Algemeen

Het begrip privacy en de wettelijke regelgeving
Bibliotheek Hoorn erkent het belang om gebruikers een zo groot mogelijke privacybescherming te bieden als binnen de grenzen van het recht mogelijk is. De eerbiediging van de privacy van de bibliotheekgebruiker is direct verbonden aan de rol van de bibliotheek in de samenleving als een onafhankelijke, laagdrempelige, betrouwbare en veilige plaats waar iedereen zich ongehinderd toegang kan verschaffen tot de aandachtsgebieden van informatie, cultuur en informatie.

Het begrip privacy heeft betrekking op verschillende aspecten van de persoonlijke levenssfeer. Er wordt onderscheid gemaakt tussen ruimtelijke, relationele en informationele privacy. De verwerking van persoonsgegevens valt onder de informationele privacy en is geregeld in de Algemene Verordening Gegevensbescherming (AVG) – de Europese opvolger van de Wet bescherming persoonsgegevens (Wbp). De AVG stelt regels voor het verzamelen en het verdere gebruik van persoonsgegevens door bedrijven en instellingen ter bescherming van de privacy van degenen die deze gegevens betreffen. Bibliotheek Hoorn volgt deze regels.

Bibliotheek Hoorn is er zich van bewust aansprakelijk te zijn voor de gevolgen van niet naleven van de wettelijke bepalingen en van handelingen die in strijd zijn met de voorschriften van de AVG. Een gebruiker kan de bibliotheek aansprakelijk stellen als hij/zij bijvoorbeeld meent dat de op hem/haar betrekking hebbende gegevens ten onrechte of zonder zijn/haar toestemming zijn verwerkt of doorgegeven aan derden. In een dergelijk geval kan gebruik gemaakt worden van de Klachtenregeling.

De AVG bepaalt dat persoonsgegevens onder andere mogen worden verwerkt:

- wanneer een gebruiker ondubbelzinnig toestemming heeft gegeven;
- wanneer de gegevens nodig zijn voor de totstandkoming en uitvoering van een overeenkomst;
- wanneer de gegevens nodig zijn voor een gerechtvaardigd belang van de bibliotheek.

Gegevens van gebruikers zijn in Bibliotheek Hoorn voornamelijk nodig in het kader van lidmaatschap en uitleenadministratie (leenovereenkomst). Het gerechtvaardigd belang om gegevens van gebruikers te verwerken kan onder meer gelegen zijn in marktonderzoek en marketing, beveiliging en de doelmatige inrichting van administratie en beheer van de bibliotheek. In dit geval zal de bibliotheek een belangenafweging maken en ervoor zorgen dat de redelijkheid van de oplossing duidelijk is en aantoonbaar kunnen maken dat voor het betreffende doel niet kan worden volstaan met geanonimiseerde gegevens. Als er geen sprake is van de totstandkoming of uitvoering van een overeenkomst en de bibliotheek ook geen gerechtvaardigd belang heeft, zal aan de gebruiker ondubbelzinnige toestemming gevraagd worden.

Doel verzamelen persoonsgegevens
Eenmaal verzamelde gegevens worden in Bibliotheek Hoorn gebruikt voor het doel waarvoor de gegevens verzameld zijn:

het doel van het verzamelen van persoonsgegevens in de bibliotheek is het kunnen uitlenen van media aan ingeschreven gebruikers, het kunnen innen van contributies en andere vorderingen, het kunnen afleveren van media en andere diensten bij gebruikers, het kunnen communiceren met gebruikers over activiteiten, producten en diensten van de bibliotheek en het kunnen uitvoeren van statistische analyses over het gebruik van diensten van de

bibliotheek. In dit kader wisselt de bibliotheek ook gegevens uit andere organisaties zoals de Koninklijke Bibliotheek (KB) (wettelijke verplichting/geen toestemming nodig), Wise en in bepaalde gevallen scholen/instellingen. Waar uit de aard van privacy nodig worden hiertoe verwerkersovereenkomsten opgesteld.

De gebruiker heeft het recht om in verband met 'bijzondere persoonlijke omstandigheden' bezwaar te maken tegen het verwerken van zijn/haar gegevens. Dit is een zogenaamd beperkt recht van verzet: de bibliotheek zal in een dergelijk geval een nieuwe afweging maken of er in dit individuele geval gehoor moet worden gegeven aan het bezwaar.

