



## De Belgische Privacycommissie: “Gebruik privacy niet als joker”

Onbekend is onbemind. Privacyregelgeving wordt vaak als een last ervaren of gewoonweg genegeerd als het kan. Nochtans worden bibliotheken en archieven dagelijks geconfronteerd met privacyproblematiek. Beide zijn een onuitputtelijke bron van informatie, maar hoe ga je hier correct mee om? META vroeg het aan de Commissie voor de Bescherming van de persoonlijke levenssfeer, de Belgische Privacycommissie of CBPL. Onze Commissie is een van de data protection authorities die werkzaam zijn in alle EU-lidstaten. Voorzitter Willem Debeuckelaere, Eva Wiertz, communicatieverantwoordelijke en Sofie Ruysseveldt, documentalist van de Privacycommissie stonden ons te woord.

### Wat is de opdracht van de Privacycommissie, hoe gaan jullie te werk?

**Eva:** De Commissie is een onafhankelijk orgaan, ingesteld bij de Kamer van volksvertegenwoordigers, niet meer bij het ministerie van Justitie zoals vroeger het geval was. Onze voornaamste taak is toezien op de bescherming van privacy en meer specifiek op de verwerking van persoonsgegevens. Concreet brengen we adviezen en aanbevelingen uit over wetsontwerpen waarbij de verwerking van persoonsgegevens betrokken is. We verlenen ook machtigingen voor het gebruik van het rijksregisternummer. We houden ook toezicht op hoe de gegevensverwerking

verloopt, we behandelen klachten van burgers en verstrekken informatie en bijstand aan zowel burgers als overheidsinstellingen. De Commissie zelf is een college van acht vaste leden en acht plaatsvervangende leden, dat om de drie weken samenkomt. Het secretariaat — niet alleen juristen maar ook externe betrekkingen en de logistieke ondersteuning — ondersteunt de Commissie. Op dit ogenblik zijn we met 56 personen.

**Willem:** Daarnaast zijn er nog de sectorale comités die voor de helft bestaan uit één van die zestien mensen van de Privacycommissie en voor de andere helft uit externe



Op de foto v.l.n.r.: Sofie Ruysseveldt, Eva Wiertz en Willem Debeuckelaere. Foto: Julie Hendrickx.

Interview: Patrick Vanhoucke, Michel Vermote en Julie Hendrickx.

specialisten. En er is ook nog de Vlaamse Toezichtcommissie voor het elektronisch bestuurlijke gegevensverkeer, onafhankelijk van de Privacycommissie. De Toezichtcommissie staat in voor alle elektronische gegevensverwerking tussen alle Vlaamse besturen en bestuursniveaus. Gelet op het feit dat heel wat bibliotheken en archieven werken in een openbare omgeving, heeft die Toezichtcommissie ook wel enig belang.

**Volgend jaar bestaat de Privacywet 20 jaar. Is de wet volgens u nog altijd voldoende of zitten er een aantal hiaten in die dringend aangepakt moeten worden?**

**Willem:** Momenteel is men bezig met een herziening van de lopende Europese privacyrichtlijn. Een proces dat van start is gegaan in mei 2009. Een aantal zaken zullen gewijzigd worden, maar de basisbeginselen blijven onaangeroerd. Die basisbeginselen zijn nog altijd actueel. Men heeft 20 jaar geleden geprobeerd om een tekst te maken die technologieneutraal was en die dus niet constant herschreven zou moeten worden. En ondanks twee grote veranderingen is dat eigenlijk in grote mate gelukt. De eerste verandering is internet natuurlijk. Men heeft geen rekening gehouden met het feit dat informatie zo snel en overal ter beschikking zou zijn. De tweede verandering hangt daarmee samen: Informatie is niet langer gelokaliseerd. Vroeger had men informatie op grote spoelen of enorme dataverwerkingsystemen. Zo had je de supercomputer van de Rijkswacht. Dat was toen het rijk van de mainframes. Nu heeft iedereen een pc en data bevinden zich overal en niet meer fysiek op een bepaalde plaats. De allerlaatste evolutie is cloud computing. Het probleem is dat alles zich overal en nergens bevindt. Er zijn dus meer problemen rond bevoegdheden: “Welke wet is bevoegd, welke commissie en welke wetgever?” Dat schept een ongelooflijk aantal juridische problemen.

