MIJN LEVEN ONLINE

MOGELIJKHEDEN EN VALKUILEN

Koning Boudewijnstichting
Samen werken aan een betere samenleving

NOTARIS.BE

MIJN LEVEN ONLINE

MOGELIJKHEDEN EN VALKUILEN

Koning Boudewijnstichting
Samen werken aan een betere samenleving

NOTARIS.BE

VOORWOORD

Ons leven is oneindig veel gemakkelijker geworden door de nieuwe informatie- en communicatietechnologieën. Met een paar klikken betalen we rekeningen of boeken we een vakantie. We lopen nooit nog verloren. We kunnen overal en altijd contact houden met de mensen die we graag zien.

Het gemak waarmee we surfen en swipen heeft ook een keerzijde. Bij alles wat we online doen, delen we persoonlijke gegevens – soms zonder erbij stil te staan. Die gegevens zijn goud in handen van advertentienetwerken en bedrijven. En in de handen van oplichters die graag van deze nieuwe kanalen gebruikmaken om hun slag te slaan.

Dit alles mag geen reden zijn om deze nieuwe digitale wereld te wantrouwen of de rug toe te keren. Gebruikers hebben veel meer mogelijkheden om zich online te beschermen dan ze soms denken. Met deze laagdrempelige praktische eerstelijnsgids willen de Koning Boudewijnstichting en de Federatie van het Notariaat hen slim leren omgaan met de nieuwe digitale technologieën.

Hoe waak je over je privacy online? Hoe doe je veilig aankopen? Hoe bescherm je je kind tegen cyberpesten? Mag je op sociale media kritiek geven op je werkgever? Wat kan je doen als je het slachtoffer werd van phishing? Kan je jouw muziekcollectie in de cloud overdragen aan je erfgenamen na je dood? Op deze en vele andere vragen geeft deze gids een antwoord.

1. PRIVACY & CYBERSECURITY

Persoonsgegevens en onlinesporen

Bij alles wat je online doet, deel je **persoonsgegevens** zoals naam, foto, telefoonnummer, bankrekeningnummer, e-mailadres, netwerk,... Het is niet altijd evident om te weten wie jouw gegevens heeft, wat ze met die informatie doen en of die eventueel misbruikt wordt.

Naast de gegevens die je bewust deelt, omdat je bijvoorbeeld een onlineformulier invult, zijn er de **sporen** die je – vaak onbewust – online achterlaat via logfiles, cookies en apps.

LOGFILES

Alles wat je online doet, wordt bewaard in logfiles. Die houden onder andere bij met welke provider je surft, wanneer je surft en hoe lang, welke pagina's je bezoekt en welke bestanden je aanklikt. Er worden geen persoonlijke gegevens bijgehouden, wel gegevens van je computer. Beheerders gebruiken logfiles om de website te verbeteren.

COOKIES

Websites gebruiken cookies, tekstbestandjes die op de harde schijf van laptop, computer, smartphone of tablet belanden wanneer je

een website bezoekt. Er zijn nuttige cookies, die ervoor zorgen dat de website je bij een volgend bezoek herkent, zodat je bijvoorbeeld niet telkens moet inloggen, of taal- of andere voorkeuren ingeven.

E-marketingbedrijven, webwinkels en sociale netwerken gebruiken ook cookies. Zij analyseren welke sites je bezoekt en welke producten je interessant vindt. Ze koppelen dat aan je persoonlijke gegevens – die je bijvoorbeeld online ingevuld hebt – om gerichte reclame te sturen of ze sturen die gegevens door naar andere bedrijven.

APPS

Snel een taal leren? Tientallen apps maken je tot een polyglot. Beter slapen? Een slaap-app zet je op weg. Gewicht verliezen, mediteren, je dag plannen? Veel apps maken het dagelijks leven comfortabeler. Maar elk gebruik ervan levert adverteerders nuttige informatie op. Telkens als je bijvoorbeeld een filmpje via de YouTube-app bekijkt, wordt die categorie in je Google-account toegevoegd aan de lijst van onderwerpen die je interessant vindt.

Hoe meer sporen jij nalaat, hoe interessanter je bent voor adverteerders.

SOCIALEMEDIAPLATFORMEN

Je kent het wel: je bekijkt schoenen op de website van een verkoper en plots achtervolgt dat paar je overal online. Socialemediabedrijven zoals Facebook gebruiken jouw zoek- of surfgedrag of likes om adverteerders te helpen gerichte reclame aan te bieden. Ze maken daarvoor onder andere gebruik van cookies en sociale plug-ins (knoppen waarmee je wat je online leuk vindt, kan delen via sociale media).

Hoe kan jij je beschermen?

Is dan niets van wat je online doet nog privé? Is privacy een illusie? Toch niet. De privacywetgeving legt beperkingen op aan bedrijven en organisaties die jouw gegevens willen verzamelen en gebruiken. Je kan ook zelf voorzorgsmaatregelen nemen om je gegevens en je toestellen te beschermen en om je onlinesporen te wissen.

PRIVACY BESCHERMEN

Let op, waakhond
Sinds 25 mei 2018 is de Europese Privacywet van kracht: de **General Data Protection Regulation** of **GDPR** (Algemene Verordening voor Gegevensbescherming of AVG). Deze nieuwe wetgeving beschermt je gegevens nog beter dan de wetgeving die België al had.

De GDPR bepaalt welke regels bedrijven, overheden en organisaties moeten volgen wanneer ze persoonlijke gegevens verzamelen, doorgeven, aanpassen, koppelen of kopiëren, en welke rechten jij hebt om je gegevens te beschermen.

Bedrijven, organisaties en overheden die met jouw persoonsgegevens aan de slag willen, hebben **plichten**:

- ze moeten een **rechtvaardige verwerkingsgrond** hebben om jouw gegevens te verwerken;
- ze moeten in hun **privacy policy** duidelijk maken waarom ze je persoonsgegevens verzamelen, wat ze ermee van plan zijn, wie ze kan raadplegen en hoe lang ze de gegevens bewaren;
- ze mogen de gegevens alleen gebruiken voor het opgegeven doel en **niet meer gegevens verzamelen en bijhouden dan nodig;**
- ze moeten steeds duidelijk vermelden waar je terechtkan met **vragen of klachten**.

Als een app of een website verschillende privacyopties heeft, moet de meest privacyvriendelijke optie standaard ingeschakeld zijn *(privacy by default)*.

Welke rechten heb je om je persoonsgegevens te beschermen?

RECHT OP INFORMATIE: je hebt het recht om te weten wie met jouw gegevens aan de slag gaat.

RECHT OM VRAGEN TE STELLEN: je mag altijd vragen of een organisatie of bedrijf gegevens over jou bewaart.

RECHT OP DIRECTE TOEGANG: je kan een afschrift krijgen van alle gegevens en opvragen waar de verwerker die gehaald heeft. De Gegevensbeschermingsautoriteit (GBA) heeft modelbrieven om dit verzoek op te stellen.

RECHT OP INDIRECTE TOEGANG: medische gegevens vraag je op via een tussenpersoon zoals de huisarts; gegevens in het kader van de veiligheid of om misdrijven te voorkomen of te bestraffen, kan je inkijken via het Controleorgaan op de Politionele Informatie (COC).

RECHT OP VERBETERING: onjuiste gegevens kan je laten verbeteren; onvolledige, irrelevante of verboden gegevens kan je laten wissen.

RECHT OP VERZET: je kan je verzetten tegen de verwerking van je gegevens, tenzij de gegevens nodig zijn om een overeenkomst te sluiten of uit te voeren, of wanneer de verwerking wettelijk verplicht is.

RECHT OM NIET ONDERWORPEN TE WORDEN AAN EEN GEAUTOMATISEERDE BESLISSING: bedrijven of organisaties mogen jouw gegevens analyseren om een profiel op te stellen; ze mogen dat profiel niet gebruiken om belangrijke beslissingen te nemen die jou nadeel kunnen berokkenen, bijvoorbeeld het verhogen van je verzekeringspremie.

Voor alle informatie over privacy: **www.ikbeslis.be** of **www.gegevensbeschermingsautoriteit.be**. Deze websites bevatten themadossiers, achtergrondinformatie en tips. Je vindt er ook alle adviezen en aanbevelingen.

NUTTIGE COOKIES BEHOUDEN, ADVERTENTIECOOKIES WEREN

Wil je niet dat bedrijven of andere organisaties jouw surfgedrag volgen? Je kan je browser (Internet Explorer, Chrome, Firefox, Edge, Safari) zo instellen dat je **cookies (selectief) weigert of wist**. Je kan de instellingen op elk moment wijzigen.

CHECKLIST
Cookies beheren

- Handmatig wissen: dit kan in elke browser via de 'instellingen' (bij browsegegevens wissen).
- Wissen na gebruik: je kan de browser de cookies laten verwijderen wanneer je de sessie afsluit.
- Alle cookies weigeren: mogelijk, maar niet aan te raden als je vlot wil surfen.
- *Third party cookies* (advertentie, sociale media) weigeren.
- Cookies aanpassen per website die je bezoekt.
- Adblockers: blokkeren advertenties en zo de cookies van advertentienetwerken. Denk er wel aan dat bijvoorbeeld mediabedrijven afhankelijk zijn van reclame-inkomsten.

GOOGLE: ALZIEND OOG UITSCHAKELEN

Google weet welke apps je gebruikt en wanneer je die gebruikt, welke zoekopdrachten je gedaan hebt, welke video's je bekeken hebt, welke mails je verstuurd hebt. Je kan een download aanvragen van alle gegevens die Google over jou heeft uit alle mogelijke Google-apps – inclusief gegevens die je verwijderd hebt.

