SMIT STUDIES MEDIA INNOVATION TECHNOLOGY

POLICY BRIEF #15

5 maart 2018

De GDPR…en wat dit voor Vlaanderen betekent

Rob Heyman, Ine Van Zeeland, Jo Pierson

25 mei is het zo ver: de GDPR (General Data Protection Regulation of Algemene Verordening Gegevensbescherming) treedt in werking in de hele Europese Unie. Deze nieuwe regulering heeft tot doel om Europeanen te beschermen in de verwerking van persoonsgegevens en tegelijk het vrije verkeer van persoonsgegevens te blijven garanderen. Een verordening betekent dat de regulering onmiddellijk van toepassing wordt en dat er meteen ook boetes kunnen worden gevorderd van overtreders. Op dit moment zijn er echter nog veel vragen en weinig duidelijkheid.

Imec-SMIT-VUB voert al sinds 2009 onderzoek naar privacy en digitale media, met het EMSOC-project (SBO, 2010-2014) als eerste mijlpaal. Dit interdisciplinair onderzoek heeft onder meer bijgedragen tot de rechtzaak van de Belgische Privacycommissie tegen Facebook. Op dit moment biedt SMIT op diverse manieren ondersteuning bij de implementatie van GDPR-vereisten voor KMO's, mediabedrijven[1] en (slimme) steden.[2] Binnen City of Things in Antwerpen zorgt SMIT mee voor de aspecten van privacy, ethiek, vertrouwen en veiligheid binnen de verschillende projecten, door onder meer een 'privacy by design'-aanpak te garanderen.[3] Het doel van deze policy brief is een antwoord te bieden op de volgende vragen: Wat weten we zeker? Wat is er veranderd? Wie krijgt er boetes? Wie moet wat doen? Hoe kan de GDPR succesvol geïmplementeerd worden en hoe kan SMIT als onderzoekscentrum daarbij helpen?

Van zodra een persoon of organisatie gegevens verzamelt, verwerkt, anonimiseert of zelfs verwijdert, die door de organisatie in kwestie of wie dan ook kunnen worden gebruikt om iemand uniek te identificeren en er een eigenschap aan te koppelen, is de nieuwe verordening

[1] Zie bv. het ICON-project Ecodalo: https://www.imec-int.com/en/what-we-offer/research-portfolio/ecodalo en SMIT betrokkenheid in de GDPR taskforce van Medianet en Technical Hub van de Belgian Association of Marketing.
[2] Zie bv. SMIT betrokkenheid in City of Things https://www.imec-int.com/en/cityofthings, en bijdragen aan de leerstoel https://www.smartcitychair.be/. Recent is ook het project SPECTRE (Smart city Privacy: Enhancing Collaborative Transparency in the Regulatory Ecosystem) gestart, dat in de komende vier jaar onderzoek zal doen naar de innovatieve rol en implementatie van DPIA in Smart Cities.
[3] 'Privacy by design' of privacy door ontwerp betekent het nemen van passende technische en organisatorische maatregelen in een zo vroeg mogelijk stadium van technologie-ontwikkeling en gegevensverwerking, ter bescherming van privacy.

van kracht. Het toepassingsgebied van de GDPR is met andere woorden zeer breed in onze informatiemaatschappij.

Wat weten we zeker? Wat is er veranderd?

Dit eerste onderdeel biedt een overzicht van veranderingen waarvan we zeker zijn dat ze nu al kunnen worden meegenomen.

Een meer uniform kader voor de hele EU
Eigenlijk is er helemaal niet veel veranderd. We moesten via de Europese Richtlijn 95/46/EC, die in nationale wetgeving werd omgezet, al aan de meeste verplichtingen voldoen. De nationale omzetting zorgde voor een **lappendeken aan verschillende nationale interpretaties**. Het was door de omzetting van deze richtlijn mogelijk dat inwoners van één land, afhankelijk van de overtreder, wel of niet werden geholpen. Herinnert u zich Netlog? Dé sociale netwerkdienst van België en een groot deel van Europa, voordat Facebook in andere talen dan Engels werd vertaald. Netlog was een Belgisch bedrijf en moest zich aan de Belgische wetgeving houden; Facebook niet, het vestigde zich in Ierland. Ierland wil een gunstig klimaat creëren voor tech-reuzen zoals Facebook en LinkedIn, zelfs als dat betekent dat dit **ten koste van privacy** gaat. Nu is er een verordening die voor ieder Europees land hetzelfde is, of toch bijna. Lidstaten kunnen zaken zoals de minimumleeftijd voor geïnformeerde toestemming zelf bepalen, waardoor nog niet alles helemaal uniform is voor heel Europa.