**“ALS BELGISCHE DATAPROTECTION AUTHORITY IN HET EUROPESE VELD HEBBEN WIJ WEL HEEL STERK DE NADRUK GELEGD OP EEN INTEGRALE EUROPESE AANPAK. MAAR WIJ STAAN DAAR VRIJWEL GEÏSOLEERD IN.”**

**Door technologische veranderingen is het moeilijker geworden om de naleving van de wet te controleren?**

**Willem:** Onze wet is eigenlijk een copy-paste van de Europese richtlijn. Dat zal moeten veranderen. Men zal andere aanknopingspunten moeten vinden qua bevoegdheid en qua regelgeving. Als Belgische dataprotection authority in het Europese veld hebben wij sterk de nadruk gelegd op een integrale Europese aanpak. De grote landen willen daar echter niet van weten. Groot-Brittannië vindt dat traditiegetrouw absolute horror.

**Klopt het dat Europa veel strikter omgaat met privacy dan de VS?**

**Willem:** Dat is zeker zo. Er zijn verschillende manieren om met privacy om te gaan, vier paradigma's. Het eerste is het marktdenken: De markt regelt alles. Is er schade — aantoonbare financiële of fysieke schade — dan wordt die vergoed door de rechtbank. Dat is de manier waarop het in de VS werkt. Een andere manier om naar privacy te kijken is het absolute veiligheidsdenken: de Patriot Act. Privacy wordt in dit geval eigenlijk alleen nog maar gebruikt om de privacy van onderzoekers te waarborgen. Elke andere vorm van privacy moet hiervoor wijken. Je hebt ook nog de markt van welzijn en geluk, diegenen die door het goede doel bezield zijn. Dat vind je in wetenschappelijk onderzoek nogal dikwijls. Zij zeggen vaak “Maar wij zijn toch goed bezig? Wij doen dit om mensen te helpen.” Of om aan een betere geschiedschrijving te doen, om de burger beter in te lichten via media en zo. “Wij doen dit met de beste bedoelingen dus val ons niet lastig met allerlei

regels, procedures en administratieve rompslomp.” Dat zou je in bibliotheken ook wel kunnen meemaken, niet? En dan heb je een vierde — wat wij verdedigen — en dat is de rechtsstatelijke aanpak waarbij je uitgaat van het paradigma van de mensenrechten. In deze traditie streef je een *balance of powers* na. Je brengt respect op voor de persoonlijke levenssfeer van mensen en hun keuzes.

**Jullie werken ook aan bewustmaking rond privacy, o.m. via de website Ikbeslis.be. Hiermee willen jullie kinderen, jongeren, ouders en scholen bewust maken van de privacyuitdagingen van nieuwe technologieën. Openbare bibliotheken willen burgers kritisch leren omgaan met informatie en ze mediawijs maken. Privacy is daar een aspect van. Op welke manier kunnen volgens u de openbare bibliotheken een bijdrage leveren tot de bewustwording rond privacy?**

**Eva:** We zouden de bibliotheken daar graag bij betrekken. Er zijn zelfs al affiches en postkaarten klaar voor in de leeszalen. Maar het probleem is: Langs Vlaamse kant is er een overkoepelend orgaan voor bibliotheken en die contacten zouden vlot kunnen verlopen maar langs Waalse kant is dat er helemaal niet. Aangezien wij een federale instelling zijn, kunnen wij niet het ene wel doen en het andere niet. Onze voorzitter en juristen geven trouwens vaak lezingen over privacy en gerelateerde onderwerpen. Dit moet ook mogelijk zijn in samenwerking met een bibliotheek.