Via 'Advertentie-instellingen' kan je zien welke gegevens Google van jou heeft en deze **informatie beperken of niet beschikbaar maken**. Als je niet wil dat Google via de app Google Maps in realtime opvolgt waar je bent, kan je de functie 'Locaties delen' uitschakelen, evenals de functie 'Web- en appactiviteit'.

Er bestaan zoekmachines die jouw zoekopdrachten niet bijhouden. De zoekresultaten kunnen minder precies zijn.

APPS: WEET WAT JE KOOPT

Apps willen veel weten. Ze vragen toegang tot je contactenlijst, foto's, camera of microfoon, je locatie. Je klikt vaak snel 'ok' wanneer apps toelatingen vragen. Soms is dat onschadelijk, maar vele apps harken meer persoonsgegevens bijeen dan ze nodig hebben en geven die ook door aan andere bedrijven.

Je leest daarom steeds best de **gebruiksvoorwaarden**, zodat je weet welke gegevens de app verzamelt, waarvoor hij die nodig heeft en aan wie hij ze doorgeeft. Als je vindt dat dit overdreven of te vaag is, kan je ervoor kiezen om de app niet te installeren of de ontwikkelaar contacteren en vragen waarom hij die info nodig heeft.

Apps moeten duidelijk maken wat ze met je gegevens doen. Ze moeten uitdrukkelijk en actief toestemming vragen, dus niet via een vooraf aangevinkt hokje. Ze moeten die toestemming vragen op een getrapte manier: bijvoorbeeld pas toegang vragen tot de camera wanneer de app de camera nodig heeft en niet bij de download.

MOBILE MAPPING

Via **Google Street View** kan je online alle straten in België bekijken. Als de openbare weg gefilmd wordt, staan er onvermijdelijk huizen, wagens, terreinen en personen op. Om in orde te zijn met de privacywet, moet Google gezichten en nummerplaten onherkenbaar maken. Als je dit onvoldoende vindt, kan je vragen om die **'blurring'** te versterken of om ook je wagen of woning onherkenbaar te maken. Het volstaat om 'Een probleem melden' aan te klikken bij Google. Als dat niet lukt, kan je de Gegegevensbeschermingsautoriteit (GBA) inschakelen.

CHECKLIST APPS

- Lees de gebruiksvoorwaarden, de privacy policy en de machtigingen, zodat je weet welke informatie de app verzamelt, wat hij ermee doet en wie toegang heeft tot die gegevens.
- Pas de instellingen aan, zodat je de toegang tot persoonsgegevens beperkt of afsluit.
- Log in met een paswoord in plaats van via Facebook.
- Vertrouw op gezond verstand: als de app naar jouw gevoel te veel informatie vraagt, installeer hem dan niet of contacteer de ontwikkelaar.

SOCIALEMEDIAPLATFORMEN: ADVERTENTIES BEPERKEN

Ontsnappen aan advertenties op sociale media is nagenoeg onmogelijk. Je kan er wel voor zorgen dat ze niet gebaseerd zijn op jouw onlinegedrag als je dat niet wil, zoals je leest in de checklist Direct Marketing. Je hebt ook steeds het recht om je kosteloos te verzetten tegen het gebruik van jouw gegevens voor direct marketing.

CHECKLIST DIRECT MARKETING

- Wees voorzichtig met likes. Zo vermijd je dat advertentienetwerken te veel weten over jouw voorkeuren.
- Herbekijk welke informatie je hebt opgegeven voor je profiel. Moet het sociale netwerk dat echt weten?
- Download je Facebookarchief via je accountinformatie. Zo heb je een zicht op advertentietopics die gelinkt zijn aan jouw profiel en adverteerders die – officieel – informatie over jou hebben.
- Pas de privacy- en advertentie-instellingen voor de computer of smartphone aan.
- Schakel locatiefuncties (waarmee sociale media via gps-locatiegegevens weten waar je bent) uit.
- Koppel eventueel klantenkaarten aan een e-mailadres dat je niet gebruikt. Data-exploitanten koppelen vaak klantenkaartgegevens aan onlinegegevens van sociale netwerken.

Socialenetwerksites zijn nooit echt 'privé'. Je hebt namelijk geen controle over de privacyinstellingen van je contacten noch over hun onlinegedrag. **Gedeeld is per definitie publiek.** Je kan wel het risico beperken. Socialenetwerksites geven je de mogelijkheid om je privacyinstellingen scherper in te stellen. Zo kan je kiezen wie jouw posts, foto's of filmpjes kan zien: alleen jijzelf, je 'vrienden', de contacten van je vrienden, of iedereen.

Als je daar niet op let, zijn je gegevens los wild. Dan kan bijvoorbeeld ook de fiscus op je socialemediaprofiel checken of je de bedrijfswagen die je voor 100% op de zaak hebt staan, niet gebruikt voor je vakantie in Italië. Inlichtingen verkregen via sociale netwerken zijn op zich geen bewijs, ze dienen als steunbewijs voor verder onderzoek.

Voor vragen en klachten:

- de Gegevensbeschermingsautoriteit (GBA) voor de verwerking van persoonsgegevens voor direct marketing: **www.gegevensbeschermingsautoriteit.be**;
- het Meldpunt van de FOD Economie (Algemene Directie Controle en Bemiddeling) als geen toestemming werd gevraagd voor reclame via e-mail: **https://meldpunt.belgie.be**.

Wat kan de Gegevensbeschermingsautoriteit voor jou doen?

HEB JE EEN VRAAG?

Dan kan je een beroep doen op hun eerstelijnshulpverlening. Die is telefonisch of via mail bereikbaar. Meer informatie over de bereikbaarheid van de hulplijn vind je op de website.

HEB JE EEN KLACHT?

Je stuurt een gedagtekende en ondertekende brief met uitleg en voldoende informatie over je zaak. De GBA bemiddelt tussen de partijen. Ze heeft onderzoeksbevoegdheid, ze kan controleren en sancties opleggen. De tussenkomst van de GBA is gratis.
www.gegevensbeschermingsautoriteit.be

HET RECHT OM VERGETEN TE WORDEN: VERVELENDE GEGEVENS LATEN VERWIJDEREN

Stel dat je een jeugdzonde hebt begaan die de media heeft gehaald. Je hebt ondertussen je leven op de sporen. Maar als je je naam googelt, slingert de zoekmachine je dat verleden in het gezicht. En in dat van je werkgever, of je zakencontacten of je nieuwe lief.

Je hebt het recht om te vragen je gegevens te wissen. Bedrijven moeten kunnen verantwoorden waarom ze dat niet willen of kunnen doen. Dit recht geldt niet alleen voor zoekmachines of voor online-krantenarchieven. Het geldt voor elke digitale opslag van jouw gegevens door elke dienstverlener.

Dit 'recht om vergeten te worden' is niet absoluut. Een diagnose die een arts in jouw onlinedossier noteert, kan je niet laten wissen. Er is bovendien het recht op correcte informatie voor andere gebruikers.

CHECKLIST ZOEKRESULTATEN VERWIJDEREN

- Neem contact op met de webmaster van de pagina die de informatie bevat. Anders verdwijnt de info uit de resultaten van de zoekmachine, maar blijft de link bestaan.
- Als dat niet lukt, ga je naar de pagina 'Inhoud verwijderen' van de zoekmachine en volg je de stappen. Je moet onder andere je identiteit bewijzen en voor elke link of URL uitleggen waarom je die weg wil.
- Je kan ook, gelijktijdig of als de zoekmachine hier niet op ingaat, een aangetekend schrijven sturen met hetzelfde verzoek.
- Als je geen gehoor krijgt, kan je klacht indienen bij de Gegevensbeschermingsautoriteit of bij de burgerlijke rechtbank.

CYBERSECURITY

Je kan je toestellen – en zo je gegevens – beveiligen door voorzorgen te nemen tegen hackers.

MALWARE: VIEZE BEESTJES BESTRIJDEN

Malware is een verzamelnaam voor ongewenste of schadelijke software. Je haalt die bijvoorbeeld binnen via de installatie van een gratis computerprogramma. Via malware kan je ongemerkt doorgestuurd worden naar namaaksites, zoals een website die lijkt op die van je bank, of valse pop-ups krijgen wanneer je aan het internetshoppen bent.

Spyware zijn computerprogramma's die jouw surfgedrag volgen en gegevens verzamelen zonder dat je het weet. Ze worden gebruikt door adverteerders of door hackers.

Bij ransomware gijzelt een virus je apparaat en/of je bestanden. Criminelen eisen een geldsom voor ze die willen vrijgeven. Ga niet in op hun vraag om te betalen, want je bent nooit zeker of ze jouw bestanden ontgrendelen. Schakel meteen je wifi uit als je zo'n virus hebt. Laat je toestel 'schoonmaken' en opnieuw installeren. Als je geregeld een back-up maakt, kan je jouw gegevens (laten) terugzetten. Je kan ook altijd eerst, via een ander toestel, surfen naar www.nomoreransom.org, een samenwerking van CERT.be en de Belgische en de Nederlandse politie. Op die website kan je checken of voor het gijzelvirus dat jouw bestanden vergrendeld heeft, de sleutel op de website staat. Die kan je gebruiken om je bestanden te ontgrendelen.

