Model Privacy Impact Assessment

Toelichting en invulinstructie bij gebruik van het *PIA risico formulier*

Colofon

Model Privacy Impact Assessment in het Hoger Onderwijs

SURF
PO Box 19035, 3501 DA Utrecht
T +31 88-7873000
info@surf.nl
www.surf.nl

Auteurs

Anita Polderdijk-Rijntjes (Windesheim)
Menno van Heumen (Hanze Hogeschool)
Ad Paulissen (Fontys)
Hans Alfons (Vrije Universiteit)

Eindredactie

Gezamenlijk product van de SURF Projectgroep 'Voorbereiding Implementatie Algemene Verordening Gegevensbescherming'

SURF is de ICT-samenwerkingsorganisatie van het hoger onderwijs en onderzoek (www.surf.nl).
Deze publicatie is digitaal beschikbaar via de website van SURFnet
(https://www.surf.nl/themas/beveiliging/beleidsondersteuning-privacy/implementatie-algemene-verondening-gegevensbescherming-avg/index.html)

Versie 1.0 December 2014

Inleiding

De werkgroep SURF-PIA heeft zoals afgesproken een voorstel gemaakt voor het gebruik van een praktisch instrument in het kader van de uitvoering van een Privacy Impact Assessment (PIA). De PIA speelt bij projecten een belangrijke rol. In een vroeg stadium kan onderkend worden of er sprake zal zijn van het werken met persoonsgegevens waarbij al dan niet aanvullende maatregelen moeten worden genomen om een mogelijke inbreuk op iemands persoonlijke levenssfeer te vermijden of te verminderen.

Het bijgevoegde instrument biedt een praktisch bruikbaar handvat om een PIA uit te voeren: compact maar volledig, vanuit het individu maar met oog voor de organisatie.

Hoe zit de PIA er uit?

Het materiaal bestaat uit:

- Toelichting PIA, inclusief overzicht begrippen
- Invulsheet (xls bestand)
- Toelichting invulsheet

De invulsheet bestaat uit een algemeen deel (tab basisinfo), waarin gegevens opgenomen kunnen worden die vanuit de Wbp gezien sowieso bekend moeten zijn. Naast de algemene gegevens is er dus het tabblad met de PIA-aspecten (invulsheet).

Deze versie van de invulsheet bevat ook een voorbeeld, namelijk een PIA van een SIS (studenteninformatiesysteem).

Voorstel

De werkgroep stelt voor de tool voor de PIA te verspreiden onder de bij SURF aangesloten instellingen en na één jaar het gebruik te evalueren. Voor de evaluatie en eventuele vragen blijft de werkgroep beschikbaar.

Bijlages:

- PIA risicoformulier (protected).xlsx
- PIA risicoformulier Student informatiesysteem.xlsx
- SURF PIA-toelichting
- PIA invulinstructie
- Definities

Bijlage: PIA toelichting

Een Privacy Impact Assessment (PIA) is een tool dat helpt bij het identificeren van privacy risico's en levert de handvaten om deze risico's te verkleinen tot een acceptabel niveau. Het is raadzaam om bij aanvang van een project waarbij persoonsgegevens een rol spelen een PIA uit te voeren om er zorg voor te dragen dat risico beperkende maatregelen direct in het project meegenomen kunnen worden. Het vertrekpunt van de PIA is dus de situatie dat een project kan voorzien dat het te maken heeft met persoonsgegevens, en daarom een impactanalyse uitvoert.

Proces; Wie maakt de PIA?

De PIA start met het verzamelen van basis informatie betreffende de registratie van persoonsgegevens. Dit is per definitie iets dat de verantwoordelijke (opdrachtgever project of eigenaar van de gegevens) voor zijn rekening zou moeten nemen. Deze heeft immers een informatiebehoefte en wil daarin voorzien worden. Dit is dan ook de aangewezen persoon om aan te geven welke informatie hij nodig heeft en met welk doel. In dit proces kan overleg met een Functionaris Gegevensbescherming (FG), privacy officer of security officer vaak helpen om doelen aan te scherpen en zo het verzamelen van privacy gevoelige data te minimaliseren.

Ook het inschatten van de risico's is iets dat de verantwoordelijk doorgaans in overleg met een privacy officer of security officer kan doen. Als er gelegenheid is om een uitgebreidere PIA te doen zou in dit verband ook de betrokkenen (degene waarover informatie verzameld wordt) bij de risico inschatting gehoord kunnen worden.

De selectie van maatregelen om de risico's te beheersen is een verantwoordelijkheid van de security officer. Dat laat niet onverlet dat de verantwoordelijke er voor moet zorgen dat deze ook geïmplementeerd worden.