**Klopt het dat congressen en studiedagen zich eerder richten op het wetenschappelijk historisch onderzoek en minder op die dingen waar openbare bibliotheken mee bezig zijn zoals sociale netwerksites? Heel veel gebruikers zijn zich niet altijd bewust van de privacyproblemen die zich daarmee kunnen voordoen.**

**Eva:** Het is zeker onze bedoeling om ons daar meer op te concentreren. In oktober geeft onze voorzitter een lezing bij een lokale afdeling van de Gezinsbond, specifiek over Facebook en andere sociale netwerksites: Wat zijn de privacyinstellingen? Wat is het veiligheidsbeleid? Hoe kan ik er voor zorgen dat enkel de door mij geselecteerde mensen mijn gegevens bekijken? We moeten ook zelf voldoende vertrouwd zijn met wat sociale netwerken aanbieden.

**In 2008 deed het Sectoraal comité van het Rijksregister een aanbeveling die het gebruik van de elektronische identiteitskaart in bibliotheken mogelijk maakt. Betekent dit ook dat een bibliotheek deze zonder meer als lidkaart mag gebruiken?**

**Eva:** Er zijn bepaalde beperkingen aan verbonden. Normaal gezien moet elke verwerking van persoonsgegevens bij ons aangegeven worden. Er zijn wel enkele uitzonderingen die opgesomd staan in het KB van 2001. Op een van die uitzonderingen kunnen bibliotheken zich beroepen: de leenadministratie of een klantenbestand bijhouden. Maar dat mag dan de enige verwerking zijn die bibliotheken op die gegevens toepassen. Als een bib een literaire avond wil organiseren en daarvoor uitnodigen wil versturen dan kan dat, maar dan valt dit niet meer onder de vrijstelling van aangifteplicht. Dan moet ze aangeven dat ze die gegevens ook voor andere doeleinden wil gebruiken. Of het moet voor leden bij de inschrijving duidelijk zijn dat ze ook uitnodigingen kunnen ontvangen. Of dat op het inschrijvingsformulier een vakje aangekruist kan worden: “Ja, ik wil uitgenodigd worden.” of “Mijn gegevens mogen gebruikt worden voor promotie of om mij op de hoogte te houden van nieuwe boeken.”

**Willem:** Je moet wel opletten wanneer je begint met *profiling* zoals we dat noemen ... Wanneer je mensen gaat categoriseren

op basis van wat ze uitlenen, en je die gegevens wilt verwerken en gebruiken, dan word je met die aangifteplicht en een aantal andere plichten geconfronteerd. Wanneer je dat rijksregisternummer gebruikt, moet je aan een aantal voorwaarden voldoen. Zo moet je een privacybeheer hebben en een veiligheidsconsulent.

**Blijven bibliotheken niet vaak steken op de richtlijn om een veiligheidsplan en een veiligheidsconsulent te hebben? Want in het geval van bibliotheken is er meestal een inrichtende overheid. Waar situeert zich dan het veiligheidsplan en de consulent, op het niveau van de inrichtende macht of op het niveau van de bib?**

**Willem:** Nee, dat kan de gemeente zijn. Er is geen absolute verplichting dat dit iemand moet zijn van de eigen organisatie. Dat kan ook een privéconsulent zijn. Maar wij promoten wel het idee dat de veiligheidsconsulent iemand is die in de instelling aanwezig is en die weet waarover het gaat. Ik kan mij bovendien niet voorstellen dat het opmaken van een veiligheidsplan voor een bib zo verschrikkelijk ingewikkeld is. Je hebt weinig gevoelige gegevens. En je gaat die gegevens ook niet verkopen aan uitgeverij of boekverkopers. Er zijn niet veel bibliotheken met een veiligheidsplan, maar er zijn er toch enkele.

