Pro biblio

In 10 stappen naar... een privacy-proof Taalhuis

Het Taalhuis van de bibliotheek verwerkt gegevens van deelnemers en vrijwilligers en moet dus voldoen aan de privacywetgeving (AVG). Volg dit stappenplan en je bent een heel eind op weg naar het beter beschermen van de privacy van taalleerders en taalvrijwilligers.

Klik op de blokken voor een uitgebreide uitleg.

1 Werk samen met jouw privacy-coördinator

Je staat er niet alleen voor. Ga in jouw bibliotheek op zoek naar de privacycoördinator en onderneem samen de volgende stappen.

2 Inventariseer de verwerking van persoonsgegevens

Onderzoek welke gegevens van taalleerders en taalvrijwilligers worden gevraagd en bijgehouden, en met welk doel dat gebeurt. Leg deze informatie vast in een zogeheten verwerkingsregister.

3 Beoordeel de registratieprocedures & inschrijf-formulieren

Check of de inschrijfprocedure voor taalleerders en taalvrijwilligers voldoet aan de eisen: de inschrijving is wettelijk, dient een doel en is noodzakelijk. Leg ook deze informatie vast in het verwerkingsregister.

4 Zorg voor voldoende beveiliging van gegevens

Weet welke documenten wel of niet beveiligd moeten zijn, beperk de toegang met bijvoorbeeld een wachtwoord en zorg dat iedereen in de organisatie zich aan de regels houdt.

5 Maak afspraken met samenwerkings-partijen

Maak je gebruik van een ruimte van de gemeente of verwijs je door naar het UWV? Breng samenwerkingspartners en leveranciers in kaart en maak met deze partijen goede afspraken over de uitwisseling van persoonsgegevens.

6 Weet wat je moet doen als je door-verwijst

Stuur je gegevens van taalleerders wel eens door aan een andere partij? Geef dit aan in het inschrijfformulier, vraag om toestemming van de taalleerder of geef de gegevens aan hem of haar mee.

7 Weet wat je moet doen bij een datalek

Een USB-stick verloren of een e-mail aan verkeerde geadresseerden gestuurd? Neem direct contact op met de privacycoördinator in jouw bibliotheek. Zorg ook voor een veilige meldcultuur onder collega's.

8 Zorg dat mensen hun privacyrechten kunnen uitoefenen

Houd er rekening mee dat een taalleerder of taalvrijwilliger persoonsgegevens wil inzien of verwijderen. Zorg dat medewerkers deze vraag herkennen en op een goede manier beantwoorden.

9 Zorg voor kennis en bewustzijn bij medewerkers

Alle collega's in het Taalhuis moeten helpen de privacy van de taalleerders en taalvrijwilligers te beschermen. Informeer hen over de stappen uit deze checklist die ook voor hen belangrijk zijn.

10 Zorg dat je klaar bent voor certificering

Wil je in aanmerking komen voor certificering van het Taalhuis? Je bent dan ook afhankelijk van wat in je bibliotheekorganisatie is geregeld. Bereid certificering voor samen met de privacycoördinator.

Taalhuis

Stappenplan voor een privacy-proof Taalhuis

Je hebt het vast gelezen, er is het nodige veranderd in de regels rond ***privacy***. Sinds mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG is van toepassing op alle ***organisaties*** en personen die in de Europese Unie persoonsgegevens verwerken. Dus ook de bibliotheek en de organisaties die actief zijn binnen de bibliotheek, zoals het Taalhuis, moeten voldoen aan de nieuwe privacywetgeving.

Waarom is privacy belangrijk?
'Sinds de nieuwe privacywet mag je helemaal niets meer.' 'Als je niets te verbergen hebt, heb je toch ook niets te vrezen?' Veelgehoorde geluiden die het belang van privacy in twijfel trekken. Heb je hiermee te maken in het Taalhuis? Weet dan wat de ***belangrijkste argumenten*** voor privacybescherming zijn. Zoals dat privacy een grondrecht is en dat er grote risico's kleven aan het onverantwoord delen van persoonlijke gegevens.

