

Zelfevaluatie Privacy bij de Nederlandse Staatsloterij

Drs. A.C. Ruoff

De Nederlandse Staatsloterij is in de loop van 2000 in gesprek geraakt met de voorganger van het College Bescherming Persoonsgegevens, hetgeen in december van dat jaar heeft geleid tot de start van een onderzoek: de Zelfevaluatie Privacy (ZEP)¹, als onderdeel van een 'proef' van de toenmalige Registratiekamer en als voorbereiding op de nieuwe privacywet, de Wet bescherming persoonsgegevens (Wbp)².

Dit onderzoek is bij de Staatsloterij het begin geworden van het privacyproject. Dit artikel beoogt met de beschrijving van deze praktijkcase inzicht te geven in benodigheden, opbrengsten en risico's van de nieuwe privacywetgeving voor de bedrijfsvoering. Het is te beschouwen als een illustratie bij het artikel 'Auditor en privacy' van Van Gils en Leentveld in Compact 2001/4.

in het land. De activiteiten vinden in Nederland plaats, zoals is aangegeven in de Wet op de kansspelen en de vergunning voor de Staatsloterij.

Van de inleg of omzet, die dit jaar circa 650 miljoen euro zal bedragen, komt ongeveer tweederde deel weer naar de klanten terug in de vorm van prijzen. De organisatie is opgedeeld in commerciële afdelingen, een ICT-afdeling en een afdeling Financiën, een staf, waaronder Voorlichting en Public affairs, Juridische zaken, Corporate planning, een Bibliotheek en het Kansspelmuseum. De Staatsloterij besteedt bepaalde activiteiten uit, zoals delen van systeemontwikkeling, klantenservice via call-centers, data-entry, voice response-systemen en telemarketingactiviteiten.

1) Zie de publicatie *WBP Zelfevaluatie*, Samenwerkingsverband Audit Aanpak, Werkgroep Zelfevaluatie, p.a. College Bescherming Persoonsgegevens; bèta-versie (4.0), november 2000; versie 1, april 2001. De bèta-versie (4.0) van het Samenwerkingsverband is gebruikt voor de zelfevaluatie bij de Staatsloterij. Ook van dit samenwerkingsverband, Werkgroep Zelfevaluatie, verscheen het *Raamwerk Privacy Audit*, College Bescherming Persoonsgegevens; versie 1, april 2001. Dit raamwerk dient als handleiding bij het uitvoeren van privacyaudits. Beide publicaties zijn te vinden op de website van het CBP, link: www.cbppweb.nl, onder de tab 'Audit'.

2) *Wet Bescherming Persoonsgegevens*, Staatsblad 2000 302, Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens, 20 juli 2000. Deze tekst is te vinden op de website van het ministerie van Justitie, link: www.justitie.nl onder 'publicaties'.

3) Anoniem houdt in dat slechts een klein team bij de Staatsloterij toegang heeft tot de gegevens van prijswinnaars. Gegevens over prijswinnaars komen alleen in geaggregeerde (het aantal en bedrag van gewonnen prijzen) of geanonimiseerde vorm (de prijs is gevallen in de stad Utrecht, of het lot is verkocht bij verkooppunt X) naar buiten.

Inleiding

Onder andere bij het bepalen van de strategie van de Staatsloterij – begin 2001 – is gebleken dat persoonsgegevens van klanten, maar ook van personeel en zakelijke relaties, voor de Staatsloterij erg belangrijk zijn. De Staatsloterij is zich terdege bewust van haar kwetsbare imago bij de Nederlandse consument. Persoonsgegevens spelen een rol in de administratie van de loterij en zijn door de privacywetgeving gebonden aan nieuwe beschermingsvoorschriften. Dit artikel behandelt de motieven van de Staatsloterij om met de 'privacyproef' mee te doen en gaat daarna in op de gevolgde werkwijze. Het directe resultaat van de zelfevaluatie was inzicht in hoe de Staatsloterij op dat moment omging met persoonsgegevens.

