Privacy Impact Assessment (PIA)

Privacybescherming staat in toenemende mate in de belangstelling. Voor een groeiend aantal bedrijven is het zorgvuldig omgaan met persoonsgegevens een onderwerp waarmee zij zich in positieve zin willen onderscheiden van concurrerende bedrijven. Daarnaast worden de boetes ook steeds hoger, zeker op het moment dat de EU-privacy verordening wordt ingevoerd.

In het regeerakkoord (PvdA/VVD-2012) is vastgelegd dat de uitvoering van een Privacy Impact Assessment (PIA) een vanzelfsprekende maatregel is bij de bouw van systemen en het aanleggen van databestanden (Privacy by Design en Privacy by Default). Voor het meewegen van privacybelangen in de besluitvorming over de ontwikkeling van producten en diensten is het van groot belang dat dit in een vroegtijdig stadium gebeurt. Als de risico's voor inbreuken op de privacy pas worden onderkend als de ontwikkeling van het product of dienst al in een vergevorderd stadium verkeert, is de kans immers groot dat noodzakelijke aanpassingen zeer tijdrovend en kostbaar zijn.

Om organisaties een instrument te bieden om privacy risico's in een vroeg stadium op een gestructureerde en heldere manier in beeld te kunnen brengen is een Privacy Impact Assessment (PIA) een optie.

Wat is een Privacy Impact Assessment (PIA)?

Een PIA stimuleert organisaties om proactief na te denken over vragen als: Wat is de impact van het beoogde project op de privacy van de betrokkenen? Wat zijn de risico's voor de betrokkenen en voor de organisatie? Is een aanpak die minder gevolgen heeft voor de privacy ook mogelijk, gegeven de doelstellingen van het project? Na het uitvoeren van de PIA kan de 'verantwoordelijke' gerichte opdrachten geven aan degene die het product of de dienst verder ontwikkelt opdat maatwerk kan worden geleverd en wordt voorkomen dat in een later stadium kostbare aanpassingen nodig zijn.

12secure-u en PIA/Privacy

Onze organisatie is expert op het gebied van huidige en aankomende privacywetgeving. Wij zijn op de hoogte van de laatste ontwikkelingen op dit gebied en hebben jarenlange ervaring met het opstellen en uitvoeren van privacy beleid, beveiligingsrichtlijnen, bewerkersovereenkomsten, Privacy Impact Assessments (PIA's), Privacy Enhanced Technologies (PET) en toepassingen van Privacy by Design en Privacy by Default.

We kunnen uw organisatie ondersteunen bij het uitvoeren van een PIA of deze voor u uitvoeren. Hiermee biedt u uw organisatie een instrument om privacy risico's in een vroeg stadium op een gestructureerde en heldere manier in beeld te kunnen brengen.

12secure-u levert naast hooggekwalificeerde consultants met ruime ervaring in het Privacy domein ook Privacy Officers met expertise en ervaring op het gebied van gegevensbescherming. Privacy Officers kunnen in-house bij u werkzaam zijn, maar ook extern. Als u zelf een Privacy Officer heeft kan 12secure-u deze ondersteunen en voorzien

van specialistisch en hoogwaardig privacy advies. Ten slotte levert 12secure-u kant en klare oplossingen voor privacy compliance.

12secure-u maakt gebruik van de methode zoals is opgezet door NOREA, de beroepsorganisatie van IT-auditors maar kan ook een methode van uw organisatie gebruiken.

Wilt u een PIA laten uitvoeren? Bent u op zoek naar een Privacy Expert, een Data Protection Officer of een IT- consultant/IT-project manager met kennis op het gebied van de Wet bescherming Persoonsgegevens? 12secure-u heeft die voor u!

Wanneer voert u een PIA uit?

Een PIA kan het beste in een zeer vroeg stadium van een project uitgevoerd worden (Privacy by Design). Immers, als u de PIA in een vroeg stadium uitvoert, helpt de PIA u om het privacybelang mee te nemen bij het verdere ontwerp van het project. Ook aanpassingen of wijzigingen van bestaande systemen of projecten rechtvaardigen een PIA. Op die manier kunt u voorkomen dat later kostbare aanpassingen nodig zijn om alsnog de noodzakelijke beheersmaatregelen met betrekking tot privacy te implementeren. Ook wanneer de omstandigheden van een project tijdens de looptijd veranderen, is het raadzaam de PIA te herhalen en/of te evalueren bij de afsluiting van een project.

Hoeveel tijd kost het om een PIA uit te voeren?

Er zijn verschillende factoren van invloed op de tijd die het kost om een PIA uit te voeren. De belangrijkste zijn:

1. Het aantal belanghebbenden bij het project en de mate waarin deze vragen of twijfels hebben over de consequenties voor privacy.
2. De impact en het belang van het project op de organisatie en de samenleving.
3. De (technische en organisatorische) complexiteit van de verwerking.