**Sofie:** Een veiligheidsplan is niet zozeer een verzameling technische maatregelen maar wel een overzicht van mogelijke problemen in verband met veiligheid. Zo'n plan is met een hele reeks eenvoudige maatregelen en organisatorische regels — bijv. in verband met het sleutelbeheer, de beveiliging van lokalen, paswoordenbeleid ... — binnen de bib makkelijk op te stellen.

**Wat zijn de belangrijkste voorwaarden van zo'n veiligheidsplan?**

**Sofie:** Er wordt aangeraden om eerst een risicoanalyse uit te voeren. Dus: eerst een inventaris maken van welke persoonsgegevens je als bib verwerkt en welke hulpmiddelen je daarvoor gebruikt. Dan stel je een lijst op met risico's en relatieve belangen en op basis daarvan selecteer en implementeer je een aantal veiligheidsmaatregelen, zowel technische als organisatorische. Een technische maatregel is bijv. de beveiliging van je netwerk, maar kan evengoed ook een systeem van autorisaties zijn dat toegang verleent tot bepaalde informatiesystemen of apparatuur. Een beheersplan heb je ook voor veiligheidsincidenten: “Wat doe je in geval van calamiteiten? Wie is verantwoordelijk om de essentiële activiteiten van de bib terug op te starten?” Het veiligheidsplan moet vervolgens regelmatig gecontroleerd en geëvalueerd worden.

**Moet het veiligheidsplan ook vermelden hoe men intern al dan niet met bepaalde gegevens moet omgaan?**

**Eva:** Eigenlijk wel, maar dat zijn dikwijls dingen die voor de hand liggen. Er zijn altijd al een aantal afspraken: “Enkel de hoofdbibliothecaris heeft toegang tot die computer.” “Dat lokaal wordt altijd afgesloten want daar staat bepaalde apparatuur.” De voornaamste bedoeling van zo'n veiligheidsplan is om dat allemaal te formaliseren en concretiseren. Het helpt ook om daar nog eens over na te denken: Is het wel goed wat we doen? Kan het niet nog beter?

**Sofie:** Een ander aspect is dat het personeel geïnformeerd moet worden over het veiligheidsbeleid. Je moet dus als bib formeel aan het personeel mededelen “Als bibliotheek stellen wij geen klantgegevens ter beschikking van commerciële bedrijven, uitgeverij, boekhandels ...”, zodat iedereen weet hoe hij of zij moet handelen.



v.l.n.r.: Willem Debeuckelaere, Sofie Ruysseveldt en Eva Wiertz. Foto's: Julie Hendrickx.

**“HET ARGUMENT ‘PRIVACY’ WORDT VAAK ONEIGENLIJK GEBRUIKT. IK ZEG NIET MISBRUIKT, MAAR ER ZIJN ARCHIEVEN DIE SLUITEN ALS EEN OESTER. ZELFS WANNEER JE KUNT AANTONEN DAT ER GEGEVENS VAN JEZELF IN ZITTEN.”**

## ARCHIEFONDERZOEK

**Historisch onderzoek vormde een centraal aandachtspunt in de conferentie die in november 2010 (in het teken van het EU-voorzitterschap van ons land) door de Privacycommissie werd georganiseerd. Is er voor de Commissie een specifieke problematiek met betrekking tot historisch onderzoek of archiefwerking?**

**Willem:** We zijn daarmee van start gegaan omdat er vraag was uit de sector zelf. De eerste die ons contacteerde was het SOMA, het Studie- en Documentatiecentrum Oorlog en Hedendaagse Maatschappij. Naar aanleiding van een concrete rel, een discussie over een publicatie over een gewezen minister van Justitie of Binnenlandse Zaken, net voor de Tweede Wereldoorlog. De erfgenamen dreigden een procedure op te starten omdat ze niet akkoord gingen met een aantal feitelijke gegevens en appreciaties die naar voor werden gebracht door de auteurs in kwestie. In verband met die feiten hebben ze bakzeil moeten halen. De onderzoekers hebben kunnen aantonen dat alles wat ze geschreven hadden, feitelijk juist was.