Meer informatie lees je in de brochure Ransomware van CERT.be, die je kan downloaden via **www.cert.be** of **www.safeonweb.be.**

CHECKLIST
SMARTPHONES EN LAPTOPS BESCHERMEN

- Doe regelmatige updates van je software en beveiliging.
- Maak back-ups.
- Leer valse e-mails herkennen.
- Gebruik goede antivirusbeveiliging.
- Gebruik sterke wachtwoorden.

www.safeonweb.be/nl/veilig-internetten

WAT ALS IEMAND ZICH ONLINE ALS JOU VOORDOET?

De meeste socialemediaplatformen hebben een knop om te melden wanneer iemand zich als jou voordoet. Als je geen eigen account hebt, kan je in het Help Centre van deze platformen een formulier invullen. Als de persoon, in jouw plaats, schadelijke daden heeft gesteld, kan je klacht indienen bij de politie voor identiteitsfraude.

KAN JE WEBCAM GEHACKT WORDEN?

Jazeker. Als je webcam gehackt is, kunnen anderen meekijken via je webcam zonder dat je die hebt ingeschakeld. Je kan het risico beperken met een goede virusscanner en een – sterk – wachtwoord voor je webcam. Er zijn in de handel ook webcamcovers te verkrijgen die je op je laptop kan plakken of schuiven.

Contacteer het Meldpunt van de FOD Economie (Algemene Directie Controle en Bemiddeling) bij phishing (p. 32-34), spam (ongevraagde e-mails) of ransomware: **https://meldpunt.belgie.be.**

2. GELD

KOPEN

Online aankopen is niet meer weg te denken uit ons leven. Vanuit de luie zetel een bloesje of een boek kiezen, zelfs via digitale weg aankoopcontracten sluiten die je vroeger per aangetekende zending in drievoud op de bus moest doen: handiger kan niet. Tenminste als je voorzorgsmaatregelen neemt om niet bedrogen uit te komen.

HOE WEET JE OF EEN WEBSHOP BETROUWBAAR IS?

Betrouwbare webshops bevatten altijd de ondubbelzinnige identiteit van de verkoper, een duidelijke prijs voor de producten, informatie over waar je de spullen kan terugsturen en wie je kan contacteren bij problemen. Voor Belgische webshops kan je uitkijken naar het BeCommerce-label.

BECOMMERCE: BEMIDDELAAR BIJ CONFLICTEN MET WEBWINKELS

BeCommerce is een Belgische vereniging van bedrijven die de kwaliteit van e-commerce willen garanderen. Leden respecteren de Europese en Belgische regels op het vlak van veiligheid, privacy en eerlijke handel. Daarnaast schikken ze zich naar de gedragsregels van het BeCommerce-kwaliteitslabel. Webwinkels met dit label zijn gecertificeerd door een onafhankelijk auditbureau. Consumenten die problemen hebben met een webwinkel en die geen gehoor vinden bij de shop zelf, kunnen de verzoeningscommissie van BeCommerce inschakelen. BeCommerce bemiddelt zowel voor klachten over leden als over niet-leden die actief zijn op de Belgische markt.

Op de website van BeCommerce vind je een formulier om een klacht te melden: www.becommerce.be.

Let erop dat je kan betalen via een beveiligde betaalzone, te herkennen aan de URL die begint met 'https://', of aan het slotje voor de URL. Je betaling wordt dan door de servers van een beveiligingsbedrijf van een code voorzien en veilig verwerkt. Betrouwbare betaaldiensten kan je ook checken via BeCommerce. Betrouwbare websites sturen meteen een ontvangstbevestiging met het overzicht van de bestelling en de betaalgegevens.

CHECKLIST
VEILIG ONLINE KOPEN

- Koop nooit iets wanneer je via een openbaar (onbeveiligd) wifinetwerk surft.
- Kies voor bekende websites; haal onbekende webshops door de zoekmachine.
- Controleer de URL van de webshop.
- Let erop dat je kan betalen via een beveiligde betaalzone.
- Als je geen betaalbevestiging ontvangt, neem je best contact op met de beheerder van de website.
- Controleer regelmatig je rekeninguittreksels.

WAT ALS EEN ONLINEAANKOOP FOUT LOOPT?

Ondanks alle voorzorgsmaatregelen kan een onlineaankoop verkeerd gaan. Er wordt meer geld van je kredietkaart gehaald dan voorzien, het pakje wordt niet geleverd of de verkoper is ondertussen failliet gegaan.

Contacteer altijd eerst de webshop en houd de e-mails die je uitwisselt bij als bewijs. De verkoper is verantwoordelijk tot het moment dat jij de bestelling in handen hebt. Als de verkoper niet reageert, kan je een klacht indienen bij de ombudsdienst van bpost **(www.omps.be)**. Die kan bemiddelen.

Als ook dat niet lukt of je bent opgelicht, kan je contact zoeken met de FOD Economie, via hun meldpunt. Je kan ook een klacht indienen via www.testaankoop.be/klachtenbox of via het ODR-klachtenplatform van de EU **(www.eccbelgie.be)**.

Kredietkaarten bieden een verzekering aan tegen internetfraude en tegen bestellingen die niet geleverd zijn, die beschadigd zijn, of die niet overeenkomen met wat je besteld had. Als je kan aantonen dat je geprobeerd hebt om het bedrag te recupereren en dat er geen kwaad opzet is, krijg je het bedrag teruggestort. Je moet de aangifte wel doen binnen drie maanden na de bestelling.

Als er een probleem is met je kredietkaart, contacteer dan jouw bank om je kaart en je internetbanking te laten blokkeren. Zet kredietkaartgegevens niet op je computer of laptop, dan kunnen hackers ze niet vinden.

WAT ALS JE PAKJE IS ZOEKGERAAKT?

1.
Contacteer de klantendienst van de koerierdienst

3.
Dien een klacht in bij de ombudsman van bpost

2.
Contacteer de verkoper

Voor binnenlandse zendingen: een klacht bij het meldpunt van de FOD Economie: **https://meldpunt.belgie.be**

Voor buitenlandse zendingen: een klacht bij het Europees Centrum voor de Consument (ECC): **www.eccbelgie.be**

WAT ALS JE AANKOOPT VIA WEBWINKELS BUITEN DE EU?

Als je spullen bestelt bij webshops in de Verenigde Staten of andere landen buiten de Europese Unie, kan je voor onaangename verrassingen komen te staan wanneer de pakjesdienst voor je deur staat. Die kan je namelijk een extra rekening voorschotelen met invoerrechten, btw en accijnzen op aankopen van buiten de Europese Unie. Op dat moment heb je twee opties: bijbetalen of het pakje weer meegeven. Als je aankoopt in webwinkels van buiten de Europese Unie, check je best eerst hoeveel invoerrechten je betaalt.

Op de website van bpost vind je ook een lijst van de tarieven voor invoerrechten: **www.bpost.be**.

KAN JE DE AANKOOP VAN EEN HUIS VIA E-MAIL BEVESTIGEN?

In de vastgoedsector wordt steeds vaker e-mail gebruikt om over een verkoop te onderhandelen en hem te bevestigen. Iedereen heeft overvolle agenda's, het is gemakkelijker om dit proces via e-mail af te handelen. Tot voor kort was er onzekerheid over de bewijswaarde van e-mail voor de verkoop van een woning.

Het is nu echter mogelijk om een geldig verkoopsakkoord te sluiten via e-mail, sms, WhatsApp of andere digitale kanalen. Er is geen digitale handtekening nodig. Koper en verkoper moeten nadien wel nog steeds de verkoopsakte tekenen bij de notaris.

Bij betwisting kan een rechter niet langer een e-mail of ander digitaal bericht negeren als bewijs. Maar het is slechts een begin van bewijs. Als je als verkoper of koper van een woning toch aanvullende zekerheid wil over een bod, heeft Test-Aankoop een modelbrief, te downloaden via hun website, die de koop schriftelijk bevestigt voor een termijn die koper en verkoper vastleggen – in afwachting van de akte.

BIDDIT.BE: ONLINE EEN WONING (VER)KOPEN OP EEN EENVOUDIGE EN VEILIGE MANIER

Biddit.be is een initiatief van de Federatie van het Notariaat (Fednot). Via de onlineverkoop kunnen kopers op een eenvoudige, transparante en veilige manier bieden op een woning. Een woning kopen via www.biddit.be is eenvoudig. Je weet meteen in welke prijscategorie een woning valt, want bij elk aanbod staat een startprijs. Een bod uitbrengen kan via je laptop met je eID-kaart, of via je mobiel toestel, met de app Itsme. Bieden kan manueel of automatisch tot een maximumbedrag dat je vooraf bepaald hebt en alleen jij kent. Elk bod is zichtbaar voor iedereen die Biddit.be bezoekt. Wanneer de biedingsperiode van 8 dagen voorbij is, weet je meteen of jij de hoogste bieder bent. In dat geval contacteert de notaris je om de verkoop te finaliseren. Een pak sneller dan bij een klassieke verkoop. Bij de onlineverkoop heeft de notaris immers alle controles vooraf afgerond, zodat je als koper én als verkoper meteen weet waar je aan toe bent. Let wel: elk bod is bindend.

Meer informatie?
www.biddit.be of via de notaris

DIGITALE HANDTEKENING

Sinds 2016 is de digitale handtekening evenwaardig aan de papieren handtekening en zijn digitale documenten dus evenwaardig aan papieren documenten. Je kan contracten afsluiten via e-mail. Digitale documenten moeten wel ondertekend zijn met een gekwalificeerde handtekening die extra veiligheidsgaranties biedt. Voor een digitale handtekening kan je jouw eID-kaart gebruiken. Daarvoor heb je een kaartlezer en de codes van je eID-kaart nodig, en moet je de software downloaden.
Meer informatie via https://eid.belgium.be/nl.

