OPLEGNOTITIE Project *voorbereiding implementatie Algemene Verordening Gegevensbescherming*

Inleiding op alle gepubliceerde stukken die n.a.v. dit project zijn opgeleverd

Versie 1.0 januari 2015

Let OP! De werk documenten m.b.t. dit project zijn specifiek ingericht voor instellingen van Hoger Onderwijs en Onderzoek. Daarbij moeten diegenen die de documenten willen gebruiken, deze *aanpassen aan de eigen werkwijze en wensen van zijn of haar instelling*, zodanig dat het werk document voldoet aan de relevante wet- en regelgeving m.b.t. privacy en gegevensbescherming en daarbij aansluit op de organisatie en het bestuursmodel van de instelling.

Inleiding

Op Europees niveau wordt sinds 2012 gewerkt aan nieuwe wetgeving op het gebied van privacy, de *Algemene Verordening Gegevensbescherming* (AVG) ter vervanging van de huidige Richtlijn Gegevensbescherming (in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens).

Ter voorbereiding op deze nieuwe regelgeving is vanuit *sectorale aanpak* in september 2013 een *Initiatiefgroep Privacy Hoger Onderwijs* ingericht waar vertegenwoordigers van universiteiten, hogescholen en academische medische ziekenhuizen alsook de Inspectie van het Onderwijs aan deelnemen. Het doel van de Initiatiefgroep is *de bewustwording bij de instellingen over zowel huidige als toekomstige regelgeving te vergroten en praktische ondersteuning te bieden bij de implementatie van de regelgeving*.

Uitvoering van dit doel is ondergebracht in het project *"Voorbereiding Implementatie Algemene Verordening Gegevensbescherming"* dat in 2014 gestart is. Een project wat op zichzelf weer is onderverdeeld in een aantal deelthema's, die van belang worden geacht met betrekking tot privacy en gegevensbescherming in het hoger onderwijs. Dat zijn onder andere het vastleggen van het huidige en toekomstige juridisch kader waarbinnen de instellingen dienen te opereren, het vaststellen van beleid op gebied van gegevensverwerking, het doen van een *privacy impact assessment* (risicoanalyse, ook wel afgekort als PIA) op verwerkingssystemen en daarnaast over omgang met datalekken, nu en in de toekomst met de voorgenomen wetswijziging die melding tot op zekere hoogte verplicht zal stellen.

De stukken van dit project zien voornamelijk op de interne bedrijfsvoering van instellingen binnen het hoger onderwijs. Er is echter ook een *HO normenkader* beschikbaar dat toeziet op contractuele en dus externe bedrijfsvoering van instellingen m.b.t. het onderwerp privacy. Dit document kunt u ook terugvinden op de website van SURFnet.

In de nabije toekomst zal de projectgroep ook nog twee separate stukken aanleveren die zich toespitsen op omgang met onderzoeksgegevens en minderjarigen gegevens. Houdt dan ook onze webpagina in de gaten voor meer informatie hieromtrent.

Stand van zaken Algemene Verordening Gegevensbescherming

Op dit moment is de tekst van de AVG nog niet definitief. De handreikingen zijn dan ook gebaseerd op de bestaande wetgeving (Wbp) en nemen daar de concept tekst (van het Europees Parlement van 12 maart 2014) zoals die er ligt van de AVG in mee. De tekst kunt u hier vinden.

Dit betekent noodzakelijkerwijs dan ook, dat de handreikingen zoals ze er nu liggen, mettertijd nog aangepast dienen te worden aan de definitieve tekst van de AVG. Deze aanpassingen zullen, zoals de huidige trend doet uitwijzen echter niet meer leiden tot een compleet andere strekking en vooral in de details liggen. De relevantie en bruikbaarheid van de huidige stukken is hiermee dus gewaarborgd.

Deliverables

Om de instellingen van hoger onderwijs en onderzoek voor te bereiden op de nieuwe Verordening worden vanuit een sectorale aanpak een drietal **deliverables** gesteld:

a) Handreikingen en seminars die kennisoverdracht beogen

b) Activiteiten die bewustwording bij de instellingen over de huidige en toekomstige regelgeving vergroten

c) Het nemen van de verantwoordelijkheid vanuit de sector om te voldoen aan de huidige en toekomstige privacywet- en regelgeving

Dit document ziet specifiek toe op het aanbieden van de *handreikingen*, die naar aanleiding van de eerste deliverable door de verschillende werkgroepen binnen het project zijn opgesteld en uitgewerkt.