Na de zelfevaluatie organiseert de organisatie de follow-up van dit project; zowel naar de medewerkers in de zin van bewustmaking, naar de bedrijfsvoering in de zin van rationalisering als naar zakenpartners in de zin van standaardisering. Ook de 'spin-off' van het project in de vorm van bewustwording, rationalisering en het expliciet maken van 'betrouwbaarheid' is een belangrijke reden geworden om van de bescherming van privacy werk te maken.

Wat doet de Staatsloterij?

De Staatsloterij organiseert niet alleen elke vier weken een Staatsloterij, waarvoor bijna de helft van de Nederlandse huishoudens één of meer loten in huis haalt, maar ook de jaarlijkse Oudejaarsloterij en sinds augustus vorig jaar de wekelijkse loterij Dayzers, een 'geluksdagloterij'. Daarnaast organiseert TicketBox – een afdeling van de Staatsloterij – de verkoop van toegangskaarten voor de grote voetbalwedstrijden in opdracht van de betaaldvoetbalorganisaties, en van grote concerten en evenementen, zoals in de ArenA en Ahoy. De Staatsloterijorganisatie heeft ongeveer 130 personeelsleden in dienst en de beschikking over ruim 3000 verkooppunten

Motieven voor de Zelfevaluatie Privacy

Klanten vormen de kurk waarop de Staatsloterij drijft. Klant- of consumentgegevens zijn dus van levensbelang voor de Staatsloterij en haar dienstverlening. Van ongeveer 1,6 miljoen klanten zijn persoonsgegevens vastgelegd, zoals NAW's en bank- of girorekening, omdat de Staatsloterij voor abonnees of 'automatische' spelers gebruikmaakt van incassomachtigingen.

Van nog eens tussen de twee en drie miljoen klanten zijn die gegevens niet aanwezig, omdat die het loterijproduct kopen bij de 'wederverkoper'. Die wederverkoper is misschien wel de belangrijkste dienstverlener van de Staatsloterij. Van hem en van andere dienstverleners gebruikt de Staatsloterij ook persoonsgegevens. Denk daarbij aan de organisaties waarmee overeenkomsten zijn gesloten zelf, hun vertegenwoordigers en contactpersonen.

Het imago bij de klant en dus bij het grote publiek kan de Staatsloterij maken en breken. Zo ook de wijze waarop de organisatie wederverkopers, klanten en prijswinnaars behandelt. Die laatste groep wordt hier apart genoemd, omdat in kansspeland een tweedeling bestaat, die wordt bepaald door het gebruik van de publiciteitswaarde van de prijswinnaars en de bescherming van de privacy van prijswinnaars. Bij de Staatsloterij is de prijswinnaar anoniem³.

Het commitment van de directie bij privacy ligt besloten in de motieven imago en betrouwbaarheid. Twee van de kernwaarden van de Staatsloterij waarbij die motivatie aansluit zijn 'de klant centraal' en 'betrouwbaarheid'.



4) Een privacycertificaat bestaat nog niet. In de 'Audit aanpak' van het CBP (2001) onderkent de werkgroep Privacy Audit van het Samenwerkingsverband een intern gericht economisch motief en een extern gericht maatschappelijk motief. Beide zijn voor de Staatsloterij van belang gebleken. In hoofdstuk II van de Audit aanpak is het certificaat benoemd als middel om aan betrokkenen aan te tonen, dat de organisatie zorgvuldig omgaat met de bescherming van persoonsgegevens. Tevens verwijst de aanpak naar een accreditatieschema.

5) *Memorie van toelichting*, Tweede Kamer, vergaderjaar 1997-1998, 25 892, nr. 3.
N.B. Praktischer en beknopter is: *Handleiding voor verwerkers van persoonsgegevens*, L.B. Sauerwein en J.J. Linne-man, ministerie van Justitie, januari 2001.
Deze tekst is te vinden op de website van het ministerie van Justitie, link: www.justitie.nl onder 'publicaties'.

Zo is privacy voor de Staatsloterij een 'unique selling proposition' in de loterijmarkt. Een privacycertificaat⁴ moet die positie op den duur bevestigen.

Tijdens de zelfevaluatie is gebleken dat de kwaliteit van het bedrijfsproces baat heeft bij goed onderhouden gegevens, niet bij overbodig bijgehouden administraties. Op die manier vraagt de Wbp van de Staatsloterij dus rationalisatie, waarin de organisatie ook een belangrijk motief is gaan zien voor het privacyproject.