DELEN

Steeds meer mensen kopen geen eigen boormachine of pastamaker of wagen meer, maar delen er één. De **deeleconomie** maakt handig gebruik van het internet en mobiele technologie om zich te organiseren. Winst staat niet centraal, het gaat om het delen van spullen of diensten, al wordt soms een (kleine) vergoeding gevraagd.

Daarnaast heb je de **platformeconomie**, vaak commerciële activiteiten die gebruikmaken van nieuwe technologieën om particulieren in contact te brengen met particuliere producenten van goederen of diensten; daarbij wordt altijd een vergoeding gevraagd. Listminut is een voorbeeld van zo'n platform.

Peer-to-peerinitiatieven krijgen van de wetgever ruimte om te groeien en zich te ontwikkelen. Dit betekent echter niet dat er geen regels of voorwaarden gelden.

Voor algemene informatie over deelplatformen, hoe ze werken en onder welke voorwaarden je er gebruik van kan maken, kijk bij: **www.bewustverbruiken.be**, **www.autodelen.net** of de deelplatformen zelf.

DELEN EN VERZEKERINGEN

Als je actief bent in de deel- of platformeconomie, check je best met je verzekeraar of je verzekering burgerlijke aansprakelijkheid ('familiale'), brandverzekering of autoverzekering volstaat. Steeds meer verzekeraars spelen ook met nieuwe formules in op deze manieren van delen en gebruik.

Voor meer informatie over de deel- en platformeconomie en verzekeringen: **www.abcverzekering.be** of bij je verzekeringsmaatschappij.

WAT ALS JE IETS HEBT UITGELEEND OP EEN ONLINEDEELPLATFORM EN HET BESCHADIGD TERUGKOMT?

Als je je spullen deelt op een onlineplatform, controleer je best samen met de gebruiker in welke staat de spullen zijn wanneer hij ze komt oppikken en wanneer hij ze terugbrengt. Op sommige deelplatforms kan je afspraken vastleggen. Als je de spullen niet of kapot terugkrijgt, moet de gebruiker ze (laten) repareren of vervangen.

WAT ALS EEN KLUSJESMAN VIA EEN DEELPLATFORM GEWOND GERAAKT?

Check met je verzekeraar of je familiale verzekering voldoende uitgebreid is. Als je een beroep doet op bezoldigde huishoudelijke diensten, moet je een verzekering voor huispersoneel hebben (arbeidsongevallenverzekering).

WAT ALS JE JE AUTO DEELT MET ANDEREN OF VIA EEN DEELPLATFORM?

Als je jouw eigen wagen op een peer-to-peerplatform (Cozycar, Sharynx, Dégage, Tapazz, Drivy, Caramigo) aanbiedt of deelt met je buren, zijn er regels voor hoe je schade meldt, hoe je verzekerd bent, wat er gebeurt als er een boete in de bus valt of er een conflict is met iemand die je wagen gebruikt heeft.

WAT ALS JE EEN KAMER VERHUURT VIA AIRBNB EN DE GAST VEROORZAAKT SCHADE?

Wanneer je een kamer of een flat verhuurt via het platform Airbnb, val je onder de regelgeving in jouw Gewest voor het verhuur van kamers en woningen voor toerisme.

INFORMATIE OVER DE REGELGEVING:

Vlaams Gewest:
www.toerismevlaanderen.be/logiesdecreet/aanmelden
Brussels Gewest:
www.werk-economie-emploi.brussels/nl_BE/toeristische-logies
Waals Gewest:
www.wallonie.be/fr/formulaire/detail/37415

CHECKLIST
VEILIG TWEEDEHANDS KOPEN ONLINE

- Bekijk het profiel van de verkoper en check zijn reputatie op het platform en/of via een zoekmachine.
- Stel vragen over het item, vraag naar de exacte eigenschappen. Bewaar de correspondentie, het oorspronkelijke zoekertje en de bankoverschrijving.
- Vraag persoonlijke gegevens zoals een adres of een telefoonnummer.
- Probeer zeker dure spullen persoonlijk op te halen, zo kan je inspecteren voor je ze meeneemt.
- Wees waakzaam bij verkopers in het buitenland. Gebruik zeker geen betaalkanalen als Western Union, Moneygram of cheques.
- Als het item toch niet of kapot aankomt, neem je best eerst contact op met de verkoper. Als er geen reactie komt, kan je een klacht indienen bij de politie.

Als een gast schade berokkent aan de kamer of de flat die je verhuurt, kan je een beroep doen op Airbnb. Als je verhuurt via Airbnb of een ander platform, verwittig je ook best je verzekeraar om te weten of je brandverzekering en familiale verzekering (verzekering burgerlijke aansprakelijkheid) aangepast moeten worden.

Als je huurt via Airbnb, kan je uit handen van oplichters blijven door alle verrichtingen te doen via de officiële website. Ga niet in op voorstellen om de reservatie en de betaling verder via e-mail af te handelen. Voer alle communicatie via het platform en betaal met een kredietkaart via de beveiligde betaalpagina.

DEELPLATFORMEN EN DE FISCUS

Voor inkomsten uit de deeleconomie komt er een fiscaal gunstregime. Tot 6.000€ per jaar is dan vrijgesteld van belastingen. Dit gunstregime geldt alleen voor belastingplichtige particulieren die peer-to-peer spullen of diensten aanbieden. De inkomsten mogen geen verband houden met een zelfstandige activiteit. Het deelplatform moet erkend zijn door het Ministerie van Financiën.

Om te weten welke de erkende deelplatformen zijn en meer te lezen over de voorwaarden:
https://financien.belgium.be/nl/particulieren/belastingvoordelen/deeleconomie.

BANKIEREN

Niemand wil voor de onaangename verrassing van een geplunderde rekening of kredietkaart komen te staan. Banken doen er alles aan om hun online- en mobiele toepassingen strak te beveiligen. Maar die veiligheidsprotocols halen weinig uit als hun klanten via de eerste de beste e-mail hun bankgegevens doorspelen. Gebruikers zelf kunnen veel onheil voorkomen met enkele eenvoudige voorzorgsmaatregelen.

HOE HERKEN JE EEN PHISHINGMAIL?
WAT KAN JE DOEN ALS ZE JE TOCH BEET HEBBEN?

Bij phishing proberen oplichters je jouw persoonlijke gegevens, rekeningnummers en pincodes te ontfutselen door zich voor te doen als jouw bank (of het bedrijf dat je kredietkaart beheert of de politie of een andere instelling).

Je ontvangt een e-mail die lijkt op een mail van je bank (of van een bedrijf of een andere instelling), met de mededeling dat je moet

inloggen via de link in het bericht. Als je dat niet doet, dreigt de mailer in vaak dwingende taal dat bijvoorbeeld je kaart geblokkeerd zal worden. Via de link beland je op een valse maar geloofwaardig uitziende website waar je je pincode of de code die je kaartlezer genereert, moet invoeren ter controle. Zodra je dat doet, kunnen de oplichters je rekening plunderen.

Oplichters passen voortdurend hun werkwijze aan. Phishingmails worden almaar professioneler opgesteld. Ze passen hun boodschap aan en zoeken nieuwe kanalen. Naast e-mail gebruiken ze steeds vaker sociale media zoals Facebook of WhatsApp om mensen in de val te lokken. Vaker gaan ze ook kleinere bedragen, in meerdere pogingen, afhalen, zodat ze langer onder de radar blijven.

HOE VOORKOM JE PHISHING?

Phishing is te voorkomen met enkele voorzorgsmaatregelen. De belangrijkste: **geef nooit je persoonlijke gegevens of codes online door.** Een bank zal nooit via e-mail om je persoonlijke codes vragen. Als je zo'n verzoek krijgt, moeten er alarmbellen afgaan.

Phishingmails worden professioneler, maar toch zijn ze vaak nog te herkennen: door het vreemde e-mailadres van de **afzender**, dat verschilt van het officiële e-mailadres van de bank (bijvoorbeeld met een extensie die geen .be of .com is), door de **aanspreking** (geen aanspreking met naam) en door de **dwingende toon** ('uw kaart wordt geblokkeerd als u niet reageert'). Bovendien verloopt internetbankkieren steeds via een **beveiligde website**, met slotje in de adresbalk, beginnend met https://. Je surft voor verrichtingen ook steeds best direct naar de **website van de bank**, in plaats van gebruik te maken van indirecte links.

Veel phishingverzoeken kan je tegenhouden met een **goede antivirusbeveiliging met een stevige firewall en spamfilter**. Als je de afzender niet kent, klik dan nooit op links in het bericht.

Je stuurt een verdachte mail best naar **je bank**, op phishing@(naam van de bank).com of.be. De bank kan dan de verdachte link blokkeren en zo voorkomen dat andere klanten opgelicht kunnen worden. Je kan het bericht ook signaleren aan het **meldpunt van de FOD Economie** (https://meldpunt.belgie.be) of doorsturen naar *verdacht@safeonweb.be* van het **Centrum voor Cybersecurity België** (CCB). Bij het CCB wordt het bericht gescand en indien nodig verder onderzocht. Frauduleuze berichten signaleert het CCB aan de belangrijkste antivirussoftwarebedrijven en leveranciers van internetbrowsers, zodat ze de valse links kunnen blokkeren.