Het einde van de CBPL
Lang leve de nieuwe toezichthoudende autoriteit die in de plaats komt van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL) in België. Eind 2017 werd deze autoriteit de Gegevensbeschermingsautoriteit of GBA gedoopt en die zal de Privacycommissie vervangen vanaf eind mei. De taken van deze nieuwe entiteit bestaan uit:[4]

- Het verstrekken van informatie
- Het begeleiden van verwerkingsverantwoordelijken
- Het controleren van verwerkingsverantwoordelijken
- Het sanctioneren van overtredingen

Het is op dit moment nog onduidelijk hoe de GBA de GDPR precies zal toepassen waardoor het voor organisaties die persoonsgegevens (laten) verwerken – van gemeenten en ziekenhuizen tot webwinkels en banken - onmogelijk is om in hun rol als verantwoordelijken voor persoonsgegevensverwerking volledig te anticiperen op de GDPR.[5] Bijvoorbeeld, een organisatie wil weten of de specifieke vorm van geïnformeerde toestemming in lijn is met de vernieuwde verplichtingen in de GDPR of hoe lang je gegevens van klanten mag bijhouden die niets meer bij je hebben gekocht? De kans is klein dat de GBA meteen op kruistocht gaat tegen overtreders. Dit omdat ze naar Europa zal kijken voor de interpretatie van de GDPR en de toepassing ervan. De autoriteit zal dus een **afwachtende houding** aannemen en rekening houden met een overgangsperiode waarin er eerst aan verduidelijking zal moeten worden gewerkt.

De dreiging van een boete
De grootst gepercipieerde verandering is de **dreiging van boetes**. Op de niet-naleving van de GDPR "administratieve geldboetes tot 20 miljoen euro of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is". Het is

[4] Meer info:
http://www.dekamer.be/kvvcr/showpage.cfm?section=/flwb&language=nl&cfm=flwbn.cfm?lang=N&legislat=54&dossierID=2648

[5] Een verwerkingsverantwoordelijke kan eender welke persoon, bedrijf, organisatie of overheid zijn die het doel van en de middelen voor de verwerking van persoonsgegevens vastlegt.

voor verschillende verantwoordelijken voor verwerking dé motivatie om meer van de GDPR te weten te komen.

Hoe groot is de feitelijke dreiging voor boetes?
De uiteindelijke dreiging is koffiedik kijken, maar er zijn alvast twee pistes die de autoriteit kan volgen: of de toezichthoudende autoriteit **start zelf een onderzoek**, of de autoriteit **komt op voor de rechten van een betrokkene of diens vertegenwoordiger** om de rechten van de betrokkene m.b.t. de GDPR te vrijwaren. (Middenveld)organisaties die strijden voor privacyrechten kunnen nu rechtzaken inspannen waarin ze een groep betrokkenen vertegenwoordigen, zoals burgers, consumenten of journalisten. De GDPR maakt het dus mogelijk om degenen van wie persoonsgegevens worden verzameld beter of pro-actiever te beschermen.

De nieuwe toezichthoudende autoriteit mag dan anders zijn dan de huidige Privacycommissie, ze zal nog steeds in **numerieke minderheid** zijn ten opzichte van alle verwerkingsverantwoordelijken. Daarbij komt dat veel verwerkingen complex en technisch zijn waardoor het onderzoek naar een overtreding tijd en specifieke expertise kost. Een voorbeeld hiervan is de **rechtzaak van de Privacycommissie tegen Facebook** waarin de commissie beroep heeft gedaan op drie onderzoeksgroepen om hen van de nodige kennis te voorzien.[6] Uitgaande van hoe de Privacycommissie nu werkt, zal de GBA altijd eerst een vaststelling moeten doen (deze kost tijd) die dan gevolgd zal worden door een vraag om bepaalde praktijken aan te passen. Indien deze niet worden gevolgd, dan zal de autoriteit in staat zijn om te sanctioneren.

