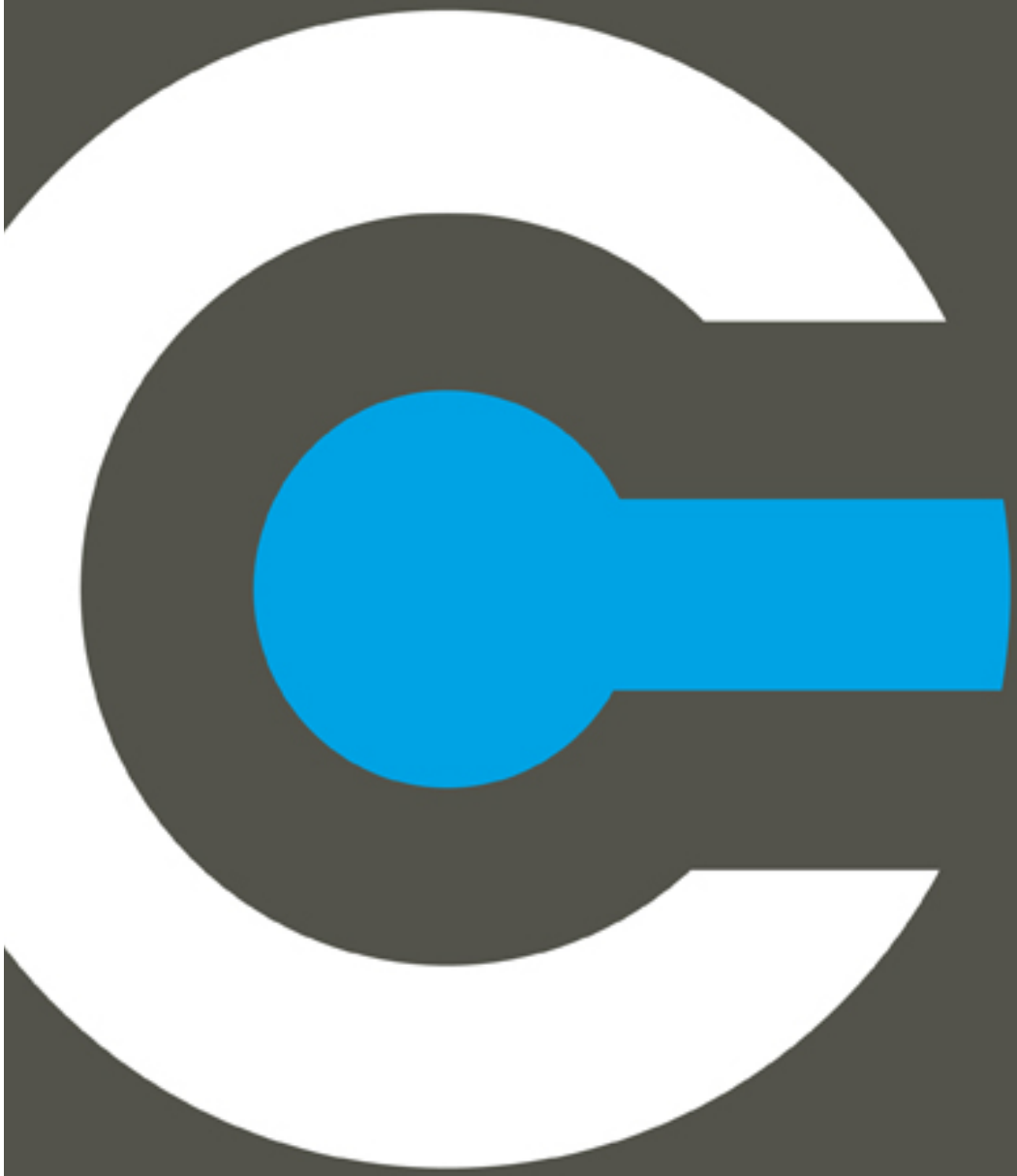
# Inventarisatie Privacy Tools

**In opdracht van ECP.NL**



**Considerati**
**24 december 2013**
**Versie 0.5**

Inhoud

# 1 Inventarisatie Privacy Compliance Tools in Nederland

Privacy is momenteel een veelbesproken begrip in Nederland. De oprukkende ontwikkeling van ICT en online diensten zorgen voor een stevig politiek en maatschappelijk debat over privacy, waarvan de uitkomst nog allerminst zeker is. Tegelijkertijd staat de techniek niet stil en ontstaan er steeds nieuwe innovatieve manieren om diensten aan te bieden met behulp van internet en nieuwe technologie. Deze veranderende wereld maakt het noodzakelijk dat wijzigingen in het wettelijk kader rondom gegevensbescherming, telecomrecht en de bevoegdheden van politie en justitie in het kader van de openbare orde en veiligheid worden doorgevoerd. In de tussentijd moeten ondernemers balanceren tussen enerzijds het verkennen van nieuwe mogelijkheden en anderzijds het opereren binnen de veranderlijke juridische kaders die gelden voor hun sector. Deze balansoefening is voor de gemiddelde ondernemer echter eerder een bron van hoofdbrekens dan een bron van inspiratie. Uiteindelijk gaat het de ondernemer om het laten groeien en floreren van zijn bedrijf.

