Privacy Enhanced Technology

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 voor het niet zorgvuldig omgaan met persoonsgegevens ook steeds hoger, zeker op het moment dat de EU privacy verordening wordt ingevoerd. Deze zal hoogstwaarschijnlijk nog strenger zijn dan de Wet bescherming persoonsgegevens (Wbp) die momenteel van kracht is.

Privacy Enhanced Technologies (PET) kunnen een organisatie ondersteunen bij het op de juiste manier omgaan met persoonsgegevens.

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 consultants voor u!

Wat zijn Privacy Enhanced Technologies (PET)?

PET is de verzamelnaam voor verschillende technieken in informatiesystemen om de bescherming van persoonsgegevens te ondersteunen. In functionele zin is het toepassen van PET niet moeilijk. Met behulp van PET kan informatie over een persoon, zoals de identiteit en persoonlijke gegevens, worden beschermd.

PET omvat alle technische maatregelen om de privacy te waarborgen. PET kunnen bijvoorbeeld worden gebruikt om de identiteitsgegevens los te koppelen van de overige gegevens die zijn vastgelegd over een persoon. Alleen met bepaalde hulpmiddelen kan dan de koppeling worden gemaakt tussen de identificerende gegevens en de overige persoonsgegevens.

Een andere mogelijkheid van PET is het voorkomen dat er überhaupt persoonsgegevens worden vastgelegd, nadat bijvoorbeeld eenmaal de identiteit is vastgesteld. Ook kan door middel van programmatuur worden afgedwongen dat het verstrekken van gegevens altijd voldoet aan het vigerende privacy beleid (‘privacy policies’).

Privacy, PET en 12secure-u

12secure-u 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) en Privacy Enhanced Technologies.

We hebben ruime ervaring met Privacy Enhanced Technologies en we kunnen uw organisatie ondersteunen bij het implementeren ervan. 12secure-u kan uw organisatie ondersteunen bij het onderzoeken van de Privacy benodigdheden voor uw organisatie, de maatregelen op te stellen zodat u voldoet aan de EU privacy verordening door het implementeren van de juiste vorm van PET en het doorlopen van de stappen die benodigd zijn om ook in de toekomst op de juiste manier om te gaan met persoonsgegeven.

12secure-u levert naast hooggekwalificeerde projectmanagers 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 opereren, maar ook extern. 12secure-u kan verder uw eigen Privacy Officer ondersteunen en voorzien van specialistisch en hoogwaardig privacy advies. Tenslotte levert 12secure-u kant en klare oplossingen voor privacy compliance.

Wat levert PET op?

PET kan worden ingezet om de gegevensbescherming binnen uw organisatie te waarborgen. Daarnaast kan PET uw organisatie in staat stellen de risico's van inbreuken op de bescherming van persoonsgegevens beter te voorkomen en te managen. Natuurlijk zijn er ook 'gewone' privacy oplossingen, maar deze steunen vaak sterk op organisatorische en procedurele maatregelen. De gegevensbescherming is daarbij zo sterk als de zwakste schakel in het proces. Uit vele beveiligings- en privacy audits is gebleken dat mensen vaak vergeten of nalatig zijn de geëigende beveiligingsmaatregelen consequent toe te passen en te blijven toepassen.

Algemene informatiebeveiliging werkt niet altijd waardoor privacy risico's ontstaan. Men bouwt dikke en dure muren rond gegevens, maar zonder organisatorische naleving van richtlijnen en procedures voorkomt dat niet het weglekken van gegevens. Het risico wordt niet uitgesloten dat ongeautoriseerde personen toegang krijgen tot persoonsgegevens met alle gevolgen van dien. Met behulp van PET kan een organisatie aan de bron al technische maatregelen treffen en het aantal identificerende gegevens tot het absolute minimum beperken. Daar waar het niet nodig is, wordt de identiteit niet vastgelegd of wordt de identiteit losgekoppeld van de overige persoonsgegevens.