Bekijk de definitie van privacy op Wikipedia

Er is veel aandacht rond misstanden in organisaties, zoals het Facebook schandaal en het medische dossier van Barbie

De belangrijkste argumenten op een rijtje

Werk samen met jouw privacycoördinator

Je staat er met deze uitdaging gelukkig niet alleen voor. In de meeste bibliotheken is een ***privacycoördinator*** opgeleid om de dienstverlening van de bibliotheek conform de AVG-regels te organiseren. De privacycoördinator is op de hoogte van alle richtlijnen.

- Ga in jouw organisatie op zoek naar de privacy coördinator. Bespreek met hem of haar deze checklist en onderneem samen de volgende stappen.

De privacy coördinator kan hulp inroepen van de Probiblio Privacy Servicedesk. Er is ook een gespecialiseerde jurist achter de hand

2

Inventariseer de verwerking van persoonsgegevens

- Om aan de AVG te voldoen, onderzoek je allereerst welke persoonsgegevens er op dit moment van de taalleerders en taalvrijwilligers gevraagd en bijgehouden worden. En met welk doel dat gebeurt. Leg deze informatie vast in het centrale verwerkingsregister dat de privacycoördinator in beheer heeft. Vul het document tijdens de volgende stappen van de checklist verder aan.

Welke gegevens worden verwerkt?
Persoonsgegevens is alle informatie aan de hand waarvan een persoon kan worden geïdentificeerd. De 'gewone' persoonsgegevens zoals naam, adres, e-mail, telefoonnummer en inlognaam mogen in ***veel gevallen*** door bibliotheken worden verwerkt, ***'bijzondere' persoonsgegevens*** meestal niet.

- Vermeld in het verwerkingsregister elk afzonderlijk gegeven dat je van deelnemers en vrijwilligers vastlegt via de registratieprocedures (bijvoorbeeld in een intake of het inschrijfformulier).

Wat gebeurt er met de persoonsgegevens?
Onder ***verwerken*** wordt verstaan alle handelingen die je kunt uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen.

- Leg in het verwerkingsregister ook vast welke systemen je gebruikt om de gegevens te verwerken, wie er toegang hebben, hoe het systeem is beveiligd en met welke andere partijen, zoals gemeente, IT-leverancier, UWV, of vrijwilligersorganisaties, je deze informatie deelt.

In welke gevallen je gegevens mag verwerken, lees je bij stap 3.

'Bijzondere' gegevens is gevoeligere informatie als medische conditie, ras en geloof.
Lees de hele definitie

Verwerken is ook: registreren, aanpassen, kopiëren, delen, verwijderen, kwijtraken, verrijken, (laten) inzien

Beoordeel de registratieprocedures & inschrijfformulieren

Nu je hebt uitgezocht welke persoonsgegevens het Taalhuis verwerkt, ga je het inschrijfformulier en de registratieprocedure van Taalhuisdeelnemers en -vrijwilligers ***onder de loep*** nemen.

Om een persoonsgegeven (bijvoorbeeld een e-mailadres) te mogen verwerken, moet aan drie eisen zijn voldaan. ***Beoordeel*** voor elk persoonsgegeven uit Stap 2 dat in de registratieprocedures en inschrijfformulieren van het Taalhuis wordt gevraagd of aan de onderstaande eisen is voldaan. Leg de informatie vast in het verwerkingsregister.

1. **Onder de AVG mag je niet zomaar (gewone) persoonsgegevens verwerken. Je hebt daarvoor een wettelijke grondslag nodig. Bepaal op welke *grondslag uit de AVG* je de verwerking van persoonsgegevens in jullie Taalhuis kan baseren en leg dit vast in het verwerkingsregister.**

Vermoedelijk kom je bij verwerkingen in het Taalhuis al snel uit bij een van deze grondslagen:
- **Uitvoeren van een overeenkomst** (grondslag 2) Het ondertekende inschrijvingsformulier vormt de overeenkomst.
- **Toestemming** (grondslag 1) Deze vorm is geschikter voor zaken als het toesturen van een nieuwsbrief of gebruik van een foto op social media. Bij personen jonger dan 16 moet een ouder of wettelijke vertegenwoordiger de toestemming verlenen.

Hulp nodig? *Raadpleeg je privacy coördinator en de aan hem/haar verstrekte Probiblio VIA-toolkit, document 4 ('Rechtmatigheid en risicoanalyse')*

Als organisatie ben je zelf verantwoordelijk voor de beoordeling

Wat zijn de zes grondslagen?