In 2014 zijn ook al een aantal seminars georganiseerd, en hebben leden van de projectgroep verschillende bijeenkomsten bijgewoond waar het thema privacy in terug kwam. In 2015 zal dit worden voortgezet en staat in ieder geval nog een seminar inzake *onderzoeksdata en privacy* op de agenda. Ook is er de mogelijkheid voor andere thema's nog seminars te organiseren. Meer informatie hierover kunt u vinden op de agenda van SURFacademy.

De handreikingen

De handreikingen zijn op basis van een aantal verschillende thema's ingericht die u hieronder kunt terugvinden. Per handreiking is een korte samenvatting van het doel en de inhoud toegevoegd om u in één oogopslag een beter beeld te geven in welke zin de lezer deze kan gebruiken ter inventarisatie, ondersteuning of aanpassing van de huidige situatie.

Let wel dat alle stukken een model indicatie zijn en deze niet zonder meer kunnen worden overgenomen. Het idee achter de handreikingen is dan ook dat zij dienen als sectormodel, waarmee de lezer zelf kan inventariseren in hoeverre een eigen privacy beleid in overeenstemming is met huidige wetgeving, en daarbij direct ook kunt inventariseren wat er verandert met ingang van de nieuwe Europese Verordening Gegevensbescherming. Daarom zijn alle handreikingen ook voorzien van verschillende stukken, de handreiking zelf en een leidraad die de lezer uitleg biedt hoe de handreiking gehanteerd kan worden. De handreikingen bevatten informatie en aanbevelingen die in beginsel vrijblijvend zijn, het is aan de Instelling zelf om te bepalen in hoeverre er uitwerking wordt gegeven, dan wel nodig is op het gebied van privacy en gegevensbescherming. Uiteraard wordt de lezer er per document op gewezen in hoeverre de wet bepaalde verplichtingen oplegt. De handreikingen zijn zowel apart als gezamenlijk hanteerbaar, afhankelijk van het doel van de lezer.

Wel delen alle handreikingen dezelfde *definitie bijlage*. Deze bijlage definieert het meest relevante privacy jargon op een zo helder en begrijpelijk mogelijke manier.

I. Handreiking juridisch kader IST en SOLL situatie

- ✓ GAPscan analyse
- ✓ Schema inventarisatie verwerkingen persoonsgegevens
- ✓ Overzicht 25 veel voorkomende verwerkingen persoonsgegevens
- ✓ Raamwerk (naslagwerk juridisch kader en GAPscan analyse)

De handreiking juridisch kader is opgesteld door de werkgroepen IST (huidige juridische situatie) en SOLL (toekomstige juridische situatie). IST oriënteerde zich in beginsel op de vraag op welke manier HO-instellingen een adequaat beeld kunnen vormen over implementatie en naleving van zowel de Wet bescherming Persoonsgegeven (Wbp) als de Algemene Verordening Gegevensbescherming). SOLL oriënteerde zich in beginsel op het uitvoeren van een analyse van die aspecten van de AVG die van

belang zijn voor het Hoger Onderwijs en Onderzoek in de vorm van een raamwerk, belangrijk onderdeel hiervan is hoe de bepalingen uit de AVG om te zetten in maatregelen en procedures.

Beide werkgroepen hebben na verloop van tijd hun krachten gebundeld, omdat de doeleinden dichter bij elkaar bleken te liggen dan verwacht. Daaruit in een compleet geheel van stukken gekomen waarmee we hopen de instellingen zowel een adequaat beeld te geven over implementatie, naleving, het uitvoeren van een analyse en bepalen van te nemen maatregelen en procedures. De kern hiervan vindt u in het stuk *Privacy GAP Scan AVG*. Deze scan is een hulpmiddel om beter zicht te krijgen op de onderwerpen die voorafgaande de invoering van de Verordening nog moeten worden opgepakt. Het moet een beeld geven van de kloof ('gap') tussen de bestaande situatie en de gewenste situatie. De focus van de scan is daarbij gericht op maatrelen die getroffen moeten worden op het terrein van beheer en beleid.

