

Privacy-aandachtspunten voor e-portfolioproviders¹

Jan Peter Bergfeld²

1. Inleiding

Een e-portfolio kan worden gezien als de vertaling naar het internettijdperk van het bekende curriculum vitae als traditionele bijlage bij een sollicitatiebrief.

De Stichting ePortfolio Support (StePS) stelt zich ten doel om de participatie en inzetbaarheid van iedereen die tot de beroepsbevolking behoort te stimuleren door de ontwikkeling en het gebruik van e-portfolio's. Het streven is erop gericht dat in 2020 de gehele beroepsbevolking beschikt over een e-portfolio en daarmee ook controle heeft over zijn of haar persoonlijke arbeids- en opleidingsgegevens.

StePS en andere aanbieders bieden burgers de mogelijkheid om gratis een e-portfolio aan te maken en op internet te plaatsen. Ze treden daarmee op als e-portfolio provider.

In dit artikel ga ik in op de belangrijkste privacy-aandachtspunten uit de algemene Wet bescherming persoonsgegevens (Wbp) in relatie tot het e-portfolio, de gebruiker en de e-portfolioproviders. Deze aandachtspunten vloeien direct voort uit onze grondwet en diverse internationale verdragen. Als er op zorgvuldige wijze invulling aan wordt gegeven vormen ze tevens een belangrijk kwaliteitsaspect van dienstverlening. Organisaties die persoonsgegevens verwerken zullen, mede onder invloed van de Europese conceptverordening gegevensbescherming, in de vorm van een privacy policy moeten laten zien hoe ze met privacyvragen omgaan. Ze kunnen daarmee de burger het signaal geven dat zijn persoonsgegevens in goede handen zijn, of juist waarschuwen dat er altijd risico's zijn. Van beide situaties zijn in dit artikel voorbeelden opgenomen.

2. Wat is een e-portfolio?

Een e-portfolio of elektronisch portfolio is een verzameling van doelgericht bij elkaar gebrachte elektronische gegevens en documenten (bestanden), die wordt beheerd door het lerende en werkende individu. Het doel van het samenstellen van een e-portfolio is het tonen van resultaten (en eventueel het leerproces) aan anderen.³

Een door een gebruiker aangemaakt LinkedIn profiel voldoet aan bovengenoemde definitie, al spelen bij LinkedIn natuurlijk ook andere doelen mee van zowel de

¹ Dit artikel is gebaseerd op een presentatie van de auteur als onderdeel van de door StePS georganiseerde expertmeeting over e-portfolio en privacy op 28 maart 2012 in Utrecht.

² Mr. dr. J.P.R. Bergfeld is als directiesecretaris, juridisch adviseur en privacyfunctionaris werkzaam bij Stichting Inlichtingenbureau. Hij was daarvoor tien jaar werkzaam als universitair docent en onderzoeker bij het Instituut voor Informatica & Recht van de rechtenfaculteit van de Vrije Universiteit te Amsterdam.

³ De definitie is afkomstig uit het White paper Architectuuraspecten e-portfolio, Kennisnet.nl/M. van der Zalm, november 2007. Ook Calbris gaat uit van deze definitie in het rapport E-portfolio, Huidige stand van ontwikkeling en toepassing, E-portfolio binnen de Zorg, Welzijn en Sport Bouwen aan kennis, Calbris, zonder datum.

gebruiker als de provider bij het aanmaken, onderhouden en exploiteren van een dergelijk profiel.

Een belangrijk aspect van bovengenoemde definitie is dat deze een heldere en inzichtelijke afbakening biedt met *niet* door het individu beheerde toepassingen, die dus niet aan de (deze) definitie van e-portfolio voldoen, maar waarbij een e-portfolio wel een belangrijke rol en functie kan hebben. Daarbij kan gedacht worden aan leerlingregistraties op scholen en opleidingsregistraties van werkgevers. Dat zijn namelijk de *anderen* uit het geformuleerde doel van de e-portfolio-definitie. Hoewel er vaak een - ook uitdrukkelijk beoogde - wisselwerking zal zijn tussen e-portfolio's en ontvangende registraties of applicaties, is het van groot belang deze niet op een hoop te gooien, aangezien het om heel andere doelen gaat en het beheer van die ontvangende registraties en applicaties doorgaans ook niet bij het individu berust.

3. Privacyrecht

Privacy is een grondrecht dat ook nog eens in verschillende internationale verdragen is uitgewerkt. De algemene Wet bescherming persoonsgegevens (Wbp) geldt als de uitwerking van artikel 10 van onze Grondwet dat het recht op privacy bevat. De Wbp is tevens de uitwerking van een Europese Richtlijn in onze nationale wetgeving.

De Wbp is van toepassing op de verwerking van persoonsgegevens. Dat leidt tot de vragen wat zijn *persoonsgegevens* en wat is *verwerking*. Een persoonsgegeven wordt in de Wbp gedefinieerd als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Onder verwerking van persoonsgegevens verstaat de Wbp: 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 persoonsgegevens.