Discussies rondom privacy en de vele veiligheidsincidenten met gegevensverwerking zorgen voor onzekerheid bij marktpartijen en consumenten. Een voorbeeld hiervan is de recente wijziging van de Telecommunicatiewet. Hierin staat dat sommige cookies vermoed worden persoonsgegevens te zijn, bijvoorbeeld omdat zij informatie over de locatie, de persoonlijke voorkeuren of andere kenmerken van een internetgebruiker bevatten. Omdat een dergelijke bepaling veel ruimte laat voor interpretatie is het voor ondernemers vaak onduidelijk wat dit betekent in de praktijk. Er is daarom behoefte aan richting en advies ten aanzien van de vraag wat er nu wel of niet kan en mag met betrekking tot verwerken van persoonsgegevens binnen een organisatie.

In deze inventarisatie laten wij zien dat er op dit gebied al veel initiatieven zijn ontplooid. Een veelgehoorde uitspraak is dat het juridisch kader rondom gegevensbescherming complex is en dat het voor veel ondernemers lastig is om dit te vertalen naar de dagelijkse praktijk. Toch zien we dat er in Nederland een aantal visionaire bedrijven zijn die – nu al – leidend kunnen zijn voor andere organisaties met betrekking tot het ontwikkelen van een intern privacybeleid dat enerzijds de klant het vertrouwen geeft dat gegevens zorgvuldig verwerkt worden en, anderzijds, bedrijfseconomisch haalbaar is.

Dit memo geeft een beknopt en schematisch overzicht van initiatieven op het gebied van praktisch privacy advies. Het gaat hierbij om het laten zien van concrete methodes, hulpmiddelen of checklists die momenteel beschikbaar zijn om de stand van zaken met betrekking tot privacy-zorg in kaart te brengen. Dit levert een beknopte lijst op van kant en klare tools die het onderwerp praktisch maken en waarmee een bedrijf of particulier direct aan de slag kan.

Dienstverlening in de vorm van advies over allerlei aspecten van privacy wordt momenteel door een groot aantal partijen aangeboden. De ondernemer moet dan echter een behoorlijke drempel overstappen, kenbaar maken aan een derde dat zijn bedrijf blijkbaar privacy zorgen heeft en wellicht ook al betalen voor het advies. Bovendien veronderstelt een behoefte aan privacy advies al een bepaalde mate van privacybewustzijn binnen de organisatie. Dit is echter niet in elke organisatie het geval. Privacy tools die men vrijblijvend kan invullen kunnen bijdragen aan bewustwording op dit terrein.

De privacy tools kunnen bestaande privacyzorgen ook verder aanwakkeren, bijvoorbeeld op het moment dat een online test tot onverwachte uitkomsten leidt.

Het doel van dit memo is dan ook om nuttige, laagdrempelige tools te signaleren, waarmee privacy awareness wordt aangewakkerd en waarmee een ondernemer of gebruiker direct aan de slag kan. Daarnaast is er de afgelopen tijd een scala van compliance checkers op het gebied van cookies op de markt gekomen. Dit aanbod is meegenomen in dit onderzoek. Dit overzicht is geen uitputtende opsomming van alle relevante initiatieven. Het doel van deze inventarisatie is het bieden van inzicht in de meest in het oog springende diensten die momenteel beschikbaar zijn voor de implementatie van het (complexe) juridische kader in de dagelijkse praktijk. Met dit overzicht schetsen we tegelijkertijd een beeld van het type dienstverlening dat ontstaat, welk soort partijen deze diensten aanbieden en in hoeverre deze producten inderdaad een goede stap richting compliance bieden voor een afnemer.

Uit deze inventarisatie blijkt dat er op dit moment nog geen sprake is van een breed aanbod aan verschillende privacy tools. Onderzoek van het Privacy & Identity Lab (PILab) (juli 2013) wijst uit dat er drie typen 'privacy tools' te onderscheiden zijn:
- Oplossingen voor het verbeteren van privacy-compliance van diensten
Denk hierbij aan best technologies en best practices die zich richten op het ontwerpen van een informatiesysteem of tools die gaan over het inrichten van de organisatie:
- Oplossingen voor het verbeteren van netwerken van organisaties en individuen
Deze oplossingen richten zich op privacybescherming door te bewerkstelligen dat er vertrouwen is tussen diverse stakeholders.
- Oplossingen voor het versterken van de positie van het data subject
Binnen deze categorie denkt het P&ILab aan best technologies en best practices die zich richten op het voorlichten van gebruikers en hulpmiddelen die een individu in staat stellen zelf zorg te dragen voor zijn of haar privacy
Voor een theoretische onderbouwing van deze onderverdeling en een uitgebreide studie naar de kansen die er zijn voor het bedrijfsleven om privacy compliance op een innovatieve en gebruiksvriendelijke manier te implementeren in organisaties en producten, zie de 'Rapportage Actieplan Privacy" PILab, juli 2013.