**Er is de mogelijkheid om een onderzoek voorafgaand aan te melden. Dat is in dit geval blijkbaar niet gebeurd. Zorgde dat voor een andere behandeling van de kwestie vanuit de Privacycommissie?**

**Willem:** Ik denk dat de kans zeer groot was, dat wij dat onderzoek niet zouden toegestaan hebben. Als je de wet op de verwerking van persoonsgegevens neemt en het KB dan gaat dat eigenlijk over levende mensen. Maar dat is natuurlijk meer theorie dan praktijk. Want als je aan historisch onderzoek doet, gaat het vaak over iemand die al overleden is. In vele gevallen worden daar ook andere mensen in vermeld of mee geconfronteerd die wel nog in leven zijn. En dan kan het natuurlijk wel. Maar eigenlijk is die procedure — nochtans een eenvoudige — niet goed gekend. Wanneer je de toestemming hebt van de betrokkenen, moet je de procedure natuurlijk niet volgen. Wanneer je die niet kan bekomen omdat het over te veel mensen gaat, kan je dat onderzoek voorleggen aan de Privacycommissie die een soort van machtiging verleent. Wij lijsten dan een aantal voorwaarden op waaraan voldaan moeten worden.

**Een van de conclusies van de conferentie was don't overuse the privacy argument. Verschuilen archieven zich in de praktijk niet al te vaak achter het argument van privacy?**

**Willem:** Ja, dat heb ik ook al ervaren. Terwijl je privacy niet moet gebruiken als een joker. Onze machtiging opent dikwijls poorten, hoewel dat niet de bedoeling is. Wij geven die om mensen nog eens te herinneren aan de verplichtingen. Het onderzoek komt dan in een publieksregister terecht waarin iedereen dus kan nagaan waar die onderzoeker juist mee bezig is. Dat is de eigenlijke bedoeling, maar sommige archivariissen zeggen: “Ah ja natuurlijk, je hebt een toelating van de Privacycommissie.” Maar dat is dus helemaal geen toelating, het toont alleen aan dat die onderzoeker op een fatsoenlijke manier is omgegaan met de onderzoeksgegevens, dat het onderzoek voorbereid was en dat de onderzoeker de wet- en regelgeving probeert na te leven. Het blijft de verantwoordelijkheid van de archivaris om toegang te verlenen, volgens de regels van de kunst en de wetgeving die van kracht is. Er is ook nog een andere regel in de Privacywet, die eigenlijk gebruikt kan worden om toegang te forceren tot bepaalde archieven, ook al zijn die gesloten. Artikel 10 van de Wet Verwerking Persoonsgegevens geeft mij het recht — vanuit de privacyoverweging — om te weten welke gegevens verwerkt of bewaard worden, waar die vandaan komen en naar wie ze overgebracht zullen worden. Op die manier kan een individu voor zichzelf en voor zijn gegevens toegang forceren tot private archieven. Maar voor de rest blijven private archieven wat ze zijn: private archieven.

**Aan historisch onderzoek gaat natuurlijk de verwerking door inventarisatie vooraf. Ook daar lijkt er soms een overgebruik van het privacyargument. Vanuit een verkeerd begrip van de spelregels worden soms voorzorgsmaatregelen genomen, zoals het verwijderen van inventarissen uit de leeszaal.**