Vormen van PET

Er worden vier vormen van Privacy Enhanced Technologies onderkend:

1. Algemene PET-maatregelen. Veel organisaties passen algemene beveiligingsmaatregelen toe, zoals versleuteling, logische toegangsbeveiliging en gegevensminimalisatie. Deze algemene beveiligingsmaatregelen hebben bij de juiste toepassing ook een 'privacy enhancing'-functie.
2. Scheiden van gegevens. Scheiding van gegevens houdt in dat persoonsgegevens wel worden verwerkt, maar dat de identificerende persoonsgegevens worden losgekoppeld van de overige persoonsgegevens. Er worden ten minste twee domeinen gecreëerd: een identiteitsdomein waarin bijvoorbeeld de naam en adresgegevens worden verwerkt en één of meer pseudo-identiteitsdomeinen waarin overige gegevens als lidmaatschap of opsporingsgegevens worden verwerkt. De scheiding tussen beide domeinen wordt aangebracht en beheerd door een identiteitsbeschermer. In de praktijk is een identiteitsbeschermer een stukje software dat op een server kan staan.
3. Privacy managementsystemen. Een bijzondere vorm van PET wordt gevormd door privacy managementsystemen die zorgen voor de geautomatiseerde toepassing van privacy beleid. Dit betreft programmatuur die als het ware als een schil om de persoonsgegevens heen ligt en alle transacties die met die gegevens plaatsvinden automatisch toetst aan het privacyreglement. Deze toetsing is gebaseerd op elektronische privacy regels ('privacy policies') die zijn afgeleid uit het privacyreglement voor de betreffende database of het betreffende informatiesysteem. Door middel van een privacy codering of privacy taal worden die privacy regels in de PET-software ingevoerd.

4. Anonimiseren. Anonimiseren kan in twee stadia van de gegevensverwerking worden toegepast. Ten eerste kan worden voorkomen dat persoonsgegevens worden opgeslagen. In het geheel worden er geen persoonsgegevens verwerkt. Deze oplossing is alleen mogelijk indien voor het doeleinde van de dienstverlening het verwerken van persoonsgegevens niet noodzakelijk is. De tweede vorm is dat wanneer de persoonsgegevens tijdelijk nodig zijn, de gegevens in eerste instantie worden verwerkt en na deze verwerking worden vernietigd of losgekoppeld van de overige gegevens. Het vernietigen en/of loskoppelen moet onomkeerbaar gebeuren. Wanneer dit niet het geval is, kunnen de persoonsgegevens en overige gegevens weer gekoppeld worden en is geen volledige anonimiteit bereikt. Indien de gegevens ook van indirect identificerende kenmerken zijn ontdaan, zijn er helemaal geen persoonsgegevens meer aanwezig. Het voordeel van anonimiseren is dat gegevens die niet zijn vastgelegd, ook niet beschermd en beheerd hoeven te worden. De beheer- en onderhoudsinspanning neemt af. Daarnaast is ook niet langer de Wbp van toepassing omdat er geen persoonsgegevens verwerkt worden.

De PET-trap

Ieder van de vier mogelijke PET-vormen heeft zijn eigen voor- en nadelen en specifieke functies met betrekking tot gegevensbescherming. De ene vorm biedt meer bescherming dan de andere. In de figuur zijn de verschillende PET-vormen gepositioneerd ten opzichte van de effectiviteit van de gegevensbescherming. Daarnaast zijn in de figuur de belangrijkste eigenschappen van de PET-vormen weergegeven. De PET-trap is geen groeimodel en behoeft niet geheel ‘tot de overloop’ te worden opgelopen. Wanneer een organisatie algemene PET-maatregelen heeft toegepast, wil dit niet zeggen dat de organisatie door moet groeien naar ‘hogere’ PET vormen. De geschiktheid van de verschillende PET-vormen is situatieafhankelijk.

