek
31	Documentenbeheer
32	Netwerksystemen
33	Computersystemen
34	Communicatieapparatuur
35	Toegangscontrole
36	Overig intern beheer
37	Bezoekersregistratie
38	Videocameratoezicht
38a	Intranet
38b	Persoonlijke websites
39	Bezwaarschriften, klachten en gerechtelijke procedure
40	Registers en lijsten
41	Oud-leden en oud-leerlingen
42	Communicatiebestanden
43	Combinaties van verwerkingen

Details over de vrijstellingen zijn te vinden op http://wetten.overheid.nl/BWBR0012461/ .