Werkwijze Zelfevaluatie Privacy

De Zelfevaluatie van het CBP is een complete handleiding en levert de inhoudelijke vragen die nodig zijn om inzicht te krijgen in de praktijk rondom de persoonsverwerkingen in relatie tot de wet. Zoals de naam al aangeeft is deze methode geschikt om zelf uit te voeren. Het voordeel daarvan is de ontwikkeling van kennis en bewustzijn bij de eigen organisatie. Toch blijft het een vrije keuze om hiervoor externe deskundigen in te schakelen. De Staatsloterij heeft voor de zelfevaluatie een interne projectleider en een jurist, parttime, ingeschakeld. Onder meer het product van de zelfevaluatie is met het CBP besproken. De vragenlijst bij de methode geeft de onderwerpen van gesprek aan. Alle afdelingshoofden en een aantal managers zijn geïnterviewd (totaal 24 interviews) aan de hand van de vragenlijst.

Wat is bij het onderzoek 'Zelfevaluatie Privacy' nodig? De voorwaarden om de zelfevaluatie tot een goed einde te brengen hebben vooral te maken met een open houding ten opzichte van het onderzoek en kennis, die de onderzoekers al doende vergaren.

* Kennis van bestaande richtlijnen voor personeel en contracten en wijzen van samenwerking met dienstverleners is nodig. Personeel behoort zorgvuldig met vertrouwelijke gegevens om te gaan; dienstverleners hebben als bewerkers een belangrijke rol in een aantal verwerkingen van persoonsgegevens. Ook voor hen geldt de eis van vertrouwelijkheid.

* Kennis van systemen en processen, in casu van de 'corebusiness'. De systemen van de Staatsloterij zijn ingericht op het optimaal ondersteunen, beveiligen en controleren van het loterijproces, niet primair op het vernietigen van gebruikte informatie als die niet meer nodig is voor het bedrijfsproces. Dit is wel één van de eisen die de Wbp stelt aan verwerkingen van persoonsgegevens, zoals die van loterijspelers.

Het onderzoek

Het privacyonderzoek⁶ levert via het houden van interviews de antwoorden op de vraagpunten uit de zelfevaluatie:

1. De melding

Kijkend naar (de voorbereiding op) de melding van de persoonsregistraties komt direct de vraag welke registraties moeten worden gemeld, en wat van die registraties gemeld moet worden. Kortom: Wat valt er precies onder de wet?

* Grote geautomatiseerde registraties zijn het duidelijkst: van consumenten, loterijdeelnemers met een machtiging voor incasso, prijswinnaars en wederverkopers. Vaak zijn van die geautomatiseerde administraties ook dossiers in archiefkasten bewaard. Die vallen er ook onder.

* De beheerder van het pasjessysteem dacht in zijn onschuld dat cameratoezicht en pasjesgebruik 'toch niets met privacy te maken hebben'. Bij nader inzien wel degelijk: camera's leggen beeldmateriaal vast, dat uniek herleidbaar is naar individuen, of dat nu personeelsleden zijn, gasten of klanten.

* Iedere geïnterviewde heeft wel een lijstje van zakelijke relaties. Soms is dat samengevoegd in een kerstkaartenbestand. Daarbij is het onderscheid tussen zakelijk, persoonlijk en huiselijk gebruik⁷ van belang. Met name voor de vraag wat men zoal bijhoudt: of daar bijzondere⁸ gegevens bij zijn en of die gegevens beschikbaar zijn voor anderen. Huiselijk gebruik valt buiten de beschouwing van registraties van de Staatsloterij, maar persoonlijk gebruik van centraal vastgelegde bestanden maakt het niet mogelijk bijvoorbeeld bijzondere gegevens vast te leggen.

2. Transparantie

Bij de vraag naar transparantie wordt duidelijk of wel altijd het doel wordt vermeld waarvoor gegevens worden verzameld en vastgelegd, bijvoorbeeld bij persoonlijke benadering zoals via direct mail.