CHECKLIST
VEILIG ONLINE BANKIEREN

- Let op met e-mails van onbekende afzenders.
- Klik nooit op een verdachte link in een e-mail.
- Zorg voor een goede antivirusbeveiliging.
- Gebruik de recentste versie van apps, software, besturingssystemen en update ze. Ze bevatten beveiligingspatches.
- Houd je bankrekening in de gaten om verdachte transacties op tijd te zien.
- Als je bankiert met smartphone, sluit steeds je sessies af wanneer je klaar bent.
- Als je smartphone gestolen wordt, laat meteen je kaart blokkeren. Zo blokkeer je de toegang tot de bankapp.
- Gebruik geen openbare wifi-verbinding voor je online bankieren.
- **Geef nooit je persoonlijke codes door.**

BEN JE SLACHTOFFER GEWORDEN VAN PHISHING?

Contacteer meteen je bank of Cardstop om je kaart(en) te blokkeren. Als er al geld van de rekening verdwenen is, moet je een klacht indienen bij de politie. Je kan dan hiermee bij de bank een verzoek indienen om de som te recupereren. De bank bekijkt geval per geval of je te goeder trouw bent geweest en/of je niet nalatig bent geweest. In de meeste gevallen vergoeden banken de verloren sommen, al heeft dit je dan wel veel kopzorgen en administratieve rompslomp opgeleverd.

MOBIELE BETALINGSAPPS

Bij handelaars scan je de QR-code van de mobiele betalingsapp om te betalen met je pincode, of kies je de handelszaak uit een lijst op je smartphone. Deze betalingsapps zijn in je smartphone gekoppeld aan je zichtrekening (na eenmalige installatie via je kaart) en aan je telefoonnummer of e-mailadres. Zo kan je bijvoorbeeld direct geld overmaken aan familie of aan vrienden wanneer jullie samen op stap zijn. Meer informatie vind je op de website van je bank. Lees ook de gebruiks- en privacyvoorwaarden om te weten wat er met jouw gegevens gebeurt.

NIEUWE REGELS VOOR ONLINEBETALINGSVERKEER

Jouw bank moet vanaf het najaar van 2018 derde partijen, zoals andere banken of webshops, toegang geven tot jouw gegevens als jij daar de toestemming voor hebt gegeven. Het wordt dan bijvoorbeeld mogelijk om een overzicht van de zichtrekeningen die je hebt bij andere banken te integreren in de app van je bank, zodat je alle betalingen via één app kan regelen. Om via webshops te betalen zonder bank- of kredietkaart. Of om via apps op basis van je uitgaven voor telecom of energie prijsvergelijkingen te krijgen voor andere leveranciers. Deze derden worden gecontroleerd door de Nationale Bank en volgen strenge veiligheidsvoorschriften.

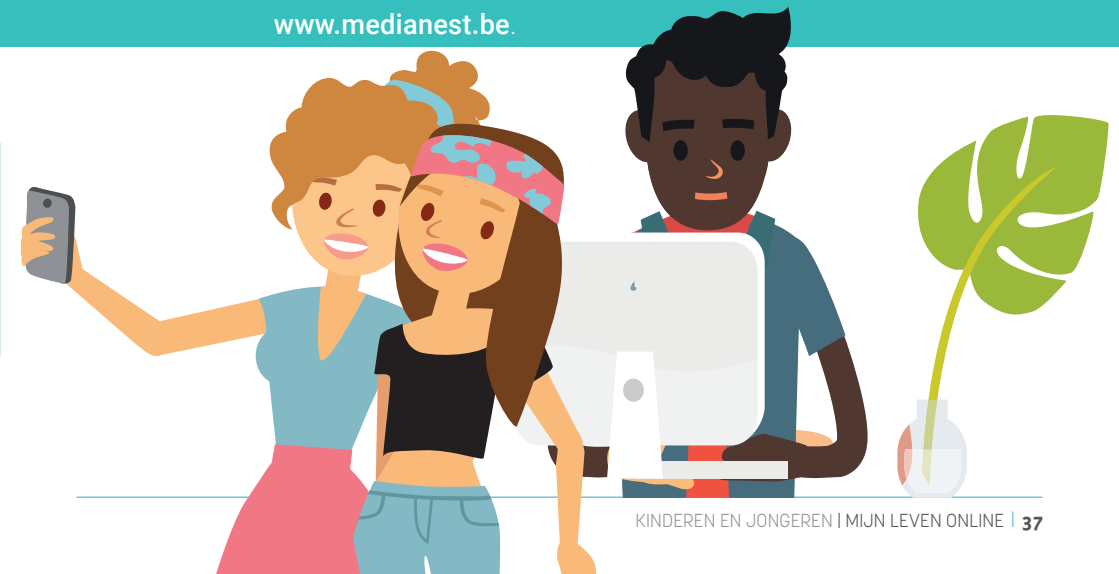
Meer informatie over veilig online bankieren vind je op de website van Febelfin: **www.safeinternetbanking.be**. Die informeert ook over de verschillende vormen van onlinefraude. Je kan ook terecht op de website van de FOD Economie en van Cyber Security België **(www.safeonweb.be**).

3. KINDEREN EN JONGEREN

De grootste valkuil is denken dat deze digital natives niets meer te leren hebben. Kinderen en jongeren hebben de technologie misschien in de vingers, maar ze missen vaak nog de emotionele of inhoudelijke vaardigheden die hen online weerbaar maken.

Ouders en leerkrachten hebben dus zeker een rol om kinderen en jongeren online te begeleiden, te leren risico's in te schatten, te helpen kritisch om te gaan met wat ze online vinden, cyberpesters of fake news te tackelen. Om kinderen en jongeren te leren wat privacy is en hoe ze de hunne en die van anderen respecteren.

Voor algemene informatie, tips & tricks over hoe kinderen en jongeren online te begeleiden en algemene informatie over internet en sociale media: **www.medianest.be**.



JONGE KINDEREN

KAN JE ONGEPASTE INHOUD OP HET INTERNET AFSCHERMEN VOOR KINDEREN?

Er is geen waterdichte oplossing. Het blijft dus belangrijk voor ouders om betrokken te zijn bij de onlineactiviteiten van hun kind en om te **praten over wat het kind online vindt en ziet**. Technische hulpmiddelen alleen kunnen dit continue gesprek tussen ouders en kinderen niet vervangen.

Dit gezegd, in veel webbrowsers en apps kan je de toegang voor kinderen geheel of deels beperken. Zo heeft Google een optie **'safe search'** die bepaalde inhoud zoals pornografie weert uit zoekresultaten. In de meeste browsers kan je aparte profielen maken voor gezinsleden en zo zoekopties beperken naargelang de leeftijd.

YouTube, een geliefde onlinepleisterplek van kinderen en jongeren, heeft een **'restricted mode'**: die schermt bepaalde inhoud af en toont commentaren – die soms grover zijn dan de filmpjes – niet. Als kinderen zelf graag filmpjes posten en ouders niet willen dat iedereen die kan zien of er commentaar op kan geven, kunnen ze de privacyinstellingen van het kanaal op 'privé' zetten.

Van apps voor iOS of Android kan je controleren vanaf welke leeftijd ze geschikt zijn aan de hand van de PEGI-scores, die waarschuwen tot welke leeftijd een game, film of app schadelijk kan zijn voor kinderen. Je kan de zoekfunctie van een account in de appwinkels zo aanpassen dat kinderen die een app zoeken, alleen apps tot aan een bepaalde PEGI-score te zien krijgen **(www.pegi.info)**.

Voor kinderen die informatie zoeken op Vlaamse websites is het uitkijken naar het WAT WAT- label (voorheen: Trusty). Websites met dit label geven betrouwbare informatie op maat van kinderen. Meer info op **www.ambrassade.be/nl/kennis/wat-wat-label.**

MOGEN KINDEREN ACTIEF ZIJN OP SOCIALE NETWERKEN?

De meeste sociale netwerken hanteren een leeftijdsgrens van 13 jaar om zelf een profiel aan te maken. Dat is ook de leeftijd die de Belgische wetgever heeft vastgelegd voor de toegang voor minderjarigen: vanaf dan kunnen jongeren zelf toestemming geven om hun persoonsgegevens te laten verwerken. Jongere kinderen mogen ook onlinediensten zoals sociale media gebruiken als ze daarvoor de toestemming hebben van hun ouders en als dit in overeenstemming is met de gebruiksvoorwaarden van het platform.

CHECKLIST SCHERMTIJD

- Praat met je kind over schermgebruik. Pas de regels aan de leeftijd aan.
- Je kan samen een schema opmaken om te bepalen wanneer en waar je kind op tablet, computer of smartphone mag. Op **www.medianest.be** vind je tools.
- Niet de duur, maar vooral het effect op je kind en het evenwicht met andere activiteiten zijn belangrijk.
- Geef zelf het goede voorbeeld: als je kind geen smartphone aan tafel mag, leg dan ook de jouwe weg.
- Als je de duur van het gebruik wil beperken: er zijn apps die de toegang tot computer, tablet, smartphone, console of smart-tv na een bepaald uur of na een bepaalde tijdspanne blokkeren.

In de praktijk zijn kinderen jonger dan 13 jaar massaal actief op Facebook, Instagram, Snapchat, WhatsApp of YouTube – al dan niet met medeweten van hun ouders. Als een kind onder 13 jaar een profiel wil en de ouders laten dat toe ondanks de gebruiksvoorwaarden, dan openen ze dat best samen. Zo kunnen ze privacy-instellingen en afspraken vastleggen, bijvoorbeeld over toevoegen van contacten.