2. Elk persoonsgegeven dat je verwerkt moet bijdragen aan het doel dat je wilt bereiken. Stel voor elk afzonderlijk persoonsgegeven *het doel* vast en leg dat vast in het verwerkingsregister.

Verwerk je een gegeven dat niet bijdraagt aan het doel van de overeenkomst? Of kun je je niet beroepen op een grondslag? Verwerk het gegeven dan niet meer.

Heb je persoonsgegevens eenmaal ontvangen of verwerkt voor een bepaald doel? Dan mag je deze niet zomaar voor een nieuw doel gebruiken. Je moet dan opnieuw om toestemming vragen of een nieuwe overeenkomst aangaan (zie vereiste 1.).

Voorbeelden van een doel:
Naam: Om aan te spreken, te kunnen herkennen, andere registratie mogelijk te maken. Moedertaal: Om te kunnen beoordelen welke vrijwilliger goed past bij de deelnemer

3. Tot slot moet een verwerking 'noodzakelijk en transparant' zijn. Bepaal dit voor elk persoonsgegeven dat je registreert en verwerkt, en leg ook dit vast in het verwerkingsregister.

Zorg dat je alleen gegevens verwerkt als dat echt noodzakelijk is voor het gestelde doel, bijvoorbeeld het leren van Nederlands. Dus niet als ze 'ooit van pas kunnen komen'. Let er extra op dat niet onnodig ***gevoelige informatie*** wordt vastgelegd.

Voorbeeld van gevoelige informatie:
Als de medische conditie van een deelnemer mogelijk van invloed is op het leren in het Taalhuis, kun je die informatie ook vastleggen zonder de precieze aandoening te noemen

Met 'transparant' wordt bedoeld dat voor de betrokkene duidelijk is welke persoonsgegevens worden verwerkt en met welk doel dat gebeurt. Informeren over het gebruik van persoonsgegevens kan via het inschrijvingsformulier of met een privacyverklaring op de website van de bibliotheek. Vermeld in beide gevallen welke persoonsgegevens de organisatie verwerkt, met welk doel, hoe lang deze bewaard blijven en hoe je contact kunt opnemen met een klacht.

Zorg voor voldoende beveiliging van gegevens

In de privacywetgeving staat dat een organisatie ‘passende technische en organisatorische maatregelen’ moet treffen om persoonsgegevens te beveiligen. Je moet zelf bepalen wanneer de gegevens voldoende beveiligd zijn. Wat betekent dit in de praktijk?

- **Tref ‘passende’ maatregelen**
  Houd rekening met de hoeveelheid gegevens en de gevoeligheid ervan. Een lijst van 10 personen met alleen voornaam en woonplaats hoeft minder goed beveiligd te zijn dan 1.000 medische dossiers met volledige naam, adres en woonplaats van de betrokkenen. De privacycoördinator kan je helpen te bepalen wat passend is voor de gegevens van het Taalhuis.

- **Tref ‘technische’ maatregelen**
  Om digitale persoonsgegevens ***technisch voldoende beveiligd*** uit te wisselen, maak je ten minste gebruik van een beveiligd bestand of omgeving. De inloggegevens (inlognaam en wachtwoord) deel je via een ander medium.

  Uiteraard is het steeds van belang goed na te denken wie toegang tot een bestand of systeem nodig heeft. Trek de toegang in zodra dit niet meer nodig is en scherm gegevens die iemand niet nodig heeft af.

- **Tref ‘organisatorische’ maatregelen**
  Zorg voor de juiste en voldoende beveiligingsmaatregelen binnen de organisatie. Informeer collega’s goed over wat wel en niet mag gebeuren rond de verwerking van persoonsgegevens. Spreek er bijvoorbeeld met elkaar over tijdens het werkoverleg. En leg afspraken rond geheimhouding vast in een ***geheimhoudingsverklaring*** die een organisatie met haar medewerkers en vrijwilligers afsluit.

- **Let ook op een goede beveiliging van persoonsgegevens in de fysieke ruimte.**
  Het is bijvoorbeeld af te raden om deze gegevens op te slaan op de lokale schijf van een computer die zich in een niet-beveiligde ruimte bevindt, ook al is de computer met een wachtwoord beveiligd. Bij diefstal kan de data toch uitgelezen worden.