Aanpak

Uitgaande van het volgende gegeven:

Risico = kans x impact

Richt de PIA zich zowel op kansen als op mogelijke impact. Eerst wordt gekeken naar de kans op mogelijke gevolgen (I), daarna naar te nemen maatregelen om kansen en gevolgen te verlagen (II).

1. Impactbepaling

Bij het beoordelen van de impact zijn er twee zaken waar rekening mee moet worden gehouden, namelijk: 'impact op betrokkene' (1) en 'impact op organisatie'(2). De impact moet zich vervolgens vertalen naar concrete maatregelen (II) ter vermijding of vermindering van de risico's.

1.1. Impact op de betrokkene

Een hogere 'impact op betrokkene' betekent dat de gegevens zelf en/of de context waarin deze gegevens worden gebruikt een verhoogd risico vormen voor de persoonlijke levenssfeer van degene op wie de persoonsgegevens betrekking hebben.

Bij het beantwoorden van de vraag wat de impact op de betrokkene is, moet aandacht besteed worden aan:

- Risico op en gevolgen van identiteitsfraude. Fraude plegen met identiteitsgegevens waarbij anderen (opzettelijk) verplichtingen aan gaan uit naam van de betrokkene zonder medeweten van de betrokkene of waarbij diens persoonsgegevens gebruiken voor het plegen van een misdrijf.
- Risico op en gevolgen van mogelijke (overige) privacy inbreuken welke een bedreiging vormen voor iemands vrijheid, financiën, relaties of gezondheid. Deze inbreuk op de privacy kan mogelijk ook leiden tot risico op discriminatie.
- De van toepassing zijnde privacy dimensie(s) of principes (zie bijlage 1 Begrippen), waaronder 'kwaliteit van de gegevens' en 'limitering van verzamelen en gebruik' van gegevens. Ook 'rechten van betrokkene' en 'verantwoording' zijn aspecten van deze principes .

1.2. Impact op de organisatie

Uitgangspunt in deze PIA is dat indien de privacy van de betrokkenen op een van deze gebieden wordt geschaad, de impact op de organisatie ook groter wordt, zeker wanneer er meer betrokkenen zijn. De organisatie krijgt dan te maken met bijvoorbeeld de volgende bedreigingen:

- De organisatie moet kostbare aanpassingen in processen of systemen doorvoeren of het project vroegtijdig stopzetten.
- Het vertrouwen van klanten, werknemers of burgers wordt geschaad.
- Negatieve publiciteit over het niet waarborgen van de privacy ontstaat.
- De organisatie wordt onderworpen aan toezicht en handhaving.
- De gegevenskwaliteit is onvoldoende voor de dienstverlening.
- De besluitvorming wordt gebaseerd op onvoldoende betrouwbare informatie.
- Maatregelen moeten worden getroffen om de gegevens te beveiligen.

De impact (zoals reputatieschade, maar ook materiële financiële schade als gevolg van compliance problemen, klachten en incidenten) die bovenstaande bedreigingen op de organisatie hebben moet de organisatie zelf vaststellen. Deze wordt onder andere beïnvloed door de branche waarin de organisatie zich begeeft, het belang dat de klanten aan privacy hechten, en de maatschappelijke aandacht.

Het project bepaalt de impact dus in twee stappen: eerst vanuit de betrokkene gezien en op grond van de projectopdracht (doelbinding!) en vervolgens vanuit de mogelijke gevolgen voor de organisatie waarbinnen het project zich afspeelt en waarbij de opdrachtgever aanspreekbaar is op de borging van de persoonlijke levenssfeer van het individu.

2. Maatregelen nemen om risico's te verkleinen of weg te nemen

Op basis van de inschatting van de impact op de betrokkene of de organisatie, moet worden nagegaan op welke wijze de risico's vermeden of verkleind kunnen worden. Het advies is na te gaan of de negatieve privacy impact op de betrokkene noodzakelijk is, en kan worden gerechtvaardigd. Bij een verwerkingsgrondslag 'gerechtvaardigd belang' of 'publiek belang' is een privacy toets wettelijk verplicht. Het belang van de organisatie en het belang van het individu moeten hierbij tegen elkaar worden afgewogen.

Het vermijden of verminderen van risico's houdt overigens niet in dat de projectdoelen moeten worden bijgesteld. Naarmate de inschatting van de impact hoger wordt, is het raadzamer om (binnen het project) maatregelen te treffen om de risico's weg te nemen of te verminderen.