Echter, nog niet in alle categorieën zijn al daadwerkelijk concrete voorbeelden te noemen die hun nut in de praktijk hebben bewezen. Het overzicht van best practices op dit gebied is dan ook nog beperkt en zal er over een jaar waarschijnlijk al weer anders uit zien.
Hieronder volgt een overzicht van de best practices, zoals we die hebben verzameld in het najaar van 2013:

# 2 Voorlichting

## 2.1 Overheidsvoorlichting

### 2.1.1 College Bescherming Persoonsgegevens (Cbp) Privacy Quickscan

Het Cbp heeft een aantal documenten opgesteld om ondernemers te helpen hun niveau van compliance met de Wet bescherming persoonsgegevens (Wbp) vast te stellen. De 'Quickscan

bescherming persoonsgegevens'[1] bestaat uit 13 duidelijk verwoorde en beknopte 'ja-nee' vragen. Het gebruik van de Quickscan is niet tijdsintensief en daarom laagdrempelig. De apart te downloaden toelichting geeft per vraag aan welke betekenis het gegeven antwoord heeft voor de organisatie; is de onderneming in overtreding van de wet, of kan de huidige praktijk van de onderneming het vertrouwen van de consument in de onderneming schaden? Vervolgens geeft de toelichting advies met betrekking tot eventueel verder te nemen stappen. De Quickscan is met name gericht op het creëren van bewustwording binnen de organisatie.
De Quickscan geeft slechts een globale indruk van de status van compliance van de onderneming, want alleen de belangrijkste aspecten van de Wbp komen aan de orde. De Quickscan biedt echter een goede eerste stap in de richting van een hoger niveau van compliance. De onderneming krijgt een goede eerste indruk van hoe het met compliance gesteld is en kan van daaruit vervolgstappen ondernemen indien nodig.

Voor een uitgebreidere check en verder onderzoek naar de Wbp compliance binnen een organisatie biedt het Cbp de zogenaamde Wbp Zelfevaluatie. Tijdens een zelfevaluatie kan het management van een organisatie een oordeel vormen over de implementatie en/of naleving van de Wbp, aan de hand van de materialen en scripts van het Cbp. De bevindingen uit de zelfevaluatie kunnen eventueel gecontroleerd worden via een onafhankelijke review om meer waarde te verkrijgen. Een methode die hierbij aansluit is het opstellen van zogenaamde Binding Corporate Rules. Het gaat hierbij om het opstellen van een interne privacy gedragscode in een bedrijf of een sector, die vervolgens door het Cbp wordt gevalideerd. De privacy-toezichthouders in Europa hebben gezamenlijk dit concept ontwikkeld en richten zich met dit hulpmiddel met name op multinationals.[2]
Een laatste noemenswaardige tool van het Cbp is het 'Raamwerk Privacy Audit', gemaakt voor een gekwalificeerde auditor, waarmee een onderneming een certificaat kan halen. Toepassing van dit model vergt wel enige tijd, voorbereiding en ervaring met het doen van audits.

Het Cbp biedt naast de hier genoemde tools nog een breed palet aan voorlichtingsmateriaal en inhoudelijke informatie over privacy compliance binnen organisaties. Met name het overzichtsdocument van de zelfreguleringsproducten van het Cbp is een goed voorbeeld van praktische informatie waarmee een organisatie kan bepalen welke tool hij nodig heeft. [3]

### 2.1.2 Autoriteit Consument en Markt (ACM)

De ACM biedt op haar website een overzicht van de regels waaraan webwinkels moeten voldoen.[4] In het kader van deze inventarisatie is het advies van ACM over het gebruik van cookies door webwinkels relevant. Ook geeft ACM informatie over het opstellen van privacy-beleid binnen een e-commerce-organisatie. ACM geeft informatie in de vorm van tekst en verwijzingen naar andere platforms, zoals Consuwijzer.

[1] Te vinden via: http://www.cbpweb.nl/Pages/ind_wetten_zelfr_compliance_qs.aspx
[2] Meer informatie via: http://www.cbpweb.nl/Pages/th_doo_bcr.aspx
[3] http://www.cbpweb.nl/downloads_audit/overzicht_producten.pdf
[4] Te vinden via: https://www.acm.nl/nl/onderwerpen/verkoopmethode/webwinkels/regels-voor-webwinkels/

### 2.1.3 Rijksoverheid.nl

In 2006 heeft de Rijksoverheid een uitgebreide handleiding voor de verwerking van persoonsgegevens gepubliceerd op www.rijksoverheid.nl.[5] Deze handleiding geeft een uitgebreid overzicht van de eisen die aan gegevensverwerking worden gesteld en is geschikt voor een meer diepgaand onderzoek binnen de onderneming naar het niveau van compliance. Hoewel bij het gebruik van de handleiding rekening zal moeten worden gehouden met eventuele veranderingen in de wetgeving, biedt deze een goede basis voor een uitgebreid onderzoek. Het document is handig opgebouwd, met duidelijke flow-charts en steekwoorden aan de zijkant voor snelle navigatie. De teksten zijn redelijk technisch, maar met uitgebreide en goede uitleg.
Het nagaan van dit document zal tijdsintensief zijn voor de gemiddelde ondernemer, maar zal uiteindelijk tot een vrijwel volledig beeld van het niveau van compliance binnen de onderneming leiden. Dit heeft als voordeel dat eventuele knelpunten tegelijk kunnen worden aangepakt.