In het geval van schade door **inbreuken of datalekken** zal onderzocht worden of de gegevensverwerking in kwestie door de gegevensverwerker voorkomen kon worden. Dat wil zeggen dat, als je kan aantonen dat een lek veroorzaakt werd door iets waar je als gegevensverwerker wat aan kon doen, je een grote kans loopt om een boete te krijgen. Een voorbeeld daarvan is de situatie waarin het datalek is ontstaan doordat een ex-werknemer nog steeds toegang heeft tot bestanden met klantengegevens. Kan je aantonen dat je alles hebt gedaan om deze risico's te vermijden, dan is de kans op een boete veel kleiner. Dit brengt ons bij wat werkelijk nieuw is in de GDPR, accountability. Er zijn voorbeelden van servers of vergeten laptops met klantengegevens van grote organisaties. Deze dragers waren onbeveiligd of onvoldoende beveiligd. In zo'n geval kan je aantonen dat er sprake is van nalatigheid door het verliezen van deze informatie. Indien iemand met deze informatie fraude kan plegen, is er een duidelijk risico dat vermeden had kunnen worden.

Accountability (verantwoordingsplicht)
De verantwoordelijke voor verwerking is ook meteen verantwoordelijk voor het toepassen van de GDPR, waarbij men moet kunnen aantonen hoe men dit laatste tracht te garanderen. Voor de GDPR was er een **meldingsplicht**, wat betekent dat iedere verwerking van persoonsgegevens aan de Privacycommissie moest worden gemeld. Deze melding werd niet nagekeken. Vanaf mei moeten verwerkingen niet meer gemeld worden, maar iedere organisatie die persoonsgegevens verwerkt, moet wel kunnen aantonen dat zij een goede huisvader is ten opzichte van persoonsgegevens en de **risico's** die daarmee gepaard gaan.

Met andere woorden: iedere **verwerkingsverantwoordelijke moet zich bewust zijn** van de manier waarop persoonsgegevens verwerkt worden binnen de organisatie. Dit wordt in de

[6] Van Alsenoy, Brendan, Verdoodt, Valerie, Heyman, Rob, Ausloos, Jef, Wauters, Ellen, Acar, Günes, Valcke, Peggy, Pierson, Jo, Kindt, Els, Lievens, Eva, Janssens, Marie-Christine, Diaz, Claudia & Preneel, Bart (2015) *From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms* (25 August 2015 - v1.3) – Report for the Belgian Privacy Commission on Facebook's revised Data Use Policy, Brussels: ICRI/CIR- KULeuven, iMinds-SMIT-VUB and COSIC-KULeuven, 109. (Retrieved from https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf)

eerste plaats gedaan d.m.v. een dataregister, een overzicht van de verschillende verwerkingsdoeleinden en gegevens die nodig zijn voor een bepaald doel. Dit kan bijvoorbeeld een winkel zijn die aankoopgegevens verwerkt van klanten, met als doel een getrouwheidskorting toe te kennen. Deze verantwoordingsplicht bestaat ook ten opzichte van **leveranciers of gebruikte diensten**: dus wie gegevens laat verwerken door iemand anders moet weten of deze organisatie dezelfde maatregelen heeft getroffen m.b.t. gegevensbescherming. Voor dit laatste zijn verwerkingsovereenkomsten nodig.

De meeste organisaties zullen daarom een **Functionaris voor de Gegevensbescherming** (FG) moeten aanstellen. Enkel heel kleine organisaties die weinig persoonsgegevens verwerken, hoeven dat niet. Die functionaris is een onafhankelijke gegevensbeschermingsspecialist die de organisatie adviseert over de beste maatregelen om persoonsgegevens te beschermen. Daarnaast moet de FG het **privacy-bewustzijn** van de organisatie verhogen. Het is ook zijn of haar taak om te controleren of de organisatie en de partners waarmee samengewerkt wordt voor de verwerking van persoonsgegevens, voldoende zorg dragen voor die gegevens.