3. Doelbinding

Bij de vraag naar het gerechtvaardigd doel komen eigen doelstellingen en de rechtmatigheid daarvan aan bod. Onder andere is dat de vraag naar de effectiviteit en de efficiency; is een stapel persoonsgegevens wel het meest

Door camera's vastgelegd beeldmateriaal valt ook onder de Wet bescherming persoonsgegevens.

6) Zie ook het artikel *Auditor en privacy – de rol van de auditor bij de implementatie van de Wbp*, Van Gils en Leerentveld, Compact 2001/4.

7) Zie voor huiselijk, persoonlijk en zakelijk gebruik artikel 2, lid a van de Wbp.

8) Bijzondere gegevens – artikel 16 van de Wbp – hebben dezelfde lading als 'gevoelige' gegevens in de Wpr, de oude privacywet.

* Onderzoek dat tijd kost en niet direct bijdraagt aan het primaire proces, eist een goede onderbouwing naar het management en naar de geïnterviewden. Omdat voordelen en opbrengsten pas in de loop van het traject duidelijk worden, is goodwill in de organisatie nodig voor een open en constructieve samenwerking.

* Kennis van de Wbp⁵, die men verkrijgt door seminars te volgen en zich in de wet te verdiepen aan de hand van specifieke vragen of situaties, die in gesprekken en interviews naar voren komen.

* Kennis van andere wetgeving en de relatie daarvan met de Wbp. Bijvoorbeeld de vergunning, die valt binnen de kansspelwet, de archiefwet en de Wet Administratieve Verplichtingen, die voor het privacyonderzoek belangrijke gevolgen heeft gehad.

(Als onderdeel van klantgegevens kwamen de onderzoekers vanzelfsprekend 'transactiegegevens' tegen; die gegevens zijn na 'gebruik' nog zeven jaar te bewaren voor de wet (Wet Administratieve Verplichtingen). Dat maakt de Wbp-eis tot vernietiging na gebruik, althans voor deze gegevens, onmogelijk.)

geschikte middel om het doel te bereiken? Welk doel dient bijvoorbeeld een archief met dossiers van ex-personeel?

Hierbij spelen ook de Wbp-beginselen ten aanzien van de begrippen subsidiariteit en proportionaliteit. Welk doel is het meest geschikt en heeft de kleinste kans inbreuk op de privacy te maken? En staat het middel in verhouding tot het doel?

4. Rechtmatige grondslag

De vraag naar de 'Grondslag voor verwerking' is een moeilijke, omdat hierin de afweging van belangen plaatsvindt tussen zakelijke doelen en privacy van betrokkenen. Deze maakt onderdeel uit van de privacytoets⁹, die voor deze vraag te beantwoorden is. Deze toets geeft antwoord op de vraag of het gerechtvaardigd belang van de verantwoordelijke niet voorbijgaat aan het belang van de betrokkene.

5. Kwaliteit

Kwaliteit van gegevens en verwerkingen. Het inzicht dat het geen zin heeft om onbetrouwbare of verlopen gegevens te bewaren, laat staan er beslissingen op te baseren. Een case uit de krant¹⁰: Na het afrekenen bij de kassa vraagt de caissière bij de supermarkt de klantenpas van de journalist te mogen gebruiken voor de volgende klant. Anders loopt die volgende klant zijn voordeel mis. De administratie van de supermarkt heeft nu op de klantenkaart van de journalist een extra transactie. Hier zorgt menselijk gedrag bij het gebruik van een klantenkaart ervoor dat de administratie niet meer klopt met de werkelijkheid. Doordat de administratie is verstoord, is de daarop gebaseerde besluitvorming niet betrouwbaar.

6. Rechten

De vraag naar het waarborgen van 'rechten van betrokkenen' drukt de organisatie in het onderzoek op de feiten: informatiesystemen zijn daar vaak (nog) niet op ingericht. De eisen van het geven van informatie (vooraf), wijzigingen doorvoeren en het organiseren van een antwoord op het verzetrecht, het afspreken van bewaartermijn en bewaarmethode voor verschillende categorieën van persoonsgegevens, het verwijderen of afschermen, het vernietigen, het vastleggen van de bron van persoonsgegevens, leveren inzicht in technische mogelijkheden en beperkingen van bestaande hulpmiddelen en procedures. Daaruit volgen noodzakelijke aanpassingen aan bestaande en eisen voor nieuwe systemen en procedures.