De Wbp onderscheidt verschillende actoren. De belangrijkste daarvan is de *verantwoordelijke*: die stelt - alleen of tezamen met anderen - het doel van en de middelen voor de verwerking van persoonsgegevens vast. Soms maakt een verantwoordelijke gebruik van een *bewerker*: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan diens rechtstreeks gezag te zijn onderworpen. De natuurlijke persoon die gebruik maakt van de diensten van een e-portfolioprovider om zijn e-portfolio te beheren wordt door de Wbp aangemerkt als betrokkene. In dit artikel wordt de betrokkene ook wel aangeduid met de termen gebruiker of burger.

Uit bovenstaande definities kan worden geconcludeerd dat e-portfolioproviders in Nederland moeten voldoen aan de inhoudelijke eisen van de Wbp. Naar verwachting wordt het privacykader binnen enkele jaren in Europees verband aangepast en zal een nieuwe privacywet moeten worden opgesteld.⁴ Mede om deze reden worden de

⁴ Zie het Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en

eisen die aan e-portfolioproviders worden gesteld gepresenteerd vanuit het perspectief van algemenere privacy-uitgangspunten, die vervolgens nader worden ingevuld voor de Wbp. Op punten waar de concept Europese verordening gegevensbescherming daarvan afwijkt wordt dit toegelicht.

4. Privacy-uitgangspunten

a. Doelspecificatie en doelbinding

Het doelspecificatiebeginsel houdt in dat een verantwoordelijke van tevoren een afgebakend rechtmatig doel dient te hebben waartoe zijn belang ook redelijkerwijs strekt. Een organisatie moet dus zijn grenzen kennen. Gelet op de doelstelling van StePS is het optreden als e-portfolioprovider een rechtmatig doel.

Het doelbindingsbeginsel schrijft voor dat persoonsgegevens alleen mogen worden gebruikt voor de doelen waarvoor ze zijn verkregen en in bepaalde gevallen voor andere doelen die daarmee *niet onverenigbaar* zijn.

b. Verzamelbeperking/gebruiksbeperking

Een verantwoordelijke mag niet *meer* persoonsgegevens verzamelen dan noodzakelijk voor het doel van de gegevensverwerking. StePS biedt een gratis e-portfolio-voorziening en kan (mag) dus niet zomaar om allerlei gegevens over bijvoorbeeld bankrekeningen en creditcards vragen. Dat ligt bijvoorbeeld anders voor de zogenoemde premium accounts van LinkedIn.

Gegevens worden voor een specifiek doel verstrekt en kunnen in beginsel niet voor andere doelen worden gebruikt. Daar bevat de Wbp wel een afwegingskader voor, waar ook de doelspecificatie weer een rol in speelt.

Als de verantwoordelijke verklaart dat persoonsgegevens niet zonder toestemming van de betreffende persoon voor andere doeleinden worden gebruikt is dat een behoorlijk stringente gebruiksbeperking en daarmee een sterke privacywaarborg voor de gebruiker. Dat zeggen de privacyverklaringen van StePS en LinkedIn overigens niet. De LinkedIn Privacy Policy Highlights geven een nette opsomming van welke persoonsgegevens worden verzameld en voor welke doelen die gebruikt worden. Zowel StePS als LinkedIn sluit uit dat persoonsgegevens aan *derden* worden verstrekt, maar *eigen* gebruik is daarmee niet (geheel) uitgesloten. LinkedIn zegt daarover: “We use the information you provide to (...) send you service or promotional communications through email (...)” En dat kan dus best promotional communication van een derde zijn, die wordt bezorgd door LinkedIn.

Ook bij StePS is dat niet expliciet uitgesloten. StePS zou bijvoorbeeld kunnen bedenken dat een jaarlijks e-portfolio-congres interessant is voor iedereen die een e-portfolio bij StePS heeft aangemaakt. Dit spoort ook met de (overige) activiteiten die zowel het organiseren van symposia als het ondersteunen van ontwikkelaars en

betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), COM (2012) 11 final, Brussel 25.1.2012.

gebruikers en het ondersteunen van promotie-activiteiten omvatten. StePS beschikt over de communicatiegegevens van de e-portfoliohouders en zou ze een mail kunnen sturen. Dat is onder de huidige privacyregelgeving toegestaan. Dat ligt duidelijk anders in de hypothetische situatie dat zorgverzekeraar Academica zou verzoeken om een mailing aan alle personen van wie uit het portfolio blijkt dat ze een wetenschappelijke opleiding *en* een baan hebben. Dit gebruik is zeker niet verenigbaar met de doelstellingen van Steps zoals die op de website zijn gepubliceerd en doorstaat niet de toetsing aan artikel 9 lid 2 Wbp.

c. Gegevenskwaliteit

Artikel 11 lid 2 Wbp verplicht de verantwoordelijke de nodige maatregelen te treffen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn. Bij het e-portfolio is veel informatie door de houder zelf ingevuld en is dit dus geen probleem.