De verantwoordelijkheid voor gegevensbescherming komt dus niet op de schouders van de FG te liggen, die **adviseert en controleert** alleen. De FG kan een medewerker zijn die ook andere taken uitvoert, maar hij of zij mag natuurlijk niet in de positie komen zichzelf te moeten controleren. Gegeven de omvang en diversiteit van deze taken is het duidelijk dat een **multidisciplinaire (bij)scholing** van deze functionarissen essentieel is. Dit betekent dat een FG naast de nodige juridische en technologische kennis ook expertise moeten hebben op vlak van communicatie, sociale onderhandeling en planning.[7]

Voor risicovolle verwerkingen – verwerkingen die door hun schaal of aard van persoonsgegevens een groter risico vormen – is een **Data Protection Impact Assessment** of DPIA nodig. Als specialist adviseert de FG over hoe zo'n *assessment* het best uitgevoerd kan worden. Het mag duidelijk zijn dat de grootschalige verwerking van de gegevens door heel grote online platformen zoals Facebook als risicovol kunnen beschouwd worden. Dit laatste geldt ook voor de verwerking van zogenaamde gevoelige gegevens zoals etnische afkomst of lidmaatschap van een vakbond. In een DPIA wordt het dataregister verder uitgewerkt om mogelijke risico's m.b.t. gegevensbeschermingsrechten van de betrokkene te identificeren. Voor de geïdentificeerde risico's worden oplossingen gezocht of gemotiveerd hoe dit risico niet verholpen kan worden. Het geheel van dit proces resulteert in een gegevensverwerkingsproces dat minder risicovol is en een rapport met de getroffen maatregels.

Wie kan wat doen om de GDPR te implementeren?

Er zijn **drie spelers die op dit moment actie kunnen ondernemen**. Zoals weergegeven in de onderstaande figuur zijn dit de toezichthoudende autoriteit, sectororganisaties en verwerkingsverantwoordelijken.

Er is **transparantie van twee kanten nodig** om de GDPR succesvol te implementeren. Verwerkingsverantwoordelijken hebben nood aan **bevestiging over de status van hun concrete verwerkingen**. Om die bevestiging te kunnen geven heeft de GBA nood aan een duidelijk overzicht per sector van 'typische' verwerkingsprocessen. Om dit schaalbaar te houden rekent de commissie op **input van sectororganisaties**.

[7] Om dit te ondersteunen plannen de VUB onderzoeksgroepen SMIT en LSTS (Law, Science Technology & Society studies) de Leerstoel 'DPO – Data Protection On the ground' op te richten, op initiatief van de Belgische Privacycommissie.

De GDPR stelt dat verantwoordelijken voor verwerking best in samenspraak met, of onder leiding van, sectororganisaties **sectorbrede afspraken** maken m.b.t. de meest voorkomende persoonsgegevensverwerkingen. Deze kunnen dan aan de GBA of toezichthoudende autoriteit worden voorgelegd om concreet te onderhandelen of afspraken te maken. Het is **pas wanneer er duidelijkheid is over deze processen**, dat er kan worden bepaald hoe deze al dan niet in overeenstemming is met de GDPR.

Het is dus de taak van de **verantwoordelijke voor verwerking** om contact op te nemen of zich te informeren omtrent initiatieven van sectororganisaties. De aangewezen persoon hiervoor in de organisatie is de FG: die kan met collega's overleggen over de praktische aanpak binnen de sector.

Sectororganisaties zorgen best voor **platformen om huidige praktijken** in kaart te brengen, gemeenschappelijke noden te identificeren en dan te bekijken hoe deze in overeenstemming met de GDPR kunnen worden gebracht. De Privacycommissie is al in gesprek met sectororganisaties om dit werk mogelijk te maken en voorziet verder ook verschillende documenten voor organisaties op hun website.[8]