7. Beveiliging en bewustzijn

Wat betreft de vraag naar passende technische maatregelen in het kader van de beveiliging was uit de vraagstelling van de zelfevaluatie niet altijd aan de geïnterviewden duidelijk of het over logische toegangsbeveiliging van systemen ging (bijvoorbeeld wachtwoorden, toegangsrechten en het gebruik daarvan) of het voorkomen van inbraak of inbreuk op privacy met grovere middelen. De privacywetgeving gaat over de bescherming van de informatieprivacy¹¹. Deze term wordt gebruikt om het onderscheid tussen de wereld van de informatie en de fysieke wereld aan te geven. Informatieprivacy is niet hetzelfde als de fysieke bescherming van personen, eigendommen en middelen, maar vraagt deels dezelfde of vergelijkbare maatregelen. Denk

aan het beveiligen van ruimten zoals computerzalen en de kamer met de personeelsadministratie.

Een aspect van het omgaan met informatie is, naast het omgaan met geautomatiseerde systemen, 'bewust omgaan met papier'. Niet altijd is duidelijk welke papieren bewaard en opgeslagen moeten worden, laat staan hoelang ze mogen worden bewaard. Dat geldt niet alleen voor e-mail die op schijf bewaard wordt. Deze problematiek is ouder. Correspondentie bewaren is soms nodig om een wettelijke verplichting of een overeenkomst na te komen, bijvoorbeeld als het gaat om papieren incassomachtigingen. Maatregelen van beveiliging gelden niet alleen voor geautomatiseerde, maar evengoed voor papieren bestanden en dossiers.

8. Bewerkers

Eén van de onderwerpen van het privacyonderzoek was het uitwisselen van bestanden met klantgegevens tussen de Staatsloterij en dienstverleners. Dit zijn de 'bewerkers' in de terminologie van de Wbp. Daarom zijn in de zelfevaluatie de diverse kanalen die de Staatsloterij gebruikt voor communicatie en distributie van gegevens, aan een veiligheidsonderzoek onderworpen.

Cases:

* Een medewerker vond op de fax een bericht van een bekende, maar bij de Staatsloterij niet nader bekende, servicefirma. Deze firma stuurde een correctie van een factuur met een waarde van circa drie ton op, waarin tevens allerlei contractuele afspraken en correcties stonden vermeld. Door een kleine fout in dit bericht – een 5 in plaats van een 2 in het faxnummer – krijgen onbevoegden gevoelige informatie in handen. Misbruik is niet uitgesloten. Zolang de ontvanger te goeder trouw is, gaat het goed. Die stelt de afzender in kennis van de fout en vernietigt de fax. Dit is een algemeen risico van faxverkeer en komt aan bod bij de zelfevaluatie, als men de verschillende communicatiekanalen aan een risicoanalyse onderwerpt bij vraag 7.

* Bewerkers – in dit geval banken – hebben soms gewoonten die de Staatsloterij als vanzelfsprekend overneemt ('fax gebruiken we toch al jaren?'). Zo biedt zij aan prijswinnaars van prijzen boven 5.000 euro de service aan om het geld telefonisch over te maken naar een bankrekening naar keuze van de klant. Het doel daarvan is de veiligheid en privacy van de klant te waarborgen. De bank vraagt de Staatsloterij dan een bevestiging van de telefonische overmaking op fax. Op dat verzoek verzond zij in het verleden de complete gegevens van de prijswinnaar en zijn prijs op de fax. Met alle risico's van de faxverzending: de fax blijft liggen, komt in verkeerde handen, komt bij een verkeerd faxnummer uit, enz. De organisatie heeft nu besloten juist in die gevallen gebruik te maken van telebanking, waarmee een meer beschermde uitwisseling van gegevens plaatsvindt. Wat voor banken heel gewoon is, is voor een prijswinnaar heel bedreigend. Een bijkomende moeilijkheid is dat faxverkeer al vóór het gebruik van e-mail een wijdverbreid en veelgebruikt hulpmiddel was. Daardoor roept het 'verbieden' ervan veel weerstand op.