INVOEGEN GRAFIEK

1. Definitiestudie
   Voordat een informatiesysteem daadwerkelijk wordt ontworpen, vindt eerst een globale verkenning plaats van de belangrijkste kenmerken van het te ontwikkelen informatiesysteem. De mate waarin bescherming van persoonsgegevens noodzakelijk is, is een dergelijk kenmerk.
2. Basisontwerp
   In deze fase wordt het procesmodel gemaakt van de gegevensstromen binnen het informatiesysteem inclusief koppelingen/uitwisselingen met andere instanties. Ook het gegevensmodel moet voor iedere gegevensstroom in het verwerkingsproces van verzamelen, opslaan, bewaren tot aan vernietigen worden weergegeven.
   Belangrijke aspecten bij het opstellen van het proces- enhet gegevensmodel voor de verwerking van persoonsgegevens zijn: herkomst van de persoonsgegevens, type persoonsgegevens, type verwerkingsprocessen, aan wie de gegevens worden verstrekt, het vereiste niveau van zelfbeschikking door de betrokkenen en informatieplicht, verantwoordelijke van de gegevens, bewaartermijnen, betrokkenen bij de verwerking, etc
3. Detailontwerp
   In deze fase wordt het basisontwerp verder uitgewerkt en in meer technische zin gedetailleerd. Een belangrijk aspect hierbij is dat het technisch ontwerp van de PET-vorm geïntegreerd moet worden in het volledige technisch ontwerp van het

informatiesysteem. De PET-vorm is immers geen los toe te voegen component en daarom kan het technisch ontwerp van PET niet los worden gezien van het technisch ontwerp van het gehele informatiesysteem.

4. Ontwikkeling
   Tijdens de ontwikkeling moet worden besloten of de gekozen PET-vorm en bijbehorende technieken door de organisatie zelf worden ontwikkeld of dat er een standaardpakket wordt gekocht. Voor anonimiseren, logging en controle zijn al redelijk wat standaardpakketten op de markt. Wanneer de vorm 'scheiding van gegevens' wordt toegepast en verschillende domeinen worden gecreëerd, is het waarschijnlijk dat er een behoorlijke component maatwerk ontwikkeld moet worden. Voor het toepassen van privacy managementsystemen is standaardsoftware op de markt verkrijgbaar.
5. Testen
   Na ontwikkeling van het informatiesysteem moet uiteraard worden getest of het systeem functioneel voldoet en of de gebruikers het nieuwe systeem accepteren. In de tests moet ook de functionaliteit en de gebruikersvriendelijkheid van PET aan de orde komen. Gezien het stadium van volwassenheid van PET is het raadzaam om eerst een kleinschalige pilot te starten. Vervolgens kan op basis van de resultaten van de pilot het PET-proof informatiesysteem eventueel worden aangepast en verder worden uitgerold in de gehele organisatie.
6. Implementatie
   In deze fase wordt het informatiesysteem inclusief de PET-vorm geïmplementeerd en gaat de organisatie gebruikmaken van het PET-proof systeem. Naast de reguliere implementatie-werkzaamheden is het van belang na te gaan welke activiteiten er moeten worden uitgevoerd om PET te laten werken. In het geval van scheiding van gegevens moeten bijvoorbeeld authenticatiemiddelen worden uitgegeven, zodat gebruikers de identiteits-beschermer kunnen gebruiken.
7. Beheer en onderhoud
   Naast de beheertaken en onderhoudstaken die standaard aan de orde zijn bij een informatiesysteem en dus ook bij de PET-vorm, is er ook PET-specifiek beheer en onderhoud.
8. Evaluatie
   Het project moet worden geëvalueerd. Hiervoor kunnen een evaluatieplan en evaluatiecriteria worden opgesteld. Op basis van de evaluatie kan onder andere worden bepaald of de PET-maatregelen effectief zijn en kunnen de noodzakelijke aanpassingen aan het informatiesysteem en de PET-vorm worden verricht. Het (laten) uitvoeren van een privacy audit biedt hierbij nuttige ondersteuning als daarbij ook de PET-mogelijkheden aan bod komen. Een organisatie kan ook besluiten haar informatiesysteem te laten certificeren op basis van de Wbp.