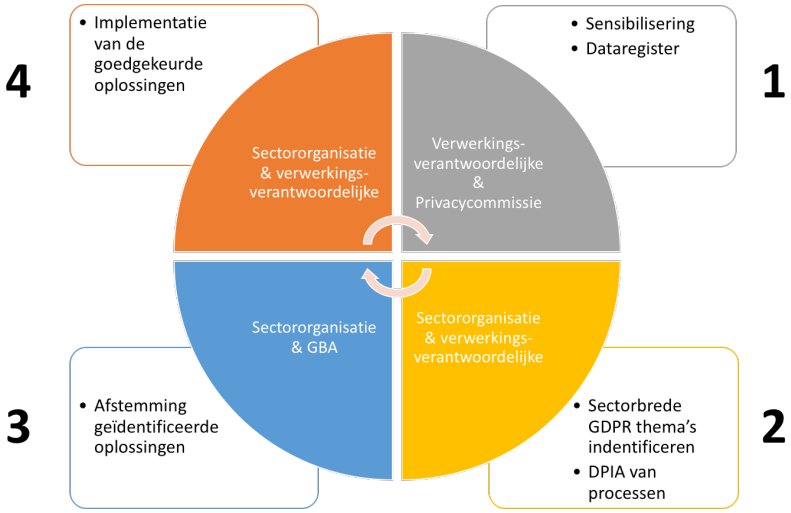
Het proces toegelicht

Uit onze interacties met verschillende sectoren (gemeenten, de advertentie-industrie, KMO's, mediabedrijven) die op zoek zijn naar oplossingen, hebben de meeste verwerkingsverantwoordelijken de weg gevonden naar documentatie van de Privacycommissie of een andere bron om iemand aan te stellen die sensibiliseert en een dataregister opstelt. Wij bevelen organisaties aan ook de volgende stappen hierna te zetten.

Door in een eerste stap processen per organisatie in kaart te brengen, kunnen in een tweede fase **gemeenschappelijke uitdagingen** worden geïdentificeerd waar een meer uitvoerige aanpak nodig is. Om accountability steeds mee te nemen in dit proces, stellen wij voor om hier een DPIA-proces te starten zodat de meeste risico's kunnen worden geïdentificeerd en worden aangepakt.

In stap 3 worden **sectorbrede oplossingen** voor verdere afstemming aan de GBA voorgelegd. De GBA zal met meer zekerheid kunnen goed- of afkeuren. Ten slotte kunnen goedgekeurde oplossingen weer door sectororganisaties en verwerkingsverantwoordelijken worden geïmplementeerd in stap 4.

[8] https://www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-0



Uitdagingen en obstakels

Dit proces zal niet zonder uitdagingen verlopen. Op dit moment doen veel organisaties voor de eerste keer de **dataregister-oefening**. Veel processen zijn niet in lijn met de principes van de GDPR, ook al hebben ze tot nu toe geen problemen veroorzaakt. Verwerkingsverantwoordelijken zullen dus weigerachtig zijn om 'slechte' praktijken kenbaar te maken. **Transparantie is een obstakel** om stap 2 te kunnen uitvoeren.

Los daarvan zullen verwerkingsverantwoordelijken en sectororganisaties in stappen 2 en 3 oplossingen formuleren en presenteren voor bepaalde delen van verwerkingsprocessen. Hier stelt zich opnieuw een transparantieprobleem. Wat als de **GBA de oplossingen afkeurt**? Is het hele verwerkingsproces en in sommige sectoren het hele verdienmodel dan illegaal?

Voor online reclame is bijvoorbeeld de situatie precair: er is een probleem met toestemming als rechtsgrond voor verwerking van persoonsgegevens en dit wordt nog verder onder druk gezet met de nog lopende herziening van de Europese ePrivacy Richtlijn.[9] De reden voor terughoudendheid van verwerkingsverantwoordelijken is, met andere woorden, een gebrek aan duidelijkheid in concrete toepassingen van de GDPR. Hier kijkt iedereen naar de Privacycommissie. Maar deze zit ook vast als zij geen inzage krijgen in concrete gevallen.

Aanbevelingen

Er is sprake van een overgangsperiode waarin enkele nieuwe principes voor verandering zorgen. Het gros van de GDPR is echter een voortzetting van de Richtlijn 95/46/EC. De onzekerheid m.b.t. boetes, de interpretatie van de GDPR en de werking van de GBA zijn problematisch voor verwerkingsverantwoordelijken. Langs de andere kant wil dit wel zeggen dat er ook niet meer gedaan kan worden dan waar wel al duidelijkheid over is. Dit wordt in het volgende stuk behandeld. Om de GDPR succesvol te interpreteren en implementeren moet alles in het werk gesteld worden om **transparanter** te zijn **over verwerkingsprocessen die niet in lijn zijn met de GDPR**.

[9] European Directive 2002/58/EC 'concerning the protection of personal data and the protection of privacy in the electronic communications sector'.