* E-mail is één van de hulpmiddelen die al intensief gebruikt worden. Terug is moeilijk, althans daarvoor is niet makkelijk draagvlak te creëren. Het blijkt nog erg lastig om e-mail te beveiligen, omdat niet elke partij dezelfde beveiligingsstandaarden hanteert. Daarom heeft de Staatsloterij voorlopig naast faxverkeer ook e-mail 'in

9) De privacytoets houdt in dat de verantwoordelijke zich, voordat hij overgaat tot een verwerking van persoonsgegevens op basis van zijn 'gerechtvaardigd belang', bijvoorbeeld direct marketing, een aantal vragen moet stellen:

- Heb ik werkelijk een zakelijk belang bij deze verwerking?
- Is dit de enige manier waarop ik dit doel kan bereiken (een minder ingrijpende manier is niet voorhanden)?
- Heb ik goed rekening gehouden met de belangen van de betrokkenen?
- Heb ik goed gezorgd voor het waarborgen van de rechten van de betrokkenen (heb ik betrokkenen gewezen op hun verzetrecht)?

Pas als alle vragen positief beantwoord kunnen worden, is zo'n verwerking op deze grond, te weten gerechtvaardigd belang van de verantwoordelijke, toegestaan.

10) *NRC Handelsblad*, achterpagina, november 2001.

11) Informatieprivacy staat voor de bescherming van de informatie over personen. Daarnaast staat de bescherming van de integriteit en intimiteit van het individu, de fysieke privacy. Het beschermen van dat laatste kan wel een doel zijn van het beschermen van het verzamelen van persoonsgegevens zoals dat met cameratoezicht gebeurt.



Drs. A.C. Ruoff is sinds 1992 werkzaam bij de Staatsloterij, aanvankelijk als extern consultant voor informatieanalyse en systeemontwerp. Vanaf 1995 is hij in dienst bij de Staatsloterij. Hij is betrokken bij diverse projecten voor onderhoud en nieuwbouw, waarbij ICT een belangrijke rol speelt. In 2001 was hij projectleider van het privacyproject waarover dit artikel gaat.

de ban gedaan' voor vertrouwelijke informatie, zoals gegevens van klanten en prijswinnaars.

Het is duidelijk dat ook de veiligheid van dataverkeer via tape, cd-rom en lijnverbindingen sterk afhankelijk is van het maken en naleven van procedureafspraken. Tapes en cd's zijn gemakkelijk te kopiëren, bijvoorbeeld tijdens transport, waardoor tijdbewaking van de verzending nodig is.

9. Niet EU-landen

Gegevensverkeer buiten de Europese Unie is aan speciale regels gebonden aangezien de wetgeving in landen buiten Europa nog niet is geharmoniseerd. Deze eis is voor de Staatsloterij niet van toepassing, want de Staatsloterij is nog steeds een Nederlandse¹² loterij zonder activiteiten in het buitenland.

De Staatsloterij is zich nu bewuster van privacyaspecten in het omgaan met klanten en klantgegevens.

12) Mocht de organisatie buiten de grenzen van Nederland treden, dan is voor deze vraag van belang welke activiteiten in het buitenland plaatsvinden en op welke wijze dat gebeurt.

13) Bij de Staatsloterij geldt een 36-urige werkweek.

Inspanningen en resultaten

Voor de zelfevaluatie was gedurende ongeveer vijf maanden¹³ 75 procent van de tijdsbesteding nodig van de projectleider en 25 procent van een tweede medewerker, een jurist. Daarnaast zijn ongeveer 25 personen drie à vier uur bezet geweest door interviews en de terugkoppeling daarvan. Naast de gespreksverslagen zijn de bevindingen van de zelfevaluatie in een rapport verwerkt.