Iets minder simpel is de vraag naar de bewaartermijn als aspect van gegevenskwaliteit. De algemene norm van artikel 11 Wbp bepaalt dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor het realiseren van de doeleinden waarvoor zij worden verzameld en/of verwerkt. In de praktijk is die norm echter moeilijk te operationaliseren. Hoe lang zou StePS of LinkedIn mijn e-portfolio mogen of moeten bewaren? In beginsel tot de gebruiker zijn gegevens zelf verwijdert. Als er geruime tijd geen gebruik van een e-portfolio wordt gemaakt kan een e-portfolioprovider toepassing geven aan de werkwijze van telecomproviders die prepaid diensten aanbieden. Hij kan een sms en/of email sturen met de boodschap dat het e-portfolio vervalt als binnen een bepaalde periode geen gebruikersactiviteiten worden ondernomen. Bij voorkeur staat dat in het kader van transparantie natuurlijk al van tevoren opgenomen in een bewaartermijn en procedure die is beschreven in de privacy policy.

De Europese concept verordening gegevensbescherming concept bevat in artikel 15 onder andere de verplichting voor de verantwoordelijke om de betrokkenen te wijzen op de vastgestelde bewaartermijn en een mededelingsplicht van hetgeen met de door hem verwerkte persoonsgegevens gebeurt na afloop van de termijn.

d. Informatiebeveiliging

Artikel 13 Wbp draagt de verantwoordelijke op om *passende technische en organisatorische maatregelen* ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen *garanderen*, rekening houdend met (1.) de stand van de techniek en (2.) de kosten van de tenuitvoerlegging, een passend beveiligingsniveau.

De tekst van artikel 13 dwingt zowel tot een kosten-batenanalyse als tot een periodieke herijking gerelateerd aan de stand van de techniek. Ondanks het gebruik van de term *garanderen*, is dit een inspanningsverplichting, waarbij een afwegingskader wordt geboden. Een aardige relativering in het kader verwachtingsmanagement is opgenomen in de privacy policy van LinkedIn: Na een opsomming wat LinkedIn allemaal *wel* doet aan informatiebeveiliging vervolgt de tekst

... However, since the internet is not a 100% secure environment, we cannot ensure or warrant the security of any information you transmit to Linked IN.

e. Verantwoordelijkheid/ Aansprakelijkheid

Uitgangspunt is dat de verantwoordelijke (in de zin van de Wbp), het woord zegt het al, verantwoordelijk en aansprakelijk is voor de gegevensverwerking. Daar moet je dus zijn als je schade lijdt of als je gebruik wilt maken van je inzagerecht en/of correctierecht.

f. Transparantie/inzagerecht

Op basis van de concept Europese verordening gegevensbescherming moet de verantwoordelijke transparante, eenvoudig toegankelijke en begrijpelijke informatie verstrekken. Het transparantiebeginsel maakt de cirkel rond naar de doelspecificatie en doelbinding. Die transparantie werkt twee kanten op: een algemene transparantie over de gegevensverwerking (welke gegevens, welk doel etc.) en een persoonlijk inzagerecht om concreet invulling te kunnen geven aan die transparantie met betrekking tot de verwerking van de eigen persoonsgegevens.

Op grond van artikel 27 Wbp moet een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens worden gemeld bij het Cbp of bij een door de verantwoordelijke aangewezen Functionaris voor de Gegevensbescherming. De dienstverlening van e-portfolioproviders valt namelijk niet onder de vele in het Vrijstellingsbesluit omschreven vrijstellingen. Onder de concept Europese verordening gegevensbescherming zal de meldingsplicht voor e-portfolioproviders waarschijnlijk vervallen.

Het persoonlijk inzagerecht zoals vastgelegd in artikel 35 Wbp vormt voor e-portfolioproviders juist weer geen probleem. Een maker van een e-portfolio vult immers zijn eigen gegevens in en kan deze desgewenst ook zelf aanpassen.

5. Conclusie

Een e-portfolioprovider moet invulling geven aan (onder meer) de bovengenoemde privacy-uitgangspunten zoals uitgewerkt in de Wbp. Door dit in de vorm van een privacyverklaring te gieten kan een e-portfolioprovider er niet alleen voor zorgen aan de verplichtingen van de Wbp te voldoen, het geeft de organisatie ook de kans om privacy(bescherming) als kwaliteitsaspect van de dienstverlening te presenteren.

De in dit artikel besproken aandachtspunten kunnen als richtsnoer worden gebruikt om een goede heldere en duidelijke privacyverklaring (privacy policy) op te stellen ten behoeve van gebruikers. Dit dwingt de leiding van de organisatie tot het maken van heldere keuzes.