Voorbeeld van goede beveiliging:
deel het beveiligde Excel-bestand via e-mail en het wachtwoord via sms

Een model geheimhoudings-verklaring is beschikbaar bij je privacy coördinator

5

Maak afspraken met samenwerkings-partijen

Taalhuizen maken deel uit van een taalnetwerk. Er werken bijvoorbeeld vrijwilligers van de vrijwilligersorganisatie, je maakt gebruik van een ruimte van de gemeente, je werkt samen in een softwarepakket of website van een IT-leverancier, je verwijst door naar een onderwijspartner, het UWV, een bank, etc. Op het moment dat deze partijen persoonsgegevens verwerken rond het Taalhuis zijn zij ***verwerker of verwerkingsverantwoordelijke***. Maak met alle partijen goede afspraken over de uitwisseling van gegevens.

- Zorg voor duidelijkheid over welke partij(en) **verwerkingsverant-woordelijke** is (zijn) en leg het besluit vast in het verwerkingsregister. De organisatie die verantwoordelijk is voor de uitvoering van het Taalhuis is de 'verwerkingsverantwoordelijke'. In de meeste gevallen is dat de bibliotheek.

- Verwerkt de partij waarmee je samenwerkt persoonsgegevens in opdracht van het Taalhuis, en is de kern van die opdracht ook het verwerken van persoonsgegevens? Dan is die partij **verwerker**. Stel met verwerkers een verwerkersovereenkomst op. Met een verwerkersovereenkomst maak je afspraken over de beveiliging van de verwerking, over onderlinge verantwoordelijkheid, aansprakelijkheid en welke gegevens worden verwerkt met welk doel. De privacycoördinator beschikt in de VIA Toolkit over een model verwerkersovereenkomst.

Let op: ***het Burgerservicenummer*** (BSN) is een 'bijzonder' gegeven en mag nooit door de bibliotheek worden verwerkt. Er zijn voorbeelden van gemeenten die het BSN of andere persoonsgegevens van deelnemers bij het Taalhuis opvragen. Dit kan grote privacyrisico's geven voor de betrokkenen. Mocht je met een gemeente te maken hebben die bijzondere persoonsgegevens opeist, zoek dan contact met je privacycoördinator of overleg met je directie.

Voorbeelden: IT-leveranciers zijn meestal verwerkers. Een onderwijsinstelling waar je naar doorverwijst of een gemeente die gegevens opvraagt voor subsidiedoeleinden zijn waarschijnlijk verwerkingsver-antwoordelijken. ***Let op:*** *dit kan voor ieder Taalhuis verschillen!*

Tip:
Vraag je privacy coördinator om hulp bij het vaststellen van de relatie van de samen-werkingspartij of raadpleeg in de Handleiding AVG van Rijksoverheid schema 3 op pagina 12

Lees meer over het verbod op het gebruik van BSN

Weet wat je moet doen als je doorverwijst

Wanneer nodig worden deelnemers van het Taalhuis doorverwezen naar partners in het netwerk. Soms wordt iemand direct doorverwezen, maar soms pas na een intake.

- Als je de tijdens de intake verzamelde gegevens wilt doorsturen naar een andere partij moet je ook voldoen aan de privacyregels. Dit kan op vier manieren:

1. Leg vast in het inschrijfformulier
Als je werkt met een inschrijfformulier kun je daarin vastleggen dat je bepaalde gegevens deelt met een of meerdere partners. Geef duidelijk aan in welke gevallen je welke gegevens doorstuurt, of je dat digitaal of op papier doet, aan welke partij(en) en met welk doel. Bespreek het opstellen van deze overeenkomst met je privacycoördinator.

2. Vraag toestemming voor digitaal delen
Wil je via een e-mail of webtool de (intake)gegevens delen met andere partijen? Vraag de betrokken persoon om ***toestemming*** en leg dit vast op papier (met handtekening) of als aantekening in het digitale dossier.

3. Vraag toestemming voor delen van enkel contactgegevens
Als er geen digitale aanmelding plaatsvindt of de deelnemer ***geeft geen toestemming*** voor het delen van zijn hele dossier, kan je ook toestemming vragen om alleen de belangrijkste contactgegevens door te geven aan de andere partij. Zo blijft risico op verlies of onterechte inzage van persoonsgegevens beperkt.