## 2.2 Keurmerken

Naast het beschikbaar stellen van informatie, is ook het uitreiken van een privacy-keurmerk een manier om voorlichting aan de consument te geven. Een consument die waarde hecht aan het keurmerk kan dit zien als een praktisch hulpmiddel om een betrouwbare dienstaanbieder te kiezen. Het verkrijgen, behouden en handhaven van een keurmerk is een intensief proces voor een bedrijf om te doorlopen. Daarmee verschilt een keurmerk wezenlijk van een checklist of een wizard waarmee eenvoudig en op hoofdlijnen een compliance check gedaan kan worden. De categorie keurmerken valt dan ook buiten de scope van dit onderzoek. We volstaan op deze plaats met het noemen van keurmerken als nuttige tools om een bedrijf concrete handvaten te bieden in de richting van privacy compliance. Drie relevante voorbeelden zijn:

- Het Privacy Waarborg, een keurmerk van de brancheverenigingen voor dialoogmarketing DDMA;[6]
- Het Privacy keurmerk van het Nederlands Privacy Instituut (NPI);[7]
- EuroPriSe, een privacy keurmerk ingesteld door de Europese Commissie.[8]

# 3 Gratis Diensten (Private partijen)

## 3.1 Bescherm je Bedrijf

Beschermjebedrijf.nl, een initiatief van Nederland ICT, biedt een online Quickscan voor bedrijven om hun niveau van informatiebeveiliging te testen.[9] De website biedt een korte vragenlijst, bestaande uit 10 vragen met 3 antwoordmogelijkheden. De Quickscan is daadwerkelijk snel gedaan en dus laagdrempelig. Daarna wordt een stappenplan doorgenomen om de onderneming te helpen bij het verbeteren van haar informatiebeveiliging. Daarnaast kan een document worden gedownload dat hulp biedt bij het opzetten van een beveiligingsplan voor het beschermen van bedrijfsprocessen, informatie en (privacygevoelige) gegevens. Deze website

[5] Te vinden via: http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html
[6] http://www.privacywaarborg.nl/voor-bedrijven/
[7] http://www.n-pi.org/tag/privacy-keurmerk/
[8] https://www.european-privacy-seal.eu/
[9] Te vinden via: www.beschermjebedrijf.nl

biedt geen specifieke privacy-check, maar richt zich meer op de informatiebeveiliging in het algemeen, met verwijzingen naar andere handige websites en documenten. Zij biedt daarom niet per se Wbp-compliance, maar zeker wel meer inzicht en structuur in (technische) informatiebeveiliging en gegevensverwerking.

### 3.2 Kennisbank ICT Issues

Op ictforyourbusiness.nl kan men een Wbp Quickscan uitvoeren om het niveau van compliance met de Wbp vast te stellen voor de eigen onderneming.[10] Daarnaast bieden zij in het artikel "De implicaties van de Wet Bescherming Persoonsgegevens op het ICT beleid" een korte uiteenzetting van de risico's, maatregelen en implicaties van de Wbp.[11] De Quickscan bestaat uit 13 vragen, gelijk aan de vragen die op de website van het Cbp worden aangeboden. De website heeft geen online invulfunctie en biedt geen verdere informatie of uitleg bij de antwoorden. De enige houvast voor ondernemers is dat wanneer een vraag met 'ja' beantwoord is, dit aangeeft dat er binnen de onderneming blijkbaar al aandacht is voor dit specifieke onderwerp, terwijl wanneer een vraag met 'nee' beantwoord wordt extra aandacht vereist is. Het is de vraag of deze tool voldoende praktische aanknopingspunten biedt om tot een hoger niveau van compliance met de Wbp te komen binnen een onderneming.

## 4 Premium Diensten

Onder een Premium Dienst verstaan we dienstverlening die is opgedeeld in twee delen. Het eerste deel is een eenvoudig standaard advies, dat gratis wordt aangeboden. Het tweede deel is een uitgebreider op maat gemaakt traject waarvoor kosten in rekening worden gebracht. Premium diensten hebben als effect dat zij in eerste instantie voor bewustwording zorgen en pas daarna een dienst aanbieden.

### 4.1 Considerati PrivacyChecker

Juridisch adviesbureau Considerati heeft een aantal online tools ter beschikking gesteld aan ondernemers om hun niveau van compliance met de Wbp vast te stellen.[12] De tools zijn overzichtelijk gepresenteerd op www.privacychecker.nl. PrivacyChecker biedt drie onderdelen:

- Privacy Impact Quick Scan. Hiermee krijgt een ondernemer snel inzicht in de mate waarin zijn product of dienst privacyrisico's meebrengt en of nader onderzoek aan te bevelen is. Aan de hand van het resultaat kan de gebruiker besluiten een Privacy Impact Assessment (PIA) te doen. In sommige gevallen is zo'n PIA wettelijk verplicht. Een PIA zorgt er voor dat de klant compliant is met deze- en andere- verplichtingen op het gebied van dataverwerking. De Privacy Quick Scan is makkelijk in gebruik en laagdrempelig.
- Wbp Compliance Scan. Deze tool geeft door middel van tien eenvoudige ja-nee vragen direct inzicht in hoe een organisatie er voor staat met betrekking tot Wbp-compliance. Doordat het resultaat meteen te downloaden is kunnen eventuele knelpunten gelijk aan het management van de organisatie worden voorgelegd. Ook is snel duidelijk welke privacy-aspecten extra aandacht vereisen. Dit maakt het aankaarten van de noodzaak

[10] Te vinden via: http://www.ictforyourbusiness.nl/?ContentId=2279
[11] Te vinden via: http://www.ictforyourbusiness.nl/?ContentId=2282
[12] Te vinden via: www.privacychecker.nl

voor veranderingen binnen een organisatie makkelijker omdat er concrete resultaten uit de Scan naar voren komen.
- Boetemeter. Deze tool is gebaseerd op de aankomende privacyverordening van de Europese Unie. De boetemeter geeft bedrijven een indruk van de maximale boete die zij zouden kunnen krijgen op basis van de nieuwe privacywetgeving. Dit zal bedrijven aansporen om op tijd maatregelen te treffen om boetes en verlies van vertrouwen in hun organisatie te voorkomen.

De tools van Considerati geven direct inzicht in aspecten van verwerking van persoonsgegevens binnen een onderneming die wellicht niet in overeenstemming met de wet zijn. Dit werkt ook op basis van alleen de gratis onderdelen. Uiteraard geven de tools een beknopt beeld, voor een uitgebreider, tailor-made advies om compliance te verhogen of voor het laten uitvoeren van een PIA biedt Considerati concrete aansluitende diensten.

## 4.2 Dirkzwager Advocaten Privacycheck

Dirkzwager Advocaten biedt een online tool bestaande uit 10 duidelijke vragen met uitgebreide uitleg om na te gaan of de gegevensverwerking binnen een onderneming compliant is met de Wbp.[13] De tool is makkelijk in gebruik en daardoor laagdrempelig. Wanneer een vraag beantwoord wordt met het 'foutieve' antwoord, stopt de tool. Aangezien bij een ongunstig antwoord compliance risico's ontstaan wordt direct aangeraden contact op te nemen met de adviseurs. Hierdoor komen in de praktijk niet alle onderdelen aan de orde in de gratis tool en wordt de gebruiker vrij snel verwezen naar betaalde onderdelen van de dienst. Voor verder advies kan contact worden opgenomen met Dirkzwager advocaten.

## 4.3 Kenniscentrum WBP

Kenniscentrum WBP biedt een online ja-nee vragenlijst met betrekking tot de verschillende aspecten van de Wbp. De vragenlijst biedt de ondernemer de mogelijkheid om aanvullingen te geven bij zijn antwoorden. Dit levert extra informatie op, waardoor een geïndividualiseerd advies kan worden opgesteld. De vragenlijst blijft dicht bij de tekst van de Wbp en is daarom redelijk juridisch. Wellicht dat het gebruik van deze dienst enige voorkennis vereist.
Een nadeel aan deze tool is dat de antwoorden via een mail naar een medewerker van het kenniscentrum worden gestuurd. Deze worden handmatig geanalyseerd, waarna een medewerker contact opneemt. In de tussentijd is de ondernemer niet wijzer, hij moet wachten op een reactie vanuit het kenniscentrum. Nadat de antwoorden zijn geanalyseerd biedt het kenniscentrum de ondernemer een aanvullend traject aan.

## 4.4 Edelman Privacy Risk Index (ePRI)

De ePRI[14] is een tool die organisaties helpt om beter inzicht te verkrijgen in hun privacy- en dataprotectierisico's. De tool vergelijkt de organisatie met organisaties die vergelijkbaar zijn wat betreft grootte, sector en geografie. Dit is mogelijk doordat de test is gebaseerd op 6,400 vragenlijsten die ingevuld zijn door privacy- en veiligheidsmedewerkers.

[13] Te vinden via: http://dirkzwagerieit.nl/privacycheck/
[14] Te vinden via: http://www.edelman.com/privacy-risks/

De tool bestaat uit twee vragenlijsten, die in ongeveer tien minuten ingevuld kunnen worden. De eerste vraagt om demografische informatie, de tweede gaat over de manier waarop uw organisatie met privacy omgaat. Dit leidt tot een anoniem rapport met het risicoprofiel van de organisatie. De gebruiker van de tool wordt na het invullen van de vragenlijsten aangemoedigd om de website met privacydiensten van Edelman te bezoeken.

### 4.5 GS1 EPC/RFID Privacy Impact Assessment tool

De EPC/RFID Privacy Impact Assessment tool[15] is een macro-enabled Excel spreadsheet waarmee, door middel van invullen, snel een overzicht verkregen kan worden in de privacyrisico's van nieuwe RFID-toepassingen binnen het bedrijf. RFID is een technologie waarmee op afstand informatie opgeslagen en afgelezen kan worden van zogenaamde RFID-tags die op of in objecten of levende wezens zitten. Hierbij kunnen ook persoonsgegevens van klanten verwerkt worden. De tool richt zich op MKB's.