Directe opbrengsten zijn de inventarisaties van persoonsregistraties en -verwerkingen. Die zijn onderdeel geworden van het Privacykader, dat de Staatsloterij als vervolg op de zelfevaluatie heeft opgesteld en waarin onder meer de eisen aan (nieuwe) informatiesystemen zijn geformuleerd. Daarmee is het privacybeleid op schrift gesteld. Het Kader bevat de inventarisaties van bestanden en verwerkingen voor de drie categorieën personen: consumenten, zakelijke relaties en personeel. Daarnaast bevat het na de zelfevaluatie opgestelde Privacykader:

- * uitleg en een samenvatting van de Wbp voor de Staatsloterij (één hoofdstuk);
- * een hoofdstuk 'classificatie van de bestanden en verwerkingen', waarvoor ook classificatie van de persoonsgegevens nodig was;
- * doelomschrijvingen (van alle verwerkingen van persoonsgegevens);
- * een gedragscode (voor medewerkers) hoe zich in het algemeen te gedragen, en in het bijzonder hoe om te gaan met persoonsgegevens;
- * invoeringseisen bij de wet, mee te nemen in alle nieuwe projecten. Bij elk project is de toets uit te voeren: welke aanpassingen en maatregelen zijn nodig in de bedrijfsprocessen om te voldoen aan de wettelijke eisen;
- * verder: privacyreglementen voor klanten (op de sites), aanpassing van de algemene voorwaarden, conceptbepalingen voor algemene inkoopvoorwaarden.

Het Privacykader is inmiddels geaccepteerd en via het intranet van de Staatsloterij voor elke medewerker beschikbaar. Het wordt gebruikt als startpunt voor projecten, zodat de wettelijke eisen als vanzelf in nieuwe informatiesystemen en procedures worden opgenomen. En privacy is bij directiebesluit een onderdeel van het eisenpakket van nieuwe systemen en projecten, terwijl de coördinatie van privacyzaken is ondergebracht bij de afdeling Internal Audit. Het totale project, waarin de zelfevaluatie is gemaakt, het privacykader is opgesteld en de overdracht aan diverse organisatieonderdelen is geregeld, heeft tot de oplevering op 1 januari 2002 circa 1,8 mensjaar aan inspanning gekost.

Misschien wel de belangrijkste opbrengst is bewustwording van privacyaspecten in het omgaan met klanten en klantgegevens. Alleen al door het houden van interviews ontstaat hier winst: elke geïnterviewde wordt gedwongen zich af te vragen met welk doel hij de beschikking heeft over persoonsgegevens en of dat doel wel gerechtvaardigd is.

Spin-off

Tot de spin-off behoren de indirecte opbrengsten van de zelfevaluatie. Er is een gedeelde visie ontstaan: de beide motivaties 'ken je klant' en 'bescherm de gegevens van je klant' zijn nu met elkaar in evenwicht gebracht. Het 'goed vertrouwen' in de veiligheid, die – zoals algemeen binnen de Staatsloterij werd gedacht – 'toch goed geregeld' was, is nu omgezet in bewustzijn voor gevoelige gegevens en gevoel voor risico's. Dit waardevolle leertraject heeft geresulteerd in een set van regels om respectvol en beveiligd met gevoelige gegevens en risico's om te gaan, zodat iedere klant kan zeggen: 'Ik kan de Staatsloterij vertrouwen'.

Slot

Dit artikel is een aanbeveling om de Zelfevaluatie Privacy te gebruiken als toetssteen voor de praktijk van de verwerking van persoonsgegevens in organisaties. De Staatsloterij vond in de nieuwe privacywetgeving een aanleiding om zich te verdiepen in haar persoonsverwerkingen en van privacy werk te maken. De organisatie ziet betrouwbaarheid als onmisbaar deel van haar imago bij de Nederlandse consument. Privacybescherming is daarin een belangrijk element. Bij de Staatsloterij heeft de zelfevaluatie goed gewerkt als katalysator; zij heeft zwakheden in de bedrijfsvoering op het punt van privacy helder aan het licht gebracht en was een start om privacybeleid, organisatorische maatregelen en eisen aan informatiesystemen op te stellen. De toetsing in het kader van de Zelfevaluatie Privacy heeft de organisatie meerwaarde geleverd in de vorm van rationalisering, het verduidelijken van bedrijfsdoelen op het punt van persoonsverwerkingen en bewustmaking van medewerkers.