**Willem:** Het is soms inderdaad een beetje een overacting. Maar je hebt ook steeds meer inventarissen die via internet beschikbaar zijn en dan krijg je een compleet andere bekendmaking. Voor je het weet kom je in een zoekmachine terecht. Dan zit het spel natuurlijk helemaal op de wagen. Wij pleiten er eigenlijk wel voor om toch in gradaties toegang te geven en om niet zomaar de inventaris op internet te zetten. Wees daar voorzichtig mee. Zeker als je namen gebruikt. Natuurlijk: Hoe verder je in het verleden teruggaat, hoe dunner die privacybescherming wordt. Inventarissen kan je ook tot op de laatste detaillistische graad doen. Maar ik zie niet in hoe je over het opmaken van een inventaris discussies kunt gaan voeren. De grote vraag is de terbeschikkingstelling: Onder welke voorwaarden doe je dat? Bij het Rijksarchief wordt er nu ook gevraagd om voor de consultatie

“WANNEER JE MENSEN GAAT CATEGORISEREN OP BASIS VAN WAT ZE UITLENEN, EN JE DIE GEGEVENS WIL VERWERKEN EN GEBRUIKEN, DAN WORD JE MET DIE AANGIFTEPLICHT EN EEN AANTAL ANDERE PLICHTEN GECONFRONTEERD.”

van het archief een verklaring te ondertekenen waarin men verklaart kennis genomen te hebben van de privacyregeling. Dat is natuurlijk ‘maar’ een verklaring maar tegelijkertijd ook een good practice omdat men op deze manier toch wijst op het bestaan van die regeling en wat je in acht moet nemen. Ik denk dat het niet slecht zou zijn dat dit veralgemeend wordt. Dus ook de verplichtingen zoals die neergelegd zijn in dat KB van 2001: Je mag enkel persoonsgegevens verwerken als het anoniem kan of gecodeerd. Nu, voor historisch onderzoek is dat zelden mogelijk. En bij publicatie mag je alleen maar die persoonsgegevens gebruiken die relevant zijn voor jouw onderzoek.

**De kernbenadering van de conferentie was *From obstruction to Construction*. Waar het privacyargument nu nog gezien wordt als een vorm van belemmering van vrij en historisch onderzoek, wil de Commissie met die conferentie eigenlijk ook duidelijk maken dat zorgvuldig omgaan met privacy een constructieve attitude kan zijn.**

**Willem:** Ook omdat we dikwijls vaststelden dat het argument ‘privacy’ oneigenlijk gebruikt wordt. Ik zeg niet misbruikt, maar er zijn archieven die sluiten als een oester. Zelfs wanneer je kunt aantonen dat er gegevens van jezelf in zitten. En dat moet je eigenlijk helemaal niet kunnen aantonen. Als dat redelijkerwijze zo is, moeten ze jou toegang verlenen. Maar zitten er ook nog gegevens in van anderen dan blijft het toch nog vaak gesloten. Maar zo werkt het niet. Vandaar dat wij ook blijven herhalen: “Kijk, die regels zijn er en als je die volgt dan heb je die toegang tot die archieven.” Op die manier hopen we ook wat angst bij een aantal beheerders, bewaarders, bibliothecarissen en archivariissen weg te nemen. Als er inderdaad een veiligheidsconsulent en -plan is, dan is dat er niet om alles onmogelijk te maken,

maar wel om alles in goede banen te leiden en onderzoek en consultatie mogelijk te maken.

**Komt er op binnenlands niveau een vervolg op de conferentie waarbij de Privacycommissie een rol kan spelen?**

**Willem:** We gaan in elk geval die brochure specifiek voor archief- en historisch onderzoek afwerken. Er zijn ook afspraken gemaakt met het Rijksarchief om een aantal zaken heel concreet te regelen in verband met toegang tot gemeentelijke bevolkingsarchieven. Zo zullen de KB's van 1992 herschreven worden. En dan is er de uitwerking van de Archiefwet. U weet dat de overbrengingstermijn van 100 jaar plots is teruggebracht naar 30 jaar. Hier is een grootscheepse discussie aan vooraf gegaan. Maar nu komt de kat op de koord. Nu moeten de KB's en de uitwerking komen. We gaan dat samen aanpakken om het naar het politieke forum een zo breed mogelijke backing te geven. En er is ook het idee om een aanbeveling te formuleren naar private archieven. Maar die aanbeveling doen we niet zomaar out of the blue. Dat gebeurt in samenwerking met de sector.