Hieronder worden nog enkele voorbeelden gegeven van de manieren waarop risico's vermeden of verminderd kunnen worden:

2.1. Vermijden van risico's

Het vermijden van de risico's kan door helemaal geen persoonsgegevens te verwerken. Het doel kan bijvoorbeeld toch bereikt worden door:

- Opslag van gegevens bij het individu in plaats van binnen de organisatie.
- Het gebruik van anonieme gegevens, of pseudoniemen.
- Het toepassen van mathematische methodes, zonder de onderliggende gegevens op te vragen en te registreren.

2.2. Verminderen van risico's

Afhankelijk van het risico en het privacyprincipe kunnen ook maatregelen getroffen worden die het risico verminderen. Hieronder zijn per privacyprincipe enkele voorbeelden opgenomen:

1. Limitering van het verzamelen van gegevens:
   Het verminderen van de hoeveelheid gegevens, door de gegevens niet op te slaan of niet te bewaren.

2. Gegevenskwaliteit:
   Introduceren van geautomatiseerde controles op gegevens.

3. Doelbinding:
   De doelen voor het verzamelen en verenigbaarheid van verdere verwerking nader specificeren en hierover communiceren.

4. Limitering van gebruik van gegevens:
   Het beperken van de mogelijkheid om grote hoeveelheden gegevens in een keer binnen en buiten de organisatie te verspreiden door gefragmenteerde opslag, in plaats van concentreren van alle gegevens in één database.

5. Beveiliging van gegevens:
   Het toepassen van encryptie en logische toegangsbeveiliging.

6. Transparantie:
   Het opstellen van een privacy beleid, gedragscode of het laten certificeren van de verwerking.

7. Rechten van betrokkenen:
   Betrokkenen zeggenschap geven over zijn gegevens door de invoer van een 'self-service' bijvoorbeeld via een beveiligd internet portal.

8. Verantwoording:
   Bijvoorbeeld invoeren van periodiek externe controle, melding in jaarverslag, organiseren van hulp na schending privacy. Maar ook werken aan bewustwording en opleiding.

Op basis van normstelsels binnen informatiebeveiliging kunnen organisaties verkennen in hoeverre de te treffen beheersmaatregelen al dan niet reeds getroffen zijn. Het in kaart brengen van de eisen waar precies aan moet worden voldaan, het definiëren van het te behalen ambitieniveau/

volwassenheidsniveau van de organisatie, welke beheersmaatregelen de organisatie zou moeten treffen (passend bij het ambitie/ volwassenheidsniveau) alsmede het in kaart brengen van de mate waarin de organisatie de te treffen maatregelen ook daadwerkelijk reeds heeft getroffen/geïmplementeerd, maakt geen onderdeel uit van de PIA. Dat is ondergebracht bij Informatiebeveiliging.

Bijlage: PIA Invulinstructie

PIA template (Excel bestand)

De PIA template die door de werkgroep PIA van SURF ontwikkeld is bestaat uit drie delen (zie ook de toelichting op het gebruik van de PIA):

- Verzamelen van basis informatie over de verwerking
- Inschatten van het risico
- Selecteren van de maatregelen

Verzamelen van basis informatie over de verwerking

Bij het verzamelen van basis informatie over de gegevens verwerking worden een 8-tal onderwerpen bevraagd welke min of meer overeenkomen met de onderwerpen die we ook op het meldingsformulier van het CBP zien terugkomen.

1. Verantwoordelijke
2. Bewerker
3. Naam van verwerking
4. Doel van verwerking
5. Grondslag voor verwerking
6. Categorieën van betrokkenen
7. Gegevens, verzameldoel en bewaartermijnen
8. Gebruikers/ontvangers

Voor nadere toelichting bij ieder van deze onderwerpen zie de bijlage.

Inschatten van het risico

Na het verzamelen van de basis informatie zal de echte risico bepaling plaats moeten vinden. Op een aantal onderdelen worden zo de risico's bekeken, te weten:

1. Type project
2. Aard van de gegevens
3. Betrokken partijen
4. Verzamelen
5. Gebruik
6. Bewaren en vernietigen
7. Beveiligen

Om in het model een link te kunnen leggen tussen de risico's en de nodige maatregelen is ervoor gekozen om de risico inschatting te doen aan de hand van kans en impact bepaling.

Risico's hangen immers samen met de kans dat een gevolg zich voordoet en de impact die dat gevolg heeft als het zich eenmaal heeft voorgedaan. De impact zoals die in de sheet voorkomt is in de basis de impact zoals deze kunnen gelden voor de betrokkene en voor de organisatie (zie de toelichting op de PIA).