II. Handreiking Beleidsmodel

- ✓ Model privacybeleid
- ✓ Leidraad model privacybeleid

Eén van die consequenties van de AVG is de verplichting om een formeel Beleid Verwerking Persoonsgegevens vast te stellen. Het was voor de projectgroep dan ook van belang om een werkgroep in te richten die zich specifiek zou inzetten om een model beleid, dat voldoet aan de bepalingen van relevante wet- en regelgeving, te creëren wat door alle instellingen kan worden gebruikt, maar juist ook nog moet worden aangepast aan de eigen werkwijze en wensen. De werkgroep heeft dit model beleid geschreven aan de hand van het model Informatie Beveiligingsbeleid van SURFibo.

Bij het model zelf heeft de werkgroep ook een *Leidraad Privacybeleid* toegevoegd, waarin toelichting wordt gegeven op onderdelen in het model beleid en een beschrijving wordt gedaan van good practice. Daarmee streeft het diegenen, die binnen een instelling privacy beleid willen ontwikkelen of verbeteren, een handvat voor nadere invulling te bieden.

III. Handreiking Privacy Impact Assessment (PIA)

- ✓ PIA toelichting en invulinstructie
- ✓ PIA template
- ✓ Voorbeeld template (obv studenteninformatiesysteem)

De werkgroep PIA werd ingesteld met het doel een praktisch instrument te ontwikkelen in het kader van het uitvoeren van een privacy impact assessment. Belang van dit thema is de steeds belangrijkere rol die een PIA (risico analyse) speelt bij projecten omdat zo in een vroeg stadium onderkend kan worden of sprake zal zijn van werken met persoonsgegevens waarbij al dan niet aanvullende maatregelen dienen te worden genomen om een inbreuk op de persoonlijke levenssfeer van een betrokkene te vermijden dan wel te verminderen.

Dit alles heeft geleid tot een instrument die een praktisch bruikbaar handvat biedt om een PIA uit te voeren: compact maar volledig, vanuit het individu maar ook met oog voor de organisatie. Naast de PIA invulinstructie zelf, heeft de werkgroep de gebruiker ook voorzien van een aparte invulinstructie (soort leidraad), aparte toelichting, en voorbeeld PIA aan de hand van een SIS (studenteninformatiesysteem).

IV. Handreiking Meldplicht Datalekken

- ✓ Stappenplan Meldplicht Datalekken
- ✓ Vraagbaak

De handreiking Meldplicht datalekken bevat een stappenplan, dat onderwijsinstellingen kunnen gebruiken bij hun voorbereiding op de meldplicht voor datalekken. Het stappenplan focust op integrale veiligheid en benadrukt daarom de taken en verantwoordelijkheden van verschillende functionarissen

binnen de onderwijsinstellingen. Daarnaast geeft deze handreiking ook antwoord op de meest gestelde vragen over de meldplicht datalekken.

Het is helaas nog onduidelijk wanneer het wetvoorstel wijziging Wbp, waarin de meldplicht datalekken is opgenomen zal worden aangenomen. Dit hangt samen met de vorderingen op Europees niveau voor de AVG, waarin een soortgelijke plicht is opgenomen. De actualiteiten worden nauw in de gaten gehouden, en van enige wijzigingen of doorvoering van het voorstel zal melding worden gemaakt en een update van deze (maar ook de andere) handreikingen worden verzorgd.

Tot slot

Zoals in de inleiding is vermeld heeft de projectgroep ook nog gekeken naar speciale privacy thema's, die een specifieke dan wel afwijkende inrichting behoeven van de 'standaard norm' voor bescherming van gegevens. Deze stukken, betreffende privacy van onderzoeksdata en privacy van minderjarigen gegevens zijn nog niet klaar, maar staan op de agenda voor publicatie in 2015.

Met uitvaardiging van de huidige set documenten hopen wij als projectgroep bij te dragen aan onze laatste deliverable, namelijk het nemen van de verantwoordelijkheid vanuit de sector om te voldoen aan de huidige en toekomstige privacywet- en regelgeving, door de instellingen te voorzien van een geheel aan informatie die inzicht moet bieden aan instelling die willen weten hoe privacy compliant ze zijn, maar ook waar en hoe ze veranderingen aan kunnen brengen om compliance te verbeteren of verhogen.