- **Geef sectororganisaties een mandaat en middelen om de verwerkingsprocessen in kaart te brengen.** Geef ze de ruimte om een agenda met de verschillende betrokken organisaties op te stellen om de GDPR verder te implementeren.
- **Gemeenschappelijke problemen moeten zo veel mogelijk gemeenschappelijk opgelost worden.** Vooral bij overheden en publieke diensten kan het niet de bedoeling zijn dat geld voor dezelfde uitdagingen meerdere keren wordt uitgegeven. De eilandenpolitiek zorgt er op dit moment voor dat vele zaken individueel worden opgelost. Ook hier is het duidelijk dat voornamelijk sectororganisaties meer middelen moeten hebben om op gemeenschappelijke problemen te werken.
- **De dreiging van boetes werkt contraproductief om de dialoog aan te gaan tussen de GBA en verwerkingsverantwoordelijken.** Voor organisaties die wel willen werken aan een beter gegevensbeleid moet het duidelijk zijn dat er een overgangsperiode is waarin vooral naar oplossingen wordt gezocht in plaats van sancties. In dit laatste geval is duidelijke communicatie over de prioriteiten van de GBA van belang.
- **Tot slot speelt de Functionaris voor de Gegevensbescherming op een aantal punten een sleutelrol en is diens professionaliteit van het grootste belang.** De GDPR verplicht de organisatie om de FG van middelen te voorzien om zijn of haar taken goed uit te voeren en zorg te dragen voor diens voortdurende professionalisering. Het faciliteren van de uitwisseling van 'best practices' en doorlopende multidisciplinaire scholing van FG's is een belangrijk aandachtspunt.

Wat kan SMIT doen?

SMIT, in het bijzonder de onderzoekseenheid 'Privacy, Ethics & Literacy' (SMIT-PEL), bieden diverse diensten, advies en participatieve methoden om privacy, ethiek en geletterdheid te ondersteunen en te versterken binnen en samen met private en publieke organisaties.

Wat betreft stap 1 in het GDPR-proces (zie hierboven), doet SMIT aan **sensibilisering d.m.v. workshops en een privacy-geletterdheid** quiz. Verder heeft SMIT ook de 'Data Flow Mapping'-methode ontwikkeld, die niet alleen gebruikt kan worden om een **dataregister op te stellen** maar ook om het **volledige proces in kaart te brengen** op een laagdrempelige manier.

In stap 2 zijn we in het Ecodalo-project (ICON), City of Things en de op te richten Leerstoel 'DPO – Data Protection On the ground' actief aan de slag met **workshops** om gemeenschappelijke problemen m.b.t. de GDPR te identificeren en te valideren met verschillende verwerkingsverantwoordelijken. Daarnaast worden ook **interdisciplinaire workshops** opgezet om GDPR-problemen op te lossen. Deze workshops hebben tot doel om de oplossingen verder af te toetsen met eindgebruikers. We kunnen hiermee de vereisten ('requirements') van de verschillende actoren en stakeholders die met persoonsgegevens werken, in kaart brengen, met als doel ze **succesvol** te **implementeren**.

Ten slotte is SMIT al vele jaren actief op het vlak van **onderzoek naar en advies inzake mediabeleid** en zijn we dus goed geplaats om beleidsaanbevelingen te doen omtrent GDPR-vereisten in de mediasector en deze samen met de sector uit te werken.

*Betrokken SMIT–onderzoekers zijn **Dr. Rob Heyman** (senior researcher), **Ine Van Zeeland** (researcher) en Prof. Dr. **Jo Pierson**, professor Users and Innovation in New Media en hoofd van de Privacy, Ethics and Literacy Unit bij imec-SMIT-VUB. De SMIT-PEL unit bestaat uit 15 junior en senior onderzoekers. Deze onderzoekseenheid heeft tot doel om (publieke) waarden in de ontwikkeling en het gebruik van digitale technologieën te identificeren, implementeren en verifiëren. We adresseren in het bijzonder aspecten van data privacy, vertrouwen en geletterdheid bij organisaties en gebruikers van digitale media en online platformen. Hiervoor bieden we innovatieve methoden en diensten aan, op basis van interdisciplinair wetenschappelijk onderzoek vanuit sociaal, technologisch, legaal en ethisch perspectief. Meer info: http://smit.vub.ac.be/*

*Eindredactie policy brief: **Tim.Raats@vub.be***