Op bepaalde websites voor kinderen kunnen ze oefenen met sociale netwerken op een veilige manier. Bij Ketnet bijvoorbeeld kunnen kinderen een profiel aanmaken, met het e-mailadres van de ouders, vanaf zes jaar. Een kind kan dan vrienden toevoegen, filmpjes of foto's posten, commentaren laten.

MAG JE FOTO'S VAN JE KIND DELEN OP SOCIALENETWERKSITES?

Het is goed om voorzichtig te zijn met het delen van foto's en filmpjes van je kinderen. Je kan met hen bespreken, zodra het kan, wat ze wel of niet graag hebben. Je kan, telkens als je een foto online wil zetten, vragen of ze het daarmee eens zijn. Kies bij voorkeur een foto waarop ze niet meteen herkenbaar zijn, zoals een foto vanop de rug of met een filter, en waak over de privacyinstellingen van jouw profiel.

PORTRETRECHT

Niemand mag online een foto van jou of jouw kind plukken en gebruiken zonder toestemming. Ook als ze zelf de foto genomen hebben, mogen ze die niet verspreiden zonder toestemming. Foto's nemen van de publieke ruimte, waar jij toevallig op staat, mag wel. Als je ziet dat iemand een foto van jou of jouw kind gebruikt heeft zonder toestemming, mag je die persoon vragen de foto te verwijderen. Als die persoon de foto op sociale media heeft gezet en niet reageert op je verzoek om hem weg te halen, kan je het socialemediabedrijf vragen om dat te doen.

Meer informatie over portretrecht vind je op **www.mediawijs.be.**

MAG JE HET PRIVÉPROFIEL VAN JE KIND BEKIJKEN? ZIJN E-MAILS LEZEN? SURFGEDRAG MONITOREN?

Kinderen hebben recht op privacy, ook in wat ze online doen. Ouders gaan dus best niet te ver in de controle van het internetgebruik van hun kind. Het is zoeken naar een evenwicht tussen bescherming en controle enerzijds en het recht op een privéleven van het kind anderzijds.

Sommige ouders proberen te controleren door hun kind te vragen hen toe te voegen als 'vriend' in hun sociale netwerken, maar zeker tieners zijn hier vaak niet mee opgezet. Als ze toch (moeten) toezeggen, passen ze vaak hun privacyinstellingen zo aan dat ze een deel van de inhoud kunnen afschermen of wijken ze uit naar andere sociale media.

Er zijn apps op de markt die (verregaande) ouderlijke controle mogelijk maken, zoals het monitoren van de activiteit van het kind op socialemediakanalen vanop afstand of het volgen van zijn locatie. Experts raden een te restrictieve aanpak af: kinderen moeten fouten kunnen maken en zo online weerbaar worden.

MOGEN BEDRIJVEN KINDEREN ONLINE BESTOKEN MET RECLAMEBOODSCHAPPEN?

Kinderen en jongeren hebben het recht zich vrij te ontwikkelen. Door hun onlinezoekgedrag te volgen en direct-marketingboodschappen daarop af te stemmen, worden ze al vroeg in hokjes geduwd. Jongeren kunnen bovendien niet inschatten wat het betekent wanneer (socialemedia)bedrijven met hun gegevens aan de haal gaan. Ze zien het verband niet tussen hun zoekgeschiedenis of Facebookprofiel en de reclame die ze krijgen aangeboden.

CHECKLIST
TUSSEN CONTROLE EN VRIJHEID

- Als je het kind de computer, laptop of tablet in de woonkamer laat gebruiken, kan je een oogje in het zeil houden.
- Je kan afspraken maken over wat wel of niet mag, bijvoorbeeld geen foto's of filmpjes doorsturen zonder toestemming.
- Bekijk samen hoe ze hun privacyinstellingen beheren en wat te doen als ze met iets vervelends te maken krijgen.
- Als je interesse toont voor het onlineleven van je kind, vergroot de kans dat het naar jou komt als er iets mis is.
- Als je (jongere) kinderen controleert, is het beter om open kaart te spelen. Achter de rug van kinderen om snuisteren in e-mails of Facebookprofiel kan het vertrouwen schaden.
- Als een kind online een stommiteit begaat, leert het door samen te praten over de gevolgen van zijn daden.

De Europese Unie raadt gerichte reclame op basis van surfgedrag van jongeren af. Maar er is geen absoluut verbod. Van kinderen onder dertien jaar moeten ouders toestemming geven om de persoonsgegevens van het kind te verwerken. De reclame-industrie reguleert ook zelf. Adverteerders wordt aangemaand geen direct marketing te richten naar kinderen jonger dan 12. In de praktijk is dat moeilijk te beheersen als kinderen online gemakkelijk kunnen liegen over hun leeftijd.

WAT ALS EEN KIND VIA EEN APP AANKOPEN DEED DIE HET NIET MOCHT DOEN?

Voorkomen is beter dan achteraf proberen de som te recupereren. Ouders leggen best goed uit wat in-appaankopen (aankopen die aangeboden worden in de app zelf) zijn en hoe je die herkent, en maken afspraken over wat wel of niet mag. Ze kunnen kiezen om

hun kredietkaart niet te koppelen aan de appwinkel of aankopen via de appwinkel beveiligen met een wachtwoord. Ze kunnen ook werken met een prepaidkaart. Ze kunnen bericht krijgen bij een aankoop, voor als hun kind toch een omweg vond, zodat ze erger kunnen voorkomen.
Het bedrag van ongewenste aankopen recupereren is niet evident. Veel hangt af van de leeftijd van het kind: als het kind al geacht wordt te weten wat het doet, zal een verkoper minder inschikkelijk zijn. Aanbieders van apps moeten het voor gebruikers wel duidelijk maken dat het om in-appaankopen gaat.

WAT ALS ONBEKENDEN CONTACT ZOEKEN MET EEN KIND OF TIENER ONLINE?

Het is belangrijk om kinderen te leren **voorzichtig te zijn met vriendschapsverzoeken** van onbekenden op sociale media of met contacten in chatrooms; geen verzoeken te aanvaarden van mensen die ze offline niet kennen; **nooit persoonlijke gegevens door te geven**; en als ze voelen dat iets niet in de haak is, **een ouder of een andere volwassen vertrouwenspersoon aan te spreken**.

Als een kind een ongepast contact signaleert, kan het zelf of samen met jou **bewijsmateriaal** (chatgesprekken met tijdstip, sms'jes, foto's) bijhouden via schermafdrukken. Je kan daarmee contact opnemen met het **socialemediabedrijf en met Child Focus.** Onlinegrooming, waarbij pedoseksuele daders proberen kinderen tot een echte afspraak te brengen, is strafbaar. Stap naar de **politie** om erger te voorkomen, ook voor andere kinderen.

WAT ALS DE ENE OUDER TOESTEMMING GEEFT EN DE ANDERE NIET?

Ouderlijk gezag wordt uitgeoefend door beide ouders. Zoals in andere opvoedingskwesties is het mogelijk dat de ouders voor het onlineleven van het kind niet op dezelfde lijn zitten. Idealiter komen ze, ook als ze uit elkaar zijn, tot een vergelijk. Bij woelige

echtscheidingen of relatiebreuken kan het gebruik van sociale media een splijtzwam zijn. De ene ouder geeft bijvoorbeeld toestemming aan de elfjarige dochter voor een Facebookprofiel, de andere ouder is tegen. De ouder die tegen is, kan Facebook vragen om het profiel af te sluiten. Facebook zal dit doen omdat een account voor een kind onder 13 jaar zonder toestemming zijn voorwaarden schendt. Die ene ouder lost dit best wel op in samenspraak met de andere ouder en met het kind. Als laatste redmiddel is er de rechtbank.

JONGEREN

WAT MOET JE DOEN ALS JE TIENER ONLINE GEPEST WORDT?

Cyberpesten is meestal een voortzetting van offline pesten. Met dat verschil dat pestberichten op socialemediakanalen als een lopend vuurtje rondgaan en snel een veel ruimer publiek bereiken. Wanneer een kind online gepest wordt, wordt dus best snel ingegrepen.

Ouders die hun kind willen beschermen tegen cyberpesten, kiezen al wel eens voor een radicale oplossing: het gebruik van sociale media beperken of zelfs verbieden. Het online- en offlineleven van kinderen en jongeren is echter verstrengeld. Het gepeste kind kan het dichtgooien van die onlinekanalen als onrechtvaardig ervaren; de maatregel kan dan zijn doel voorbijschieten.

Beter is om het kind **online weerbaar te maken**, ook tegen pesters. Het belangrijkste beschermingsmechanisme voor kinderen is de **goede relatie met hun ouders**. Zij kunnen hun kind troosten, ondersteunen en samen een aanpak uitwerken om het pesten te bestrijden.

Ook als je geen techie bent, verdiep je je best in een aantal functionaliteiten: je kan de **privacyinstellingen verscherpen**, zodat pesters

geen bericht kunnen posten zonder goedkeuring; de pester blokkeren; de pestberichten, via de meldknop, signaleren aan het socialemediakanaal. Met schermafdrukken heb je **bewijzen** van het pestgedrag. Al zullen kinderen dergelijke berichten uit schaamte vaak snel verwijderen.