**Hoe gaat u zelf met uw eigen privacy om? Bent u terughoudender geworden in het verspreiden van informatie over uzelf sinds u voor de Privacycommissie werkt? Doet uw functie u ook op een andere manier nadenken over uw privacy?**

**Willem:** Ik ben liberaler geworden. Zeer vreemd, maar het is wel zo. In de jaren tachtig heb ik — met het petje van voorzitter van de Liga voor Mensenrechten op — een artikel geschreven in een juridisch tijdschrift waarin ik pleitte voor het absolute recht voor de persoonlijke levenssfeer. De privacywetgeving was toen in opmaak. Als ik dat nu herlees denk ik bij mezelf “Oei, oei, oei, zo'n strenge houding.” (lacht) Ik gebruik Facebook bewust niet en ik let toch wel op wat ik op internet zet en wat ik rondstuur. Wat je doet op internet heeft zijn gevolgen. Ook naar de pers toe zal ik opletten wat ik zeg off the record. Ik geloof daar trouwens niet meer in, in off the record (lacht). ■

> **De Commissie voor de Bescherming van de Persoonlijke Levenssfeer heeft een vademecum uitgewerkt dat historisch onderzoekers en archivisten wil ondersteunen bij de naleving van de privacyregels. Dit vademecum zal vanaf half oktober beschikbaar zijn op de website van de Commissie (<http://www.privacycommissie.be> - rubriek “In praktijk” > “Onderzoek”), waar nu reeds een vademecum beschikbaar is dat zich meer toespitst op sociologisch en statistisch onderzoek.**

## HET VEILIGHEIDSPAN

Voor het opstellen van een veiligheidsbeleid stelde de Privacycommissie een richtlijn op: *Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens*. Het document bevat een lijst van tien actiedoelstellingen in verband met informatiebeveiliging.

Het veiligheidsbeleid is een geschreven document waarin de maatregelen en procedures voor de beveiliging van persoonsgegevens nauwkeurig worden omschreven. Dit document bestaat o.m. uit:

- een risicoanalyse;
- de geselecteerde veiligheidsmaatregelen;
- de beschrijving van de verschillende taken, verantwoordelijkheden en organisatorische

regels voor de toepassing van het veiligheidsbeleid;

- de werkwijze voor sensibilisering, informatieverstrekking en opleiding m.b.t. het veiligheidsbeleid en de in werking gestelde veiligheidsprocedures en -maatregelen;
- het beheersplan voor veiligheidsincidenten;
- de maatregelen m.b.t. controle, audit, evaluatie en verbetering van het veiligheidsbeleid.

Dit document moet door de directie worden goedgekeurd en aan alle personeelsleden en relevante externe partijen kenbaar worden gemaakt. In de praktijk wordt vaak een ingekorte versie met de belangrijkste punten van het beleid verspreid binnen de organisatie. De

volledige versie kan dan op het intranet worden geplaatst of op een locatie waar iedereen toegang tot heeft. Dit beleid moet constant worden bijgewerkt in functie van de behoeften en evoluties. Daarnaast moet de directie ook een veiligheidsconsulent aanstellen die verantwoordelijk is voor de uitvoering van het veiligheidsbeleid.

> **Uit: Sofie Ruyssveldt, ‘Privacy in openbare bibliotheken, Deel 2: praktische richtlijnen’, in: *Wegwijzer voor bibliotheken & documentatiecentra*, Brussel, Politeia, losbladig, oktober 2011, 2.7/1.**  
> **Het referentiemodel kunt u raadplegen op: <http://www.privacycommissie.be/nl/static/pdf/referentiemaatregelen-vs-01.pdf>**