De gebruiker heeft een 'absoluut recht van verzet' in geval van direct marketing doeleinden. Aan dit recht van verzet zal door Bibliotheek Hoorn altijd gehoor worden gegeven en de verwerking zal bij een ingediend bezwaar onmiddellijk worden beëindigd.

De leenhistorie is voor alle bibliotheekleden standaard ingeschakeld. Gebruikers kunnen zo zelf nagaan welke titels zij in de loop der tijd geleend hebben. Via 'Uw gegevens' is op de website of op een publieksscherm na het intoetsen van pasnummer en wachtwoord de leenhistorie op te roepen. De gebruiker kan via de klantenservice van Bibliotheek Hoorn verzoeken de leenhistorie te verwijderen. Dit verzoek zal altijd worden gehonoreerd.

Bibliotheek Hoorn houdt een bestand bij met profielgegevens van gebruikers aan de hand van materialen die zij hebben geleend. Het doel van deze registratie is om producten en diensten van de bibliotheek te verbeteren en uit te breiden en individuele gebruikers zo goed mogelijk te adviseren en aan hun specifieke voorkeuren en interesses tegemoet te komen. Binnen Bibliotheek Hoorn heeft een beperkt aantal mensen uit aard van hun functie toegang tot de profielgegevens. Deze speciaal aangewezen medewerkers zijn daarbij gebonden aan strikte geheimhouding. Op grond van wettelijke bevoegdheden van politie en justitie kunnen deze instanties toegang verleend worden tot de profielgegevens ((zie onder Vorderingen door de politie).

Privacy aan de balie heeft betrekking op de ruimtelijke privacy bij het informatie- en advieswerk in de bibliotheek. De AVG is hierop niet van toepassing. Bibliotheek Hoorn werkt in de vestigingen met klantenservicebalies waardoor vragenstellers zoveel mogelijk in de gelegenheid worden gesteld om aan een 'eigen' balie te woord te worden gestaan. Medewerkers worden erop gewezen dat zij zich te allen tijde bewust dienen te zijn dat er wellicht anderen kunnen meeluisteren en dat zij in iedere situatie de privacybescherming van gebruikers in acht moeten nemen. De bibliotheek is niet verantwoordelijk voor (privé)documenten die door bezoekers in kopieerapparatuur of op andere wijze in de openbare ruimten dan wel (na bezoek aan) kantoorruimten worden achtergelaten. Documenten als print-outs en kopieën die zijn achtergelaten worden aan het eind van de betreffende dienst vernietigd.

Een privacy statement is opgenomen op de website. Bibliotheek Hoorn heeft een privacy coördinator.

Vorderingen door de politie/advocatuur
Als de politie Bibliotheek Hoorn benadert om bepaalde persoonsgegevens te verstrekken op grond van haar bevoegdheden in verband met de voorkoming, opsporing en vervolging van strafbare feiten vervalt een aantal eisen uit de AVG. De bibliotheek is dan verplicht mee te werken, mits aangegeven wordt op grond van welke wettelijke bevoegdheid gegevens gevorderd worden. De genoemde bevoegdheden van justitie in verband met het vorderen van gegevens hebben alleen betrekking op die gegevens die de bibliotheek normaliter zelf registreert. De bibliotheek kan dus niet verplicht worden om de gegevens nader te bewerken,

te analyseren etc. Als er geen wettelijke plicht bestaat, werkt de bibliotheek in principe niet mee.

Vorderingen door de politie of advocatuur worden uitsluitend behandeld door de teamleider van de vestiging waar de persoonsgegevens zijn ingevoerd, de privacy coördinator en/of de directeur. Medewerkers klantenservice vragen in voorkomende gevallen aan de aanvrager om een schriftelijke vordering naar de coördinator Publieksservice te sturen, waarin het wetsartikel is vermeld waarop de vordering is gebaseerd en zo concreet mogelijk de gegevens die worden gevorderd. Medewerkers verstrekken niet uit zichzelf gegevens aan politie en/of andere justitiële ambtenaren. De directeur heeft de uiteindelijke beslissing op advies van de privacy coördinator, terwijl de coördinator Publieksservice verantwoordelijk is voor de verdere afhandeling. De coördinator Publieksservice legt schriftelijk vast welke gegevens aan wie zijn verstrekt en waarom. Er worden nooit meer gegevens verstrekt dan gevorderd zijn. De schriftelijke vastlegging wordt aan de privacy coördinator in bewaring gegeven. De directeur meldt de verstrekking van de gegevens bij FOBID en het bestuur.