Socialemediabedrijven reageren echter niet altijd op de **vraag om dergelijke berichten of pagina's te verwijderen**. Ze doen dat alleen als het bericht hun gedragscode schendt. Om te weten wat je dan best doet in jouw geval, kan je de Click Safe Hulplijn voor Veilig internet van Child Focus contacteren **(www.clicksafe.be)** of het Vlaams Kinderrechtencommissariaat **(www.kinderrechtencommissariaat.be).**

Cyberpesten stop je op dezelfde manier als offline pesten. In de meeste gevallen zitten de cyberpesters bij het kind op school. **De school kan dus een bondgenoot zijn.**

Een valkuil waar ouders niet in mogen trappen, is het heft in eigen handen nemen en zelf filmpjes van de pesterijen online plaatsen om de dader te schande te maken. Want dan delen ze persoonsgegevens van minderjarigen zonder toestemming en kunnen deze filmpjes ook later hun eigen kinderen blijven achtervolgen.

Bij zeer ernstige pesterijen, bijvoorbeeld fysiek geweld of bedreigingen, kunnen ouders juridische stappen overwegen. Als het tot een strafklacht komt, kan justitie een maatregel opleggen aan de minderjarige dader en gelden de gebruikelijke regels van de ouderlijke verantwoordelijkheid.

Op **www.medianest.be** en **www.mediawijs.be** vinden kinderen & tieners, ouders en professionals tips en stappenplannen tegen cyberpesten.

CHECKLIST CYBERPESTEN

- Zet samen de privacyinstellingen op scherp en blokkeer de pester(s).
- Signaleer de pester, via de meldknop, aan het sociale netwerk.
- Neem schermafdrukken als bewijsmateriaal.
- Betrek de school.
- Dien bij zeer ernstige en aanhoudende pesterijen eventueel klacht in.
- Plaats niet zelf filmpjes van de pesters online.

HOE SCHADELIJKE OF KWETSENDE BEELDEN OF BERICHTEN VERWIJDEREN?

Bij een kwetsende of te revelerende foto of gemeen filmpje over een jongere is de eerste reflex: dit moet er meteen af. Je kan socialemediabedrijven vragen om kwetsend materiaal te verwijderen via de meldknop. Bij ernstige situaties gaan die meestal op dit verzoek in, maar een antwoord kan even op zich laten wachten.

De snelste weg is degene die het bericht of het beeldmateriaal plaatste, te vragen om dit te verwijderen, en/of diens ouders aan te spreken. Als dat niet lukt en als sociale netwerken niet reageren, kunnen ouders of jongeren zelf aankloppen bij Child Focus. Ook de school kan bemiddelen.

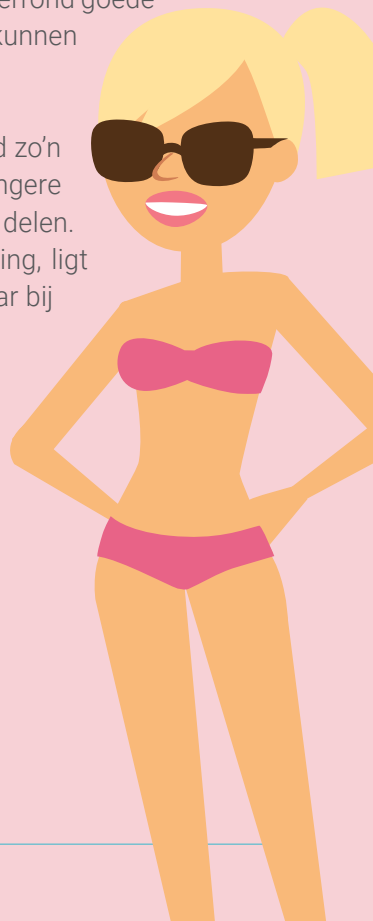
Ze kunnen ook een klacht indienen bij de Gegevensbeschermingsautoriteit of bij de politie. Maar als het doel is om het materiaal te verwijderen, gaat dit sneller via Child Focus, dat een directe lijn heeft met sociale netwerken.

Een klacht indienen is zinvol als je geen gehoor vindt bij de andere partijen, als de dader weigert het materiaal te verwijderen of als er een gevaar is voor het kind, bijvoorbeeld bij zeer expliciete beelden. Child Focus bekijkt samen met de ouders en eventueel de politie of de beelden verder verspreid zijn en of het kind begeleiding nodig heeft.

SEXTING: ONSCHULDIG EXPERIMENT OF GLAD IJS?

Jongeren experimenteren. Ze verkennen hun lichaam en zijn nieuwsgierig naar dat van anderen. In dit digitale tijdperk grijpen ze daarvoor ook naar technologie. Een op de tien jongeren zegt aan sexting te doen – waarbij ze seksueel getinte berichten of beelden van zichzelf sturen om te flirten, aandacht te trekken of als 'bewijs van liefde'. In meer dan driekwart van de gevallen is de bestemmeling een partner of een vriend(in).

Paniek is een slechte raadgever. Als uitkomt dat een jongere aan sexting doet, kan je dit aangrijpen om met het kind te praten over grenzen en risico's. Zodra de foto verstuurd is, hebben ze namelijk geen controle over wat ermee gebeurt. Sexten doen ze best alleen met iemand die ze kunnen vertrouwen en met wie ze hierrond goede afspraken hebben gemaakt. Als extra veiligheid kunnen ze hun gezicht onherkenbaar maken.



Bespreek ook wat ze kunnen doen als ze ongewild zo'n foto ontvangen. Wees alert voor signalen dat de jongere onder druk werd gezet om de foto's te maken of te delen. Als de foto toch gedeeld werd zonder toestemming, ligt de fout niet bij de jongere die de sext stuurde, maar bij degene die het vertrouwen beschaamde.

Als een jongere intieme beelden uitwisselt met zijn lief, met wederzijdse toestemming en voor eigen gebruik, is dat niet strafbaar. Dat wordt niet beschouwd als kinderporno. Als een jongere een foto doorstuurt zonder toestemming van de afgebeelde persoon, kan dat wel strafbaar zijn.

www.sexting.be

IS ONLINE PORNO KIJKEN STRAFBAAR VOOR JONGEREN?

Officieel is er een minimumleeftijd van 18 jaar om naar pornografie te kijken. Maar deze beelden zijn zo toegankelijk dat de leeftijdsgrens theoretisch is. Porno kijken is in de praktijk dus niet strafbaar voor jongeren. Dergelijke beelden doorsturen, bijvoorbeeld naar vrienden, is dat echter wel.

Het is belangrijk voor ouders om met hun kind te praten over online-porno. De confrontatie met bepaalde beelden kan jongeren in verwarring brengen en het zicht van onrealistische pornolichamen kan hen onzeker maken. Ouders en tieners moeten zich bewust zijn van alarmsignalen die aangeven dat ze te vaak kijken. Bij tekenen van overmatig gebruik of beginnende verslaving kan je terecht bij het CAW (**www.caw.be**) of bij een seksuoloog.

Meer informatie voor jongeren over onlinepornografie: **www.allesoverseks.be**, een website van Sensoa. Illegale beelden kan je melden aan Child Focus: **www.childfocus.be.**

VLOGGEN

Na school duiken kinderen en tieners elke dag massaal online om de vlogs (video weblogs) van hun YouTube-helden te bingen. Veel tieners experimenteren met een eigen vlogkanaal op YouTube of Musical.ly. Ouders die het voor hun kleine vlogger veilig willen houden, kunnen de mogelijkheid om te reageren onder de video's uitschakelen of negatieve commentaren filteren. Ze kunnen hun kind vragen om hun vlog te tonen voor ze het online zetten.

CHECKLIST ONLINEGAMING

- Gebruik nooit je echte naam, deel je adres of woonplaats niet in de chat en wees voorzichtig met foto's.
- Chat je in je game met tegenspelers? Praat dan alleen over de game en in de game.
- Let op de PEGI-score, om games te kiezen die aangepast zijn aan de leeftijd, of bekijk filmpjes met hints en tricks voor het spel online om een idee te krijgen van de inhoud.
- Game je te veel? Zolang je nog andere hobby's hebt, afspreekt met vrienden en je (huis)werk niet verwaarloost, is er niet meteen een reden om je zorgen te maken.
- Als dit verandert, als je boos, angstig of slechtgehumeurd bent als je niet kan gamen, moet je ingrijpen.
- Doe de test op de website van De Druglijn. Daar vind je ook adressen van hulpverleners: **www.druglijn.be**.

SNAPCHAT: SCREENSHOTS EN GEOLOCALISATIE

Snapchat, een chatapp waarmee je berichten, foto's en videoverhaaltjes kan sturen aan vrienden in je netwerk, is razend populair bij tieners. De berichten blijven 24 uur beschikbaar voor ontvangers en vernietigen zichzelf dan, tenzij je ze opslaat. De posts worden op de servers van Snapchat gewist na maximum 30 dagen. Snapchat is niet zonder gevaren voor wie denkt dat er geen spoor van de berichten blijft. Zo kan de ontvanger een screenshot nemen van je post en dat verspreiden. Snapchat geeft een melding wanneer iemand een screenshot neemt, maar die functie is te omzeilen en er zijn nog andere apps waarmee je screenshots kan nemen. Ouders waarschuwen hun tieners best ook voor de geolocalisatiefunctie, waardoor alle contacten kunnen zien waar je bent. Je kan je onzichtbaar maken of alleen zichtbaar maken voor dichte contacten.

SCHOOL

KAN DE SCHOOL FOTO'S VAN JE KIND ONLINE PLAATSEN?