4. Geef de gegevens mee aan de betrokkene
De meest privacyvriendelijke oplossing is de gegevens die je wilt delen met een andere organisatie aan de betrokkene mee te geven. Hij of zij kan zo zelf kiezen welke gegevens worden gedeeld tijdens het bezoek aan de partnerorganisatie.

Leg vast bij toestemming: (1) dat hij of zij toestemming verleent en (2) weet aan welke partij gegevens worden doorgestuurd en wat het doel van het doorsturen is, (3) de wijze van geven van toestemming, bijvoorbeeld mondeling, (3) tijd en datum van de toezegging, (4) naam van de Taalhuismedewerker aan wie de toestemming is gegeven

Tip: *Noteer het ook als iemand geen toestemming verleent om gegevens door te sturen*

7

Weet wat je moet doen bij een datalek

Het kan de beste overkomen: een USB stick verloren, laptop of telefoon gestolen, een e-mail aan een verkeerde geadresseerden gestuurd of een computer in een openbare ruimte blijkt niet (voldoende) beveiligd te zijn. Voorbeelden van beveiligingsincidenten of mogelijk een datalek.

- Volg de procedure in je organisatie voor het melden van een (mogelijk) datalek. Bij twijfel: **direct melden** bij de privacycoördinator.
- Laat je informeren door de privacycoördinator in jouw bibliotheek. Hij of zij is verantwoordelijk voor de afhandeling van datalekken, heeft een procedure opgesteld en kan beoordelen wat moet gebeuren. Zoals hoe het incident opgelost wordt of de schade voor betrokkenen beperkt blijft, en eventuele communicatie naar betrokkenen en de Autoriteit Persoonsgegevens.
- Zorg dat je regelmatig, bijvoorbeeld tijdens een teamoverleg, collega's herinnert en aanspoort incidenten op te merken en te melden. Een veilige meldcultuur is belangrijk; waardeer het als iemand een melding maakt, zeker als de melder zelf een rol heeft in het veroorzaken van het datalek.

8

Zorg dat mensen hun privacyrechten kunnen uitoefenen

Mensen hebben verschillende rechten om controle te houden over hun persoonsgegevens. Deze worden ook wel de ***rechten van betrokkenen*** genoemd. Denk aan het recht van inzage en het recht gegevens te laten verwijderen. Het is van belang om, mits dat mogelijk is, gehoor te geven aan personen die daar een beroep op doen. Dit draagt bij aan het vertrouwen in je organisatie.

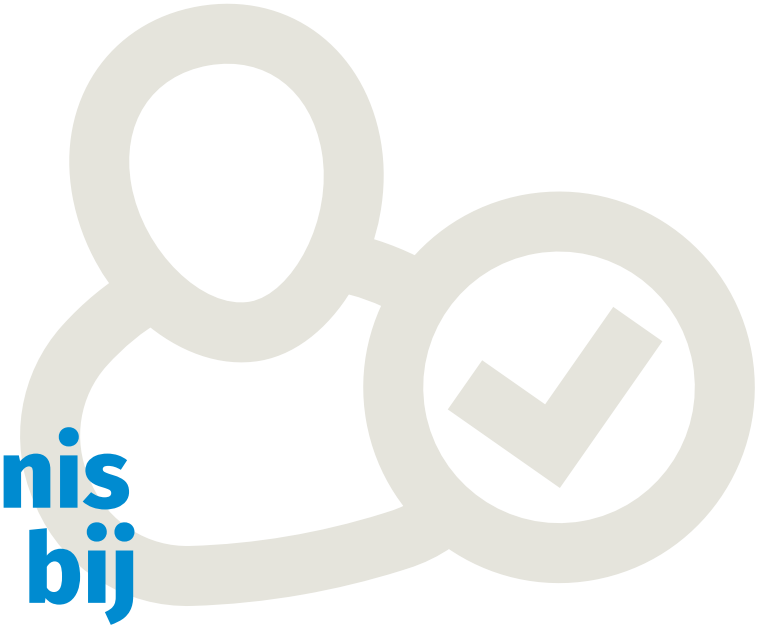
- Houd er dus rekening mee dat iemand deze vragen ook aan het Taalhuis kan stellen. Het is belangrijk dat niet alleen jij, maar alle medewerkers deze vragen als zodanig herkennen en ze vervolgens op een goede manier beantwoorden.
- Wanneer iemand zijn of haar privacyrechten bij het Taalhuis uitoefent, moet je ***vaststellen*** of die persoon is wie hij of zij zegt te zijn. Je wilt immers voorkomen dat je iemand toegang geeft tot de persoonsgegevens van een ander.