De hoeveelheid tijd en doorlooptijd die het uitvoeren van een PIA kost, zal per PIA verschillen en hangt van veel factoren af. Het uitvoeren van de gehele PIA voor een eenvoudige gegevensverwerking zal enkele dagdelen kosten, dit is inclusief het verzamelen van gegevens en het uitvoeren van een controle. Bij complexere projecten kan dit enkele dagen zijn. Dit lijkt een substantiële investering maar daarmee kan een zeer omvangrijke schadepost worden voorkomen of beperkt. Bij het opstellen van de PIA streven wij ernaar de benodigde tijd zoveel mogelijk te beperken.

Wat levert een PIA op?

Een PIA kent een aantal belangrijke doelen, de meest belangrijke is:

1. Het voorkomen van kostbare aanpassingen in processen, herontwerp van systemen of stopzetten van een project door vroegtijdig inzicht in de belangrijkste privacy risico's.
   Daarnaast kunnen nog de volgende doelen worden onderscheiden:

2. Het verminderen van de gevolgen van toezicht en handhaving.
3. Het verbeteren van de kwaliteit van gegevens.
4. Het verbeteren van de dienstverlening.
5. Het verbeteren van de besluitvorming.
6. Het verhogen van het privacy bewustzijn binnen een organisatie.
7. Het verbeteren van de haalbaarheid van een project.
8. Het verstevigen van het vertrouwen van de klanten, werknemers of burgers in de wijze waarop persoonsgegevens worden verwerkt en privacy wordt gerespecteerd.
9. Het verbeteren van de communicatie over privacy en de bescherming van persoonsgegevens.

Wat zijn de stappen in een PIA proces?

De uitvoering van een PIA kan bestaan uit de volgende stappen:

A. Opstellen aanpak waarin o.a. bepaald wordt wie de PIA gaat uitvoeren en op welke wijze.
B. Verzamelen relevante informatie over het project om de PIA in te vullen.
C. Invullen van de PIA vragenlijst.
D. Beoordelen impact en opstellen waar nodig (aanvullende) maatregelen.
E. Opstellen van het PIA verslag.
F. Eventueel laten uitvoeren van een (onafhankelijke) toets op de PIA.

12secure-u kan u in het gehele traject ondersteunen.

De aanpak

De vragenlijst kan worden ingevuld door één persoon of door een team. Het heeft de voorkeur om de PIA door een team uit te laten voeren. De resultaten van de PIA worden daardoor beter omdat de verschillende deelnemers ieder vanuit hun eigen invalshoek het project kunnen bekijken. Voordat begonnen wordt met het uitvoeren van de PIA is het belangrijk vast te stellen wat u wilt bereiken, wie wat met de resultaten gaat doen en op welke manier de resultaten gebruikt gaan worden. De antwoorden op bovenstaande vragen worden samengevat in een plan van aanpak.

Na het opstellen van het plan van aanpak wordt relevante informatie verzameld en verwerkt. Vervolgens wordt de PIA ingevuld. De PIA is een vragenlijst op basis waarvan een aantal privacy relevante aspecten van het project (waaronder de voorgenomen handelingen met persoonsgegevens en de gegevensstromen) én de privacy impact van een project inzichtelijk worden.

Op basis van het overzicht van de risicogebieden waar de privacy van de betrokkenen mogelijk wordt geschaad kunt u een inschatting maken hoe groot de impact is binnen uw project en op uw organisatie. Vervolgens kunnen maatregelen genomen worden om de risico's te verkleinen.

Op basis van de inschatting van de impact op de betrokkenen of de organisatie, moet worden nagegaan op welke wijze de risico's vermeden of verkleind kunnen worden. U wordt

geadviseerd na te gaan of de negatieve privacy impact op de betrokkene noodzakelijk is en kan worden gerechtvaardigd. De belangen van de doelen van het project, het belang van de organisatie en het belang van het individu moeten hierbij worden afgewogen. Het vermijden of verminderen van risico's houdt overigens niet altijd in dat de projectdoelen moeten worden bijgesteld.

Naarmate de inschatting van de impact hoger wordt, is het raadzamer om maatregelen te treffen om de risico's weg te nemen of te verminderen.

De resultaten van de PIA worden vastlegt in een verslag. Op basis van dit verslag kan de gebruiker van de resultaten van de PIA eventueel noodzakelijke beslissingen nemen. Tot slot kan het raadzaam zijn dat u de PIA rapportage (en de onderliggende ingevulde PIA vragenlijst) laat reviewen. Een review kan zowel intern als extern uitgevoerd worden.

De vragenlijst bestaat uit 7 onderdelen die achtereenvolgens ingaan op:

1. Het type project.
2. De gegevens die u wilt gebruiken.
3. De partijen die betrokken zijn bij de uitvoering van het project.
4. Verzamelen van gegevens.
5. Gebruik van gegevens.
6. Bewaren en vernietigen van gegevens.
7. Beveiligen van gegevens.