Bij het begin van het schooljaar moeten ouders aangeven of ze akkoord gaan dat foto's en filmpjes van hun kind worden verspreid op de website of de Facebookpagina van de school. Idealiter kunnen ouders toestemming geven per toepassing – bijvoorbeeld niet voor Facebook, wel voor de (gesloten) fotopagina van de school – maar veel scholen vragen één algemene toelating.

Scholen springen soms nog onzorgvuldig om met het portretrecht. Zo zijn er scholen met een Facebookpagina per klas die 'openbaar' is – dus ook toegankelijk voor wie geen Facebookaccount heeft. Ze doen dat zodat alle ouders ze kunnen raadplegen, maar meteen is de pagina open voor iedereen. Of er zijn scholen die klasblogs op de schoolwebsite niet beveiligen met een wachtwoord. Ouders die niet graag hebben dat er beelden van hun kind worden verspreid, weigeren dan beter toestemming.

De verschillende onderwijsnetten hebben hun eigen richtlijnen voor scholen. Daarnaast heeft de Gegevensbeschermingsautoriteit een stappenplan dat scholen kan helpen om gegevens beter te beschermen. De brochure is te downloaden via de website van de GBA: **www.gegevensbeschermingsautoriteit.be**.

MAG EEN KIND OP SCHOOL DE SMARTPHONE GEBRUIKEN?

Het gebruik van de smartphone is vastgelegd in het schoolreglement. Sommige scholen verbieden de toestellen en verplichten leerlingen om hun smartphone op school een hele dag op te bergen. Andere tolereren het tokkelen tijdens de pauzes. Tijdens de lessen gaat de telefoon dan bijvoorbeeld in een bakje in de klas.
Scholen mogen persoonlijke spullen afnemen als leerlingen daarmee de lessen of de orde verstoren. Ook de smartphone. Ze mogen die

niet langer bijhouden dan nodig. In het schoolreglement staat meestal hoe lang dat is. Ze mogen ook niet de inhoud raadplegen zonder toestemming van de jongere en zijn ouders.

Op hogescholen en universiteiten is het gebruik van smartphones en laptops moeilijker in te perken. De verhalen over spieken via smartphone of smartwatch zijn legio. Elke onderwijsinstelling heeft in haar examenreglement regels tegen digitale fraude. Vele weren smartphone en smartwatch tijdens examens.

Meer informatie
voor kinderen en jongeren:
www.jongerengids.be
www.ikbeslis.be
www.clicksafe.be
www.medianest.be
www.veiligonline.be/online-relaties-en-seksualiteit

Meer informatie
voor volwassenen:
www.childfocus.be
www.ikbeslis.be
www.clicksafe.be
www.medianest.be

4. WERK

Mobiele technologie heeft het idee van kantoorwerk op zijn kop gezet. Werken hoeft niet meer op een vaste plek op een kantooreiland. Professionals tokkelen op smartphone, tablet en laptop op de trein, thuis, in de luchthaven, op café, in het park, bij klanten op verplaatsing. De werkvloer is overal.

Veel mensen gebruiken de laptop of de smartphone van het werk ook buiten de kantoorruimtes of buiten de kantooruren. Of ze gebruiken de computer op het werk om tijdens een koffiepauze of tijdens de lunch of gewoon tussendoor een restaurantje te boeken voor 's avonds of even te scrollen door hun Facebooktijdlijn.

Wat kan er en wat kan niet? Het is voor werkgevers en werknemers nog wat zoeken. De werkvloer is niet de woonkamer. Zodra je een arbeidscontract ondertekent, aanvaard je dat op het werk beperkingen gelden op jouw rechten. Dit betekent echter niet dat je daar of op je werk geen recht op privacy of vrije meningsuiting meer hebt.

We brengen namelijk veel tijd door op het werk. Volgens het Europees Hof voor de Rechten van de Mens is het daarom niet meer dan normaal dat we ook daar bijvoorbeeld een privébericht kunnen sturen, of online een lekker adresje zoeken. Door thuiswerken vervaagt bovendien de grens tussen werk en privé.

TRANSPARANTIE LOST VEEL OP

Veel conflicten zijn te vermijden met transparante bepalingen over internetgebruik in het arbeidsreglement of met een aparte internetpolicy die bepaalt waar, wanneer en hoe werknemers internet, e-mail en sociale media op de werkvloer mogen gebruiken. Werkgevers moeten die richtlijnen expliciet meedelen.

Als er duidelijke afspraken zijn, als er geen misbruik wordt gemaakt en als het werk gedaan wordt, zijn veel werkgevers bereid om enigszins soepel om te gaan met internetgebruik op de werkvloer, al zijn er ook bedrijven die de toegang blokkeren, bijvoorbeeld om de veiligheid van hun netwerk te garanderen.

Een werkgever mag, om de goede werking van het bedrijf te verzekeren, toezicht uitoefenen. Met de snelle technologische evolutie heeft hij daarvoor veel controlemogelijkheden ter beschikking. Wat hij wel of niet mag doen, wordt geregeld door verschillende wetten en collectieve arbeidsovereenkomsten.

Als het toch tot een conflict komt, kan de vertrouwenspersoon op het werk, de vakbond of de Gegevensbeschermingsautoriteit bemiddelen. Gezien de gezagsrelatie tussen werkgever en werknemer, doet de werknemer deze stap meestal pas na ontslag. De werknemer kan ook naar de arbeidsrechtbank gaan.

MAG EEN WERKGEVER EEN SOCIALEMEDIAPROFIEL VAN EEN KANDIDAAT-WERKNEMER UITPLUIZEN?

Sociale media bieden sollicitanten kansen om in het oog te lopen. Op LinkedIn kunnen ze vaardigheden, diploma's en werkervaring in de verf zetten. Op Instagram kunnen ze eigen werk tonen. Ze kunnen zichzelf op Twitter of Facebook profileren met publieke posts die duidelijk maken wat ze boeit en wie ze zijn.

Socialemediakanalen kunnen sollicitanten net dat beetje voor geven op concurrenten die alleen een motivatiebrief en een cv hebben gestuurd. Rekruteerders schuimen ook zelf het internet af om interessante informatie over sollicitanten te vinden.

Als sollicitant heb je de plicht om je mogelijke werkgever tijdens de sollicitatie op de hoogte te brengen van alle informatie die hij nodig heeft om over jouw kandidatuur te beslissen. Als de informatie niet

relevant is voor de betrekking, mag je die privé houden.

Werkgevers willen zoveel mogelijk weten. Ze googelen kandidaat-sollicitanten en nemen een kijkje op hun socialemediaprofielen. Staat die sollicitant vaak op foto's waar de drank rijkelijk vloeit? Liket hij bedenkelijke meningen? Als dit profiel publiek is, kan een sollicitant weinig doen aan een werkgever die online gaat kijken.

Een dossier aanleggen, online of op papier, met gegevens die de werkgever heeft gevonden, mag niet. Als ze dat willen doen, moeten werkgevers kunnen aantonen dat het nodig en relevant is en moeten ze de sollicitant op de hoogte hebben gebracht.

Sommige werkgevers lossen dit op door in de vacature op te nemen dat kandidaten gegoogeld worden. Wat zeker niet kan: 'gevoelige' informatie, zoals gegevens over etnische afkomst, seksuele geaardheid, geloofs- of politieke overtuiging, bijhouden.

Het gebeurt dat potentiële werkgevers bijvoorbeeld een vriendschapsverzoek sturen naar een sollicitant om toegang te krijgen tot diens profiel. Dat is onaanvaardbaar, maar de kandidaat durft misschien niet te weigeren om zijn kansen niet te hypothekeren. Een lapmiddel is om het verzoek te accepteren, maar de privacyinstellingen voor die 'vriend' op scherp te zetten.

CHECKLIST
SOLLICITEREN IN HET DIGITALE TIJDPERK

- Kam je socialemediaposts uit om eventueel 'bezwarend' materiaal te verwijderen.
- Stel privacyinstellingen streng in, zodat 'niet- vrienden' je posts niet kunnen zien.
- Zoek jezelf via zoekmachines om te weten wat over jou verschijnt.
- Heb je toch jeugdzonden waarvan onlinebewijs is? Je hebt het recht om te vragen om die informatie te wissen. Hoe dit moet, lees je op pagina 19.

KAN JE OP HET WERK SOCIALE MEDIA RAADPLEGEN?

Werkgevers zijn niet per se afkerig van het gebruik van sociale media op de werkvloer. Veel bedrijven zijn actief op LinkedIn, Facebook of Twitter en stimuleren hun medewerkers om als **ambassadeurs van het bedrijf** nieuwsjes of vacatures te verspreiden in hun eigen sociale netwerken.

Werkgevers willen wel vermijden dat er arbeidstijd verloren gaat; of dat het computernetwerk van het bedrijf schade wordt toegebracht door virussen of spam die onvoorzichtige surfers binnenhalen. Ook een selfie op kantoor of inchecken via sociale media voor een meeting met een potentiële klant kan een veiligheidsrisico inhouden voor het bedrijf.

De meeste ondernemingen hebben daarom bepalingen over onlinemediagebruik in het **arbeidsreglement** of een aparte internetpolicy over welk internetgedrag (niet) is toegelaten. De werkgever mag **grenzen opleggen** aan het privégebruik van telecommunicatie-

middelen die hij ter beschikking stelt. Hij mag het privégebruik van e-mail of internet beperken – bijvoorbeeld alleen tijdens de middagpauze of bepaalde websites niet. Hij mag het verbieden.

De werkgever heeft ook **controlerecht**. Als hij bij een werknemer misbruik vermoedt, moet hij