Vrijwilligers
Vrijwilligers van Bibliotheek Hoorn worden vanaf de inwerkprocedure op de hoogte gesteld van hun verantwoordelijkheden op het gebied van privacy. Dit is ook in hun overeenkomst vastgelegd. Bibliotheek Hoorn werkt sinds 2018 met het vrijwilligersregistratiesysteem Afas/Insite. Hierin zijn contactgegevens van de vrijwilligers die werkzaam zijn bij de bibliotheek vastgelegd, naast hun overeenkomsten en verklaringen van goed gedrag (VOG). Optioneel kunnen vrijwilligers competenties en/of wensen toevoegen. Toegang voor bewerking is voorbehouden aan de Coördinator Vrijwilligers en de medewerker Personeelszaken, net als algemene toegang.

Sollicitatieprocedure
Profielen van kandidaten op social media bekijken is niet zonder meer toegestaan. Bibliotheek Hoorn zal hier alleen toe overgaan met een duidelijke grond (zoals om te achterhalen of iemand aan specifieke functie-eisen voldoet) en niet meer gegevens verzamelen dan strikt noodzakelijk is. Vooraf wordt toestemming gevraagd voor een referentiecheck en indien toegepast wordt bij de sollicitant getoetst of de gevonden informatie klopt.

Alle informatie die tot een persoon te herleiden is valt onder de AVG en mag niet langer bewaard worden dan noodzakelijk. Dit geldt ook voor aantekeningen over een sollicitatiegesprek en gegevens die een kandidaat zelf online heeft ingevuld. Cv’s van kandidaten die afgewezen zijn, worden maximaal vier weken bewaard. Kandidaten hebben het recht om te vragen volledig uit de systemen van Bibliotheek Hoorn verwijderd te worden. Tevens hebben zij het recht om te weten wat er precies over hen is opgeslagen.

Specifiek

Digitaal/ICT
Bibliotheekbezoekers dienen er op te kunnen vertrouwen dat er zorgvuldig met hun digitale gegevens wordt omgegaan en dat hun privacy gewaarborgd is. Om te voorkomen dat kwaadwillenden inzicht kunnen krijgen in persoonsgegevens en in leen- en zoekhistorie, is het belangrijk dat bibliotheken gebruik maken van een beveiligde omgeving.

Gegevens van bibliotheekbezoekers worden in principe niet aan derden doorgegeven. Er zijn echter enkele situaties waarin een dergelijke doorgifte wel kan plaatsvinden, namelijk de volgende:

- bij interbibliothecair leenverkeer;
- bij aanmelding op www.bibliotheek.nl;
- bij door ons ingeschakelde hulppersonen;
- op grond van wettelijke verplichtingen.

Interbibliothecair leenverkeer
Klanten kunnen via het interbibliothecair leenverkeer in veel gevallen (kopieën van) werken opvragen uit de catalogus van andere bibliotheken. Bij een dergelijke aanvraag zijn wij genoodzaakt enkele persoonsgegevens door te geven aan de betreffende bibliotheek (onder meer naam, pasnummer, etc.). Wij wijzen erop dat de verantwoordelijkheid voor de zorgvuldige omgang met deze doorgegeven persoonsgegevens ligt bij de betreffende externe bibliotheek.

Website
Via de website www.bibliotheek.nl kunnen klanten gebruikmaken van verschillende aanvullende diensten (zie de website voor het actuele aanbod). Deze website wordt geëxploiteerd door de Koninklijke Bibliotheek. Om van deze diensten gebruik te kunnen maken, dient men op de website een account aan te maken. Op het moment dat een account op www.bibliotheek.nl is aangemaakt, geeft de klant toestemming voor het verstrekken van zijn of haar lidmaatschapsgegevens van onze bibliotheek aan de Koninklijke Bibliotheek. De Koninklijke Bibliotheek koppelt deze gegevens vervolgens aan dit nieuwe account. Zij verwerken deze gegevens overeenkomstig hun eigen privacy policy.

Door ons ingeschakelde hulppersonen
Het kan zijn dat Bibliotheek Hoorn een externe partij inschakelt om bepaalde verwerkingen voor haar uit te voeren (bijv. een bepaalde statistische analyse of het verzorgen van een mailing). In die situaties zullen we steeds met die derde afspraken maken over het gebruik, de beveiliging en de geheimhouding van gegevens (verwerkersovereenkomst). Het komt erop neer dat deze derde partijen de gegevens van onze klanten nooit voor hun eigen doeleinden mogen gebruiken.

Afgifte op grond van wettelijke verplichtingen
Onder bepaalde omstandigheden is Bibliotheek Hoorn wettelijk verplicht klantgegevens af te geven aan overheidsinstanties (zoals politie/justitie, fiscus, etc.). Wij zullen dergelijke gegevens alleen afgeven wanneer wij daartoe wettelijk verplicht zijn. Het is ons niet altijd toegestaan de klant te informeren over een dergelijke afgifte (zie ook *Vordering door de politie/advocatuur*).

Cookies
Op de website van Bibliotheek Hoorn wordt gebruikgemaakt van cookies. Cookies zijn tekstbestandjes die op de computer van de klant worden geplaatst. In het cookiestatement staat nader uitgewerkt welke cookies er worden gebruikt, welke gegevens daarmee worden verwerkt en voor welke doeleinden dit geschiedt.

Statistische analyse door Google Analytics
Deze website maakt gebruik van Google Analytics, een webanalyse-service die wordt aangeboden door Google Inc. (“Google”), om ons online aanbod voortdurend te optimaliseren. Wij hebben Google Analytics zodanig ingesteld dat wordt voldaan aan de eisen die de Autoriteit Persoonsgegevens aan deze verwerking stelt. Mocht de klant niettemin toch niet willen dat zijn of haar websitebezoek via Google Analytics wordt gemeten, dan kan hij of zij de Opt-out Browser Add-on installeren die te vinden is op https://tools.google.com/dlpage/gaoptout.

Privacy Statement
Op de website van Bibliotheek Hoorn wordt ons privacy statement vermeld. Hierin staat onder andere het volgende: “Aan een zorgvuldige omgang met persoonsgegevens wordt door Bibliotheek Hoorn groot belang toegekend. Bibliotheek Hoorn is verantwoordelijk voor de bescherming van de persoonsgegevens van haar leners volgens de regels en voorwaarden zoals gesteld in de AVG.”

Bibliotheek Hoorn maakt gebruik van veiligheidsprocedures, onder meer om te voorkomen dat onbevoegden toegang krijgen tot deze gegevens. Leners hebben het recht de over hen opgenomen gegevens in te zien, te (laten) verbeteren, aan te vullen of te verwijderen.

Bibliotheek Hoorn behoudt zich het recht voor om wijzigingen aan te brengen in het privacy beleid. Het verdient daarom aanbeveling naast kennisneming van het privacy statement regelmatig het volledige privacy beleid met betrekking tot klantgegevens na te kijken op updates. Als er updates hebben plaatsgevonden zullen deze op de website zichtbaar zijn in het privacy beleid en de datum van het beleid wordt aangepast.

Beveiligde verbinding
Bezoekers van de Hoornse website kunnen gebruik maken van een beveiligde verbinding waarbij gegevens gecodeerd worden verzonden. Een beveiligde gecodeerde verbinding (SSL) is herkenbaar aan https voor de URL en vaak is een slotje zichtbaar in de URL.

cWise (bibliotheeksysteem)
Klanten van Bibliotheek Hoorn kunnen gebruik maken van het bibliotheeksysteem cWise, beschikbaar gesteld via ProBiblio. Men heeft in de bibliotheek, thuis of elders toegang tot cWise via eigen pc, tablet of smartphone of via een van de publiekspc’s in de bibliotheek. Met c Wise (communityWise) kunnen gebruikers zoeken in de catalogus, zelf online recensies, beoordelingen en tags aan titels toevoegen, en kan men met andere gebruikers ervaringen delen en tips uitwisselen. Door in te loggen via ‘Mijn menu’ heeft men toegang tot de eigen persoonlijke gegevens en kan men verlengen, reserveren, openstaande registraties voldoen via iDeal, etc. Klanten bevinden zich na het inloggen in een beveiligde omgeving. De gegevens worden versleuteld verzonden. Dit is herkenbaar aan de *s* achter *http* en aan het over het algemeen zichtbare slotje in de URL-regel.

Bij het in ‘Mijn menu’ via iDeal voldoen van openstaande registraties zoals contributie, boete, e.d. beschikt men over een beveiligde betaalomgeving.

Logt een klant voor de eerste keer in bij cWise, dan wordt men er op gewezen dat als men acht jaar of ouder is, men verplicht is om het standaard wachtwoord bestaande uit de twee cijfers van de geboortedag en de laatste twee cijfers van het geboortejaar te veranderen in een zelf te kiezen wachtwoord. Dit wachtwoord moet uit zes of meer tekens bestaan. Er wordt op gewezen dat een wachtwoord geheim is. Er staat “Een wachtwoord is geheim. Kies een wachtwoord dat goed te onthouden is, maar niet makkelijk te raden is door iemand anders.” En: “Uit veiligheidsoverwegingen is na vijf foute inlogpogingen de toegang voor een dag geblokkeerd.” Als een lener het wachtwoord kwijt is dan kunnen wij dat resetten en krijgt de lener een eenmalige code om in te loggen, daarna kan gelijk weer een eigen wachtwoord worden ingevuld. Personeel van de bibliotheek kan niet nagaan wat het wachtwoord van een klant is.

cWise maakt in de portal gebruik van cookies, maar op een zeer spaarzame manier. Deze cookies worden gebruikt voor:

- Het bijhouden van sessie-gegevens, met een vervaltijd van maximaal een uur

- Het onthouden van het pasnummer of gebruikersnaam van de gebruiker, als de gebruiker dit zelf activeert

Conform de cookiewet van 2015 wordt de bezoeker vooraf gevraagd of akkoord wordt gegaan met het gebruik van cookies.

BicatWise
Bibliotheek Hoorn maakt gebruik van BicatWise ten behoeve van de ledenadministratie, collectiebeheer, catalogus, bestellingen, etc. Om toegang te krijgen tot het algemene BicatWise dient het personeel in te loggen. BicatWise kent een aantal specifieke bevoegdheden. Denk daarbij aan het verwerken van contributies, het plaatsen van bestellingen, e.d. Om hiervan gebruik te kunnen maken moet men een specifieke inlogcode intoetsen, inlogcodes die bij een beperkt aantal mensen die uit de aard van hun functie toegang behoeven bekend zijn.

Om te voorkomen dat bezoekers toegang hebben tot de gegevens in BicatWise en de Hoornse kantooromgeving is het zeer gewenst dat personeelsleden bij het verlaten van een servicedesk de personeelspc vergrendelen via Ctrl Alt Delete. Daarnaast dienen medewerkers zich er bewust van te zijn dat het in geval van een storing of probleem zeer klantvriendelijk kan lijken om een bezoeker gebruik te laten maken van een personeelspc, maar dat dit niet is toegestaan.

Publiekspc's
Hoorn heeft in elke vestiging publiekspc's staan, die zijn voorzien van een beveiligingsschil geleverd door Xafax. Bezoekers van vestigingen van Bibliotheek Hoorn kunnen hun documenten niet opslaan op de servers in de bibliotheek. Hoorn heeft daardoor niet de verantwoordelijkheid voor het beheer en het beveiligen van deze documenten.

Iedere bibliotheekbezoeker kan via de werkplekpc's een aantal sites gratis raadplegen. Wil men gebruik maken van internet of Office, dan moet er ingelogd worden met òf een bibliotheekpas òf een aangeschafte tegoedbon. Bij gebruik van browsers wordt standaard met de incognitomodus gewerkt. Hierdoor wordt de browsegeschiedenis van de bezoeker niet bewaard.

Bezoekers kunnen uit veiligheids- en beheeroverwegingen geen software installeren op de publiekspc's. Is men klaar met het pc-gebruik, dan moet men uitloggen. Vervolgens wordt de pc in het kader van privacybescherming automatisch afgesloten en herstart. Bij de herstart worden alle gegevens van de gebruiker verwijderd. De pc wordt "geschoond" en opgeleverd in oorspronkelijke staat.

Bij laptops gebruikt voor cursussen wordt deze d.m.v. software geschoond bij het afsluiten.

Wifi
In alle vestigingen kan gratis gebruik gemaakt worden van Wifi. Daartoe hangen in alle vestigingen zogenaamde accesspoints. Via deze accesspoints maakt men gebruik van een open onbeveiligd Wifi netwerk. Voor het gebruik van Wifi in onze vestigingen hanteren wij het Reglement Gebruik Internet, Wifi en computers, het reglement is te vinden op de website.

Reserveringen
In het kader van de privacy zijn de reserveringsbonnen die uit het bibliotheeksysteem Wise komen in mei 2018 aangepast. Daarbij speelt een aantal punten:

- vaak staan reserveringen in publiek toegankelijke kasten. Daardoor is het ongewenst om de naam en/of het pasnummer op de bon te printen. Daarom staan nu alleen de eerste drie letters van de achternaam en de eerste voorletter er op;
- alleen de laatste 5 cijfers van het pasnummer van de lener worden getoond;
- de eerste drie letters van de achternaam staan ook links bovenaan om het makkelijker te maken om te zoeken in de reserveringskast;
- tevens is alles links uitgelijnd, ook om het geheel beter zichtbaar te maken in kast.

Voor de bonnen van interbibliothecair leenverkeer is de KB verantwoordelijk. Omdat deze bonnen te veel gegevens bevatten, worden de materialen bij klantenservice bewaard, totdat de klant het ophaalt.

Rol van de Koninklijke Bibliotheek (KB)
Als lid van Bibliotheek Hoorn kan de klant gebruik maken van verschillende aanvullende landelijke diensten die vallen onder de verantwoordelijkheid van de Koninklijke Bibliotheek. Via de *website www.onlinebibliotheek.nl* kunnen bijvoorbeeld e-books geleend worden. Ook op de website *www.bibliotheek.nl* worden specifieke diensten door de Koninklijke Bibliotheek aangeboden. Om van deze diensten gebruik te kunnen maken, dient de klant op de website(s) voor de desbetreffende diensten een account aan te maken.

Wij wisselen op voorhand een beperkte set persoonsgegevens met de Koninklijke Bibliotheek uit om het mogelijk te maken dat de klant door de Koninklijke Bibliotheek als lid van de bibliotheek wordt herkend. Op het moment dat de klant een account voor deze dienst(en) aanmaakt geeft hij of zij hiermee toestemming voor het verstrekken van zijn of haar lidmaatschapsgegevens van Bibliotheek Hoorn aan de Koninklijke Bibliotheek. De Koninklijke Bibliotheek koppelt deze gegevens vervolgens aan dit nieuwe account. Zij verwerkt deze gegevens overeenkomstig haar eigen privacyverklaring: *https://www.onlinebibliotheek.nl/klantenservice/privacy-policy.html.*

Als de klant gebruik maakt van de diensten via *www.onlinebibliotheek.nl* en/of *www.bibliotheek.nl*, kan hij of zij voor de rechten als betrokkene rechtstreeks contact opnemen met de Koninklijke Bibliotheek. De klant kan van modelbrieven gebruik maken en die zijn beschikbaar op: *https://www.kb.nl/avginzage*.

Klantcontact met privacygevoelige, juridische en/of financiële informatie
Bibliotheken spelen een actieve rol in het sociale domein en breiden hun dienstverlening steeds meer uit. Denk bijvoorbeeld aan het convenant dat in 2016 met de Belastingdienst is afgesloten. De medewerkers in de frontoffice worden daardoor steeds vaker geconfronteerd met hulpvragen waarbij privacy-aspecten en gevoelige financiële informatie een rol spelen.

Het is belangrijk dat de bibliotheek hier goed op voorbereid is en hierover afspraken maakt met het frontoffice-personeel. Zo hoeven medewerkers niet zelf te bepalen hoe ver ze gaan in het helpen van de klant en vermijdt de bibliotheek onnodige risico's.

Om de medewerker goed toe te rusten, moet de Bibliotheek een aantal randvoorwaarden realiseren. In het uitgebreide protocol Privacy in de Frontoffice zijn afspraken, uitgangspunten, gedragsregels en voorbeeldsituaties opgenomen. De bibliotheekrealiteit zal door maatschappelijke en technische ontwikkelingen blijven veranderen. Het protocol is daarom geen statisch document. Het wordt waar nodig aangepast en is afhankelijk van verschuivingen van de situatie in de bibliotheek.

Filmen/fotograferen van klanten/bezoekers
Volgens de Nederlandse wetgeving is in principe voor het filmen en uitzenden van beeldmateriaal met betrekking tot personen toestemming nodig van degenen in kwestie.

Natuurlijk is dit vrijwel ondoenlijk waar het grote groepen mensen in openbare ruimten betreft en bijvoorbeeld in de journalistiek gebeurt dit in de praktijk ook niet. Bibliotheek Hoorn heeft de wetgeving naast de dagelijkse praktijk van bibliotheken met veel ervaring op het gebied van het filmen/fotograferen van evenementen gelegd en hanteert de volgende richtlijnen:

- bij het filmen/fotograferen van grote groepen mensen in de publieke ruimte, zoals bij evenementen als Nederland Leest, de Boekenweek etc. kunnen we niet goed apart toestemming vragen om te filmen en het beeldmateriaal te publiceren. Dat hoeft in feite ook niet zolang het een algemeen overzicht blijft;
- zodra er mensen in het bijzonder worden uitgelicht, zullen we er naar streven aan hen wel toestemming te vragen en het doel van het uitlichten aangeven;
- bij interviews vraagt de bibliotheek zeker toestemming van de betrokkene(n) om beeldmateriaal te gebruiken en geeft aan waar het voor gebruikt zal worden;
- het beeldmateriaal kan op onze website en andere media als bijvoorbeeld YouTube gepubliceerd worden. Als mensen achteraf bezwaar aantekenen tegen hun aanwezigheid op dit beeldmateriaal zullen we die fragmenten er uitsnijden of, als dit niet goed mogelijk is, het filmpje verwijderen;
- bij het filmen/fotograferen van meer besloten groepen, zoals bij workshops, schrijversontmoetingen en groepsbezoeken, zullen we (bij voorkeur ruim van te voren, maar in ieder geval voor we beginnen) het aankondigen als we van plan zijn te filmen/fotograferen;
- bij een aankondiging vlak van tevoren zijn er bij bezwaren van deelnemers twee mogelijkheden: we besluiten niet te filmen, omdat we wensen dat iedereen deelneemt of we geven degene(n) die niet gefilmd willen worden de optie om niet deel te nemen. Waar voor gekozen wordt, hangt helemaal af van de aard van het evenement, de reactie van de deelnemers en het belang van de verfilming. Aankondiging ruim van tevoren (bijvoorbeeld bij de uitnodiging) voorkomt deze keuze;
- bij het filmen/fotograferen van individuele mensen vragen we altijd toestemming en geven we aan waar het beeldmateriaal voor gebruikt zal worden;
- bij het filmen/fotograferen van individuele kinderen vragen we toestemming aan de kinderen zelf en aan hun ouders. Als de ouders niet bij het filmen aanwezig zijn vragen we het telefoonnummer en bellen we om toestemming voor het gebruik van het beeldmateriaal te vragen;
- bij het filmen/fotograferen van grote groepen kinderen in de publieke ruimte geldt hetzelfde als voor volwassenen;
- bij het filmen/fotograferen van meer besloten groepen kinderen is de toestemming bij evenementen in samenwerking met scholen meestal al via de school geregeld. Als dit niet zo blijkt te zijn, of het evenement is niet in samenwerking met een school opgezet, kondigen we de mogelijkheid van verfilming met informatie waar we die film voor willen gebruiken ruim vooraf aan in de berichtgeving naar de ouders toe.

Fotograferen/filmen door bezoekers
Dit betreft filmen/fotograferen in met name de publieksruimten. In het kader van privacybescherming en veiligheid is het bezoekers niet toegestaan in de ruimten van de bibliotheek te filmen en/of te fotograferen zonder toestemming. Toestemming wordt alleen in bijzondere gevallen verleend, met name als een gerechtvaardigd belang van de bibliotheek in het geding is en dan uitsluitend onder door de bibliotheek naar de AVG-wetgeving bepaalde voorwaarden. De privacy coördinator adviseert de directeur hierin. De directeur is degene die beslist.

Datalekken

De Autoriteit Persoonsgegevens (voorheen College bescherming persoonsgegevens) heeft

beleidsregels gepubliceerd over de meldplicht datalekken. De beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek en of er gemeld moet worden aan de Autoriteit en/of aan betrokken. Bibliotheek Hoorn conformeert zich aan deze beleidsregels.

Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we van een datalek. Het risico op datalekken wordt steeds groter omdat persoonsgegevens in steeds meer databanken en/of op dragers zijn opgeslagen. Er zijn verschillende categorieën datalekken denkbaar; bepalend voor de reikwijdte van wetswijziging is dat er sprake moet zijn van een inbreuk op een beveiligingsmaatregel en dat er ernstige nadelige gevolgen zijn voor de privacy van betrokkenen.

Er is een algemene meldplicht datalekken voor alle organisaties in de publieke en private sector ingevoerd. De meldplicht geldt voor de ‘verantwoordelijke’ zoals deze in de Wbp is gedefinieerd. ‘Betrokkenen’ zijn de personen van wie de persoonsgegevens zijn gelekt. Omdat er sprake is van een hoge sanctie bij niet naleving van de meldplicht heeft dit een directe relatie met de governance van de bibliotheek.

Zodra een datalek bekend is, zal Bibliotheek Hoorn beoordelen of het datalek gemeld moet worden bij de AP. Wij zullen hierbij een inschatting maken van de ernst van de nadelige gevolgen voor de bescherming van de persoonsgegevens. Wij zullen het datalek ook melden aan de betrokkenen als de inbreuk op de verwerkte persoonsgegevens ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer. Wij zullen bij een melding aan de AP aangeven of wij van plan zijn om ook de betrokkenen van de inbreuk in kennis te stellen (de AP kan deze melding aan betrokkenen eventueel afdwingen).

Ook zullen wij alle eventueel voorkomende lekken documenteren. Dit overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk en de tekst van kennisgeving aan de betrokkene(n).

Verder zal Bibliotheek Hoorn in de verwerkersovereenkomsten met (IT-)leveranciers een vergelijkbare meldplicht opnemen, die erop neerkomt dat deze leveranciers ons informeren indien sprake is van een datalek.

Bij de beoordeling of een datalek gemeld moet worden melden, gelden de volgende drie vragen die voor melding bevestigend beantwoord dienen te zijn:

1. Is er sprake van een inbreuk op de beveiligingsmaatregelen (een datalek)?
2. Zijn de verwerkte persoonsgegevens daardoor blootgesteld aan verlies of onrechtmatige verwerking?
3. Heeft deze blootstelling geleid (of is er een aanzienlijke kans) tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens of ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkenen?

Bij de beantwoording van de eerste vraag moet niet alleen gedacht worden aan actieve handelingen om de beveiliging te doorbreken zoals hacken van bestanden, maar moet ook aan diefstal of verlies van dragers waarop persoonsgegevens zijn opgeslagen worden meegenomen. Wanneer gegevens zodanig zijn beveiligd dat het redelijkerwijs is uitgesloten dat een datalek kan leiden tot kennisname van persoonsgegevens door onbevoegden, kan kennisgeving aan de AP en betrokkene achterwege blijven. Blootstelling aan ernstige nadelige gevolgen in de vorm van onrechtmatige verwerking moet objectief en naar feitelijke omstandigheden van het geval worden vastgesteld. Bij de beantwoording van de laatste vraag zijn vooral aard en omvang van de inbreuk van belang, de aard van de gelekte persoonsgegevens en de mate waarin technische beschermingsmaatregelen zijn getroffen

ten aanzien van de desbetreffende persoonsgegevens. Het gaat hierbij om een inschatting van de ernst van de gevolgen. De beleidsregels van de AP bevatten uitgebreide handvatten om deze inschatting te kunnen maken.

De Europese Privacy Verordening kent ook een meldplicht voor datalekken; de invoering meldplicht datalekken in Nederland loopt vooruit op de regelgeving die op dit moment in Brussel wordt voorbereid.

Procedure
Datalekken of vermoedens van datalekken moeten altijd doorgegeven worden aan de privacy coördinator. Medewerkers worden hier bij de inwerkprocedure van op de hoogte gebracht. Bewerkers worden hiervan op de hoogte gebracht, alsmede van het feit dat zij sub bewerkers op de hoogte dienen te stellen.

De privacy coördinator onderzoekt de achtergronden van de melding en bespreekt de bevindingen met de directeur. Samen beoordelen zij (met betrekking van de interne systeemeigenaar – de 'business owner' van het systeem die goed in beeld heeft wat er in het systeem gebeurt en welke gegevensstromen in/uit gaan) of het datalek gemeld moet worden en aan wie, waarbij de directeur de doorslaggevende stem heeft. Als het datalek digitale beveiliging betreft, wordt ook de medewerker ICT bij de beoordeling betrokken.

De privacy coördinator zorgt voor melding aan de AP, als daar toe besloten wordt. Directeur, privacy coördinator en de medewerker pr en communicatie bespreken hoe de melding aan betrokkenen dient te geschieden, als daartoe besloten wordt. De afdeling communicatie zorgt voor de uitvoering. Directeur en privacy coördinator maken tevens de afweging of een jurist moet worden ingeschakeld. De directeur heeft daarin de doorslaggevende stem.

Ten slotte wordt bij constatering van een datalek in het managementoverleg door het managementteam besproken wat voor maatregelen er nodig zijn om een dergelijk lek voortaan te voorkomen, met advisering van de privacy coördinator (eventueel in overleg met de beleidsmedewerker ICT). De privacy coördinator zorgt ook dat de documentatie rond het voorval opgeslagen en bewaard wordt.