## 5 Betaalde Diensten

Diverse partijen bieden dienstverlening over de implementatie van privacyrecht in een bedrijf. Vanwege het ontbreken van een "preview", zoals dat bij de premium diensten gebeurt, hebben deze diensten een iets minder laagdrempelig karakter. Er is al snel een kennismaking met het bedrijf nodig. Hieronder een overzicht van aansprekende dienstverleners.

### 5.1 ICTRecht Websitescan/Bedrijfsscan

ICTRecht biedt een volledige websitescan aan, waarbij onder andere compliance met de Wbp en het gebruik van cookies onder de loep wordt genomen.[16] Vervolgens adviseren zij de onderneming over de uitkomsten van de scan. Bij ICTRecht kan een webwinkel daarnaast een certificering halen om aan te tonen dat deze aan de wet- en regelgeving voldoet. Ook biedt ICTRecht diverse zelfhulp-boeken op het gebied van privacy en compliance aan.[17] Met behulp van deze boeken kunnen ondernemers achterhalen of de gegevens die zij verzamelen persoonsgegevens zijn en hoe deze dienen te worden beveiligd.

### 5.2 Cordemeyer en Slager Advocaten

Cordemeyer en Slager Advocaten biedt een Quickscan voor webwinkels, waarmee zij juridische documenten kunnen toetsen op compliance.[18] Daarnaast kan een ondernemer bij Cordemeyer en Slager Advocaten terecht voor uitleg en toelichting op de verschillende privacy vraagstukken.

### 5.3 Duthler Associates

Duthler Associates heeft een volledig werkproces opgezet om ondernemers zo goed mogelijk te helpen bij het verhogen van hun compliance met de Wbp, bestaande uit een tien-stappen Privacy Impact Assessment.[19] In een factsheet[20] hebben zij de belangrijkste aspecten van een

[15] Te vinden via: http://www.gs1.org/epcglobal/pia/
[16] Zie: https://webwinkelrecht.nl/diensten/juridische-producten/juridische-scan/
[17] Te vinden via: https://ictrecht.nl/boeken/privacy/
[18] Te vinden via: http://www.cordemeyerslager.nl/quickscans/quickscan-it-overeenkomsten
[19] Te vinden via: http://www.duthler.nl/nl/node/270 of deze: http://www.duthler.nl/node/325
[20] Zie: http://www.duthler.nl/sites/default/files/130411%20Factsheet%20PIA.pdf

PIA op een rij gezet: waarom een PIA nodig is, voor wie een PIA belangrijk is en wat het oplevert. Het doorlopen van de tien-stappen PIA van Duthler Associates zal zeker de compliance binnen een organisatie verhogen, maar het lijkt een vrij tijdsintensieve methode, waardoor naar verwachting de kosten voor de afnemer snel oplopen.

### 5.4 Magpie Solutions

Deze organisatie biedt een 'pre-scan' aan waarbij de Wbp bij medewerkers wordt geïntroduceerd.[21] Wbp-specialisten kunnen helpen bij de juridische en administratieve invoering en borging van gestelde privacy-doelen. Voor grote organisaties bieden ze de 'Magpie Wbp-applicatie' aan. Deze tool genereert documenten die een audit van het CBP kunnen doorstaan en geeft aan of je in overeenstemming met de Wbp werkt.

### 5.5 SECWATCH

SECWATCH biedt op hun website een korte uitleg van persoonsgegevens en de vereisten van de Wbp. Om compliance binnen de onderneming te verhogen biedt SECWATCH de Wbp privacy audit aan, waarmee een duidelijk beeld wordt gegeven van de huidige situatie in een bedrijf, waarna wenselijke en noodzakelijke verbeterpunten worden uitgelicht. Daartoe moet wel contact met het bedrijf worden opgenomen.

## 6 Betaalde privacy tools

Bij het zoeken naar betaalde tools hebben we de afbakening gemaakt naar tools die de ondernemer concreet helpen om privacy in zijn bedrijf te implementeren en daarmee aan de privacywetgeving te voldoen. Het blijkt echter dat er op dit moment weinig van zulke tools zijn. De inventarisatie leverde in elk geval te weinig op om al va best practices te kunnen spreken. Wel worden er tools ontwikkeld, zoals SWELL van Novay, maar deze is momenteel nog niet verkrijgbaar. Daarnaast zijn er security tools op de markt, zoals de onderstaande van Aon, waarmee ook een aantal privacy-issues geadresseerd kunnen worden. Een best practice op het gebied van *privacy* kan dit echter nauwelijks genoemd worden, omdat de tool zich primair op security richt. Het verenigen van een data governance tool met een security tool is in de praktijk lastig, omdat de expert op het ene gebied geen expert is op het andere gebied. Hier is wetenschap voor nodig. PILab heeft zich in haar Actieplan Privacy het doel gesteld om deze brug te slaan en in kaart te brengen wat hier voor nodig is. Dit project zal in het voorjaar van 2014 haar eerste resultaten opleveren.
Wij merken tot slot op dat tools die zich uitsluitend op security richten op zich ook een positieve bijdrage kunnen leveren aan privacy compliance van een bedrijf, omdat het op orde hebben van de security een vereiste is uit de Wet bescherming persoonsgegevens.

### 6.1 SWELL

Onderzoeks- en adviesorganisatie Novay biedt diensten aan op onder andere het gebied van identity, privacy en trust. Daarnaast is Novay betrokken bij SWELL, een project dat intelligente tools ontwikkelt om de werkdruk van kenniswerkers te verlagen.[22] De tool moet de kenniswerker controle en inzicht geven in wie welke persoonlijke informatie wanneer nodig heeft. Een dergelijk inzicht raakt nu al snel verloren door de grote hoeveelheid mobiele apps die

[21] Voor een demonstratie van deze tool, zie: http://www.magpiesolutions.nl/screenshots/index.html
[22] Zie: http://www.novay.nl/projecten/swell/67101

toestemming vragen voor het gebruik van allerlei informatie. SWELL probeert een privacy oplossing te bieden die gebruikersvriendelijk is, tegemoet komt aan de persoonlijke wensen van de gebruiker en tevens de situationele context in ogenschouw neemt. Momenteel is dit project nog in ontwikkeling.

### 6.2 Cyberrisicotool van Aon

Risicoadviseur en verzekeringsmakelaar Aon lanceerde in september een nieuwe diagnosetool voor cyberrisico's.[23]
De tool anticipeert op de inwerkingtreding van de EU Privacy Verordening, met strengere eisen op het gebied van informatiebeveiliging en dataprivacy. Twee belangrijke elementen daaruit zijn de meldingsplicht voor datalekken en hoge sancties bij het niet nakomen daarvan. De tool helpt risicomanagers om bewustwording binnen de organisatie te vergroten en inzicht te geven in de gevolgen.
Op basis van diverse meerkeuzevragen beoordeelt de tool het technologiegebruik van medewerkers, de huidige controlestructuur en het standpunt van directie of bestuur ten opzichte van cyberrisico's in een organisatie. De tool geeft een overzicht van de belangrijkste cyberrisico's en begeleidt de ontwikkeling van controlestructuren die essentieel zijn voor een effectieve strategie op het gebied van cyberrisicomanagement.

## 7 Privacy awareness tools

Uit het vorige hoofdstuk bleek al dat er momenteel geen concrete tools op de markt zijn die de ondernemer helpt bij het implementeren van privacy(wetgeving). Wel zijn er tools op het gebied van privacy awareness. Deze richten zich met name op het gebruik van cookies. Hieronder zetten wij enkele van zulke tools op een rij.

### 7.1 Evidon InForm

InForm van Evidon geeft internetgebruikers duidelijke informatie over advertenties in browsers, zoals gegevens van de bedrijven achter de advertenties en welke bedrijven gegevens verzamelen. Ook assisteert de tool bij het geven van toestemming voor het plaatsen van cookies. De tool assisteert bedrijven bij het naleven van het Self-Regulatory "AdChoices" Program. Dit programma is opgezet om ervoor te zorgen dat bedrijven in de Verenigde Staten transparant zijn naar gebruikers toe, om zo te voorkomen dat strengere overheidswetgeving noodzakelijk is.
http://www.evidon.com/inform

### 7.2 Evidon Analytics

Analytics is een tool voor websitehouders en biedt de mogelijkheid om third party tracking op je website te managen. Hierdoor heb je de controle over welke gegevens er verzameld en

[23] Zie: http://www.aon.com/netherlands/persberichten/2013/30-9-2013-Aon-lanceert-diagnosetool-cyberrisico-s-op-FERMA.jsp

doorverkocht worden en biedt de tool de mogelijkheid om de privacy van bezoekers te beschermen.
http://www.evidon.com/analytics

### 7.3 Ghostery

Ghostery is een tool die internetgebruikers controle geeft over hun privacy tijdens het browsen op internet. Ghostery geeft een overzicht van onder andere cookies, tags, web bugs en pixels die geplaatst worden door websites en advertentienetwerken. Gebruikers hebben de mogelijkheid om deze websites of advertentienetwerken vervolgens te blokkeren.
http://www.ghostery.com

# 8 Diensten met betrekking tot Cookies

## 8.1 Hulpbijcookies

Hulpbijcookies biedt websites een Quickscan om te achterhalen welke cookies de website gebruikt. Daarna wordt een Cookie Policy opgesteld en een Cookie Proof plugin geïnstalleerd zodat de website voldoet aan de wetgeving.
De kosten voor dit traject zijn €185-€245.
http://www.hulpbijcookies.nl

## 8.2 Social Mingle

Op Social Mingle kun je voor €75,- een cookiemelding op je website laten plaatsen.
https://socialmingle.net/nl/

## 8.3 Zanox

Zanox biedt een complete Cookie Tool Generator. Deze tool laat ondernemers direct en gratis een script genereren waarmee zij een cookiemelding op hun website kunnen plaatsen die conform de Nederlandse wetgeving is.
http://toolbox.zanox.com/cookiewall/

## 8.4 Idvos

Idvos biedt verschillende diensten aan met betrekking tot cookies. Naast algemene informatie op hun website verwijzen zij naar websites van andere instellingen voor nadere informatie. Daarnaast bieden zij cookiemeldingen voor websites/webshops en cookie analyses.
http://www.idvos.nl/cookies-wet-eu-nl-regelgeving#aanvraag

## 8.5 Optanon ePrivacy

Optanon biedt een oplossing voor websites die aan de Europese cookieregels willen voldoen. Door enkele regels code te implementeren heeft de gebruiker de keuze uit diverse manieren om om toestemming voor cookies te vragen en kan hij testen welke manier het beste werkt. De tool kost $295 per jaar.
http://www.cookielaw.org/optanon-eprivacy/

# 9 Inhoudelijke stap richting compliance

Bij de inventarisatie van best practices is specifiek stilgestaan bij de vraag in hoeverre de tools daadwerkelijk bijdragen aan de *privacy maturity* van de organisatie die de tool gebruikt. Aspecten die hierbij een rol spelen zijn: het genereren of versterken van privacybewustzijn van de gebruiker, het hebben van concrete handvaten om een goed privacybeleid op te stellen en het bieden van een manier om de compliance te versterken. Wanneer we deze aspecten beschouwen als samenhangende onderdelen van een groter geheel, spreken we over de mate van volwassenheid van privacyzorg binnen een organisatie: de privacy maturity. Idealiter dragen de diverse tools hieraan bij. Een randvoorwaarde hiervoor is uiteraard dat de tools de gebruiker wijzen op de basisvereisten van het gegevensbeschermingsrecht.[24]
Deze basisvereisten die in de tools aan de orde moeten komen zijn:

- Duidelijkheid over welke gegevens worden verwerkt;
- Het formuleren van heldere doelen waarvoor gegevens worden verwerkt;
- Het hebben van een legitieme grondslag voor de verwerking: dit is in de praktijk meestal een overeenkomst waarin dat expliciet vermeld is, de toestemming van de consument of een redelijk belang van de organisatie;[25]
- Degene over wie de persoonsgegevens iets zeggen, de betrokkene, heeft recht op informatie over de verwerkingen en recht op inzage in de gegevens die verwerkt worden;
- De betrokkene heeft ook recht op correctie, wijziging of verwijdering;
- Het nemen van beveiligingsmaatregelen op het gebied van software, ICT-infrastructuur, personeelsbeleid, autorisaties, toegang tot de persoonsgegevens en toegang tot de gebouwen; Uit het onderzoek blijkt dat dit onderdeel zich bevind op het terrein van IT security. Op het gebied van security zijn vele tools, hulpmiddelen en diensten op de markt. Aangezien zij zich niet specifiek richten op privacy zijn deze tools buiten beschouwing gelaten.
- Bewaartermijnen van de gegevens;
- Informatie over het delen van gegevens met andere organisaties, bijvoorbeeld om de gegevens te bewerken of verrijken, of omdat er een samenwerking of handelsrelatie is met de derde partij;
- Voor de cookie-tools geldt dat minimaal aandacht besteedt moet worden aan informatieverstrekking aan het publiek en het implementeren van een adequate manier om toestemming voor het gebruik van cookies te verkrijgen van de betrokkene.[26]

[24] Met name de Wet bescherming persoonsgegevens (Wbp) en het grondrecht op bescherming van de persoonlijke levenssfeer, art. 10 Grondwet
[25] De mogelijke grondslagen staat limitatief opgesomd in art. 8 Wbp
[26] De basis van het wettelijk kader voor het gebruik van cookies is art. 11.7a van de Telecommunicatiewet. NB: Deze bepaling is momenteel onderwerp van een wetswijziging.

## 10 Overzicht

In de onderstaande tabel zijn de bovengenoemde diensten in een overzicht opgenomen.

| | INFORMATIE-BLAD/ FACTSHEET | VRAGENLIJST/ ZELFCHECK | WIZARD/ INSTANT ADVIES GENERATOR | VERWIJZING NAAR ADVIES-GESPREK/ AFNEMEN DIENST | WEBSITESCAN / BEDRIJFSSCAN | COOKIE-DIENSTEN |
|---|---|---|---|---|---|---|
| ETAALDE DIENST | | | | ICTRecht, Cordemeyer en Slager Advocaten, Considerati, Duthler Associates, DirkZwager Advocaten, Magpie Solutions, SECWATCH | ICTRecht, Cordemeyer en Slager Advocaten | Hulpbijcookies, Social Mingle, Idvos, |
| REMIUM DIENST | | Kenniscentrum WBP | Considerati Privacychecker, Dirkzwager Advocaten Privacycheck | | | Bite the Lemon |
| GRATIS DIENST | Bescherm je Bedrijf | Bescherm je Bedrijf, ICT Issues | | | | Zanox |
| OVERHEIDS-VOORLICHTING | Handleiding WBP Rijksoverheid | CBP QuickScan, Handleiding WBP Rijksoverheid | | | | |