Hierbij wordt in het model de volgende risico matrix gebruikt:

	Kans Laag	Kans Middel	Kans Hoog
Impact Laag	Risico Zeer Laag	Risico laag	Risico Middel
Impact Middel	Risico Laag	Risico Middel	Risico hoog
Impact Hoog	Risico Middel	Risico Hoog	Risico Zeer Hoog

Het model somt per onderdeel allerlei kans en impact verhogende aspecten op die je kunnen ondersteunen bij het maken van een juiste risico inschatting.

Selecteren van maatregelen

Het beperken van risico's richt zich op het verkleinen van de impact en/of het verlagen van de kans. Derhalve zijn ook de maatregelen in het model onderverdeeld naar impact beperkende en kans verlagende maatregelen. Bij ieder maatregel kan aangegeven worden hoe groot de noodzaak is voor het treffen van de maatregel:

- M > Must: maatregel wordt vereist
- S > Should: maatregel wordt dringend gewenst
- C > Could: maatregel is gewenst maar niet noodzakelijk

In het model zou het zo moeten uitwerken dat wanneer het risico "zeer hoog" is er meer maatregelen een "must" zijn. Als een risico "hoog" is omdat de kans dat een bepaald gevolg zich voordoet "hoog" is dan zal de aandacht in eerste instantie meer uit moeten gaan naar kans beperkende maatregelen en iets minder naar impact beperkende maatregelen.

Voorbeeld PIA; SIS
Er is een voorbeeld PIA gemaakt voor het domein Studentinformatiesysteem. Voor de definitie van dit domein is de HORA (Hoger Onderwijs Referentie Architectuur) gebruikt.

Hoewel de basis informatie voor de instellingen grotendeels hetzelfde zal zijn is het wel verstandig om bij het toepassen in de eigen organisatie ook dit deel van de spreadsheet nog kritisch door te lopen.

De verwerkingsdoelen die benoemd zijn, zijn de elementen die ook terug te vinden zijn in het Vrijstellingsbesluit paragraaf 5 artikel 19.

De bewaartermijn die hier gehanteerd worden komen uit de selectielijst voor het HBO welke door de vereniging Hogescholen is opgesteld en door veel HBO instellingen is geadopteerd.

In de invulsheet is het risico ten aanzien van het type project en de beveiliging niet ingeschat omdat hiervoor geen algemene inschatting te maken is. De inschatting van deze risico's is sterk organisatie afhankelijk.

Bijlage: begrippen

Verantwoordelijke	De verantwoordelijke is degene die het doel en de middelen voor de verwerking vaststelt. Dit kan een afdeling of bestuursorgaan of een natuurlijk persoon zijn.
Bewerker	Een bewerker is een persoon of organisatie aan wie de verantwoordelijke de verwerking van persoonsgegevens heeft uitbesteed. Ook als er alleen sprake is van opslag van persoonsgegevens in de cloud is er al sprake van een bewerker (i.c. de hosting partij).
Naam verwerking	Hier dient de verwerking van persoonsgegevens omschreven te worden. Dat kan door de naam van de verwerking te vermelden zoals deze binnen de organisatie(s) van de verantwoordelijke(n) bekend is, bijvoorbeeld ‘personeelsadministratie’ of ‘klachtenregistratie’.
Doel van verwerking	Een precieze en duidelijke omschrijving van het doel (of de samenhangende doeleinden) van de verwerking is van belang, omdat aan de hand van het doel van de verwerking de hoeveelheid, de soort, de kwaliteit en de bewaartermijn van de gegevens worden getoetst.
Grondslag voor verwerking	De WBP kent een beperkt aantal grondslagen op basis waarvan persoonsgegevens verwerkt mogen worden: 1. Toestemming 2. Overeenkomst 3. Wettelijke verplichting 4. Vitaal belang 5. Publiekrechtelijke taak 6. Gerechtvaardigd belang
Categorieën van betrokkenen	Hier dient u aan te geven over welke (groepen van) personen gegevens worden verzameld. Bijvoorbeeld studenten, medewerkers, alumni,…
Gegevens, verzameldoel en bewaartermijnen	Per categorie van betrokkenen dient aangegeven te worden welke (categorieën van) gegevens verwerkt worden en per (categorie van) gegeven(s) dient aan gegeven te worden met welk doel deze verwerkt wordt en hoelang ze bewaard blijven.
Gebruikers/ontvangers	Degene aan wie de persoonsgegevens worden verstrekt (of toegang hebben tot die gegevens). Bijvoorbeeld degene die belast is met de verwerking ervan, een leidinggevende, een extern orgaan als de belastingdienst.