Bekijk het overzicht van de rechten van betrokkenen onder de AVG

Tip:
Neem bij een verzoek contact op met je privacycoördinator en volg zijn of haar instructies.

Je mag bijna nooit een kopie van het identiteitsbewijs bewaren. Lees hoe je iemands identiteit kan vaststellen

9



Zorg voor kennis en bewustzijn bij je collega's

Ook de collega's in het Taalhuis spelen een belangrijke rol in het privacy-proof houden van de processen en diensten van het Taalhuis.

▶ Houd je collega's daarom op de hoogte van de privacyregels door met hen de stappen uit de checklist te doorlopen die voor hen relevant zijn:

- Wat is privacy en waarom is het belangrijk?
- Op welke momenten heb je hiermee te maken in het Taalhuis? (stap 2)
- Welke werkafspraken hebben we voor inschrijving van een nieuwe deelnemer? (stap 3)
- Hoe zijn de gegevens beveiligd? (stap 4)
- Hoe verwijs je door naar partners? (stap 6)
- Wat moet je doen bij een datalek? (stap 7)
- Hoe herken je dat een privacyrecht wordt uitgeoefend door een deelnemer en wat moet je dan doen? (zie stap 8)
- Informeer hen ook over de aanstaande certificering van het Taalhuis. (stap 10)

Zorg dat je klaar bent voor certificering

Voldoen aan de privacywetgeving is één van de normen voor de ***certificering van Taalhuizen***. Als je deze checklist hebt doorlopen en uitgevoerd, heb je serieuze stappen gezet richting een groen vinkje naast deze norm.

Het Taalhuis is in veel gevallen onderdeel van de bibliotheek; voor certificering van deze norm ben je dus ook afhankelijk van wat elders in de bibliotheekorganisatie is geregeld.

De privacycoördinator van de bibliotheek is je contactpunt om hierover vragen te stellen. Bijvoorbeeld:

- Zijn alle medewerkers in de organisatie bewust gemaakt (getraind) van het belang van privacy en wat dat voor hen en hun werk betekent?
- Zijn alle medewerkers die klantcontact hebben geïnstrueerd of getraind, zodat zij rechten van betrokkenen (zie stap 8) herkennen? En is een procedure geïmplementeerd voor het adequaat afhandelen van deze verzoeken?
- Is er een procedure datalekken geïmplementeerd en zijn medewerkers goed op de hoogte van wat zij moeten doen bij een (vermoedelijk) datalek?
- Is er een actueel privacy statement op de website gepubliceerd?
- Is er een verwerkingsregister? Staan daarin de verwerkingen die in het Taalhuis plaatsvinden in vermeld?

Informatie over hoe de certificering van het Taalhuis verloopt, hoe je je erop kunt voorbereiden, en op welke punten auditoren aandacht vestigen, vind je op de website van de certificeringsorganisatie CBCT: www.certificeringsorganisatie.nl/taalhuizen. Veel succes!

Lees het artikel van Bibliotheekblad over de certificering van Taalhuizen

Stappenplan afgerond, hoe nu verder?

Gefeliciteerd, je hebt grote stappen gezet in de privacy van het Taalhuis!

Eigenlijk ben je nooit helemaal klaar met privacy, wetgeving blijft in beweging en ook je organisatie staat niet stil. Samen met je privacycoördinator houd je de vervolgstappen in de gaten.

Een goede leidraad is om jaarlijks opnieuw te beoordelen of de diensten van het Taalhuis nog volgens de geldende privacywetgeving wordt uitgevoerd en of er nieuwe diensten zijn ontwikkeld waar persoonsgegevens bij betrokken zijn.

Informatie

Ellie van der Meer & Thomas Bersee, adviseurs Basisvaardigheden
basisvaardigheden@probiblio.nl

Koen Baaij, adviseur Privacy
privacy@probiblio.nl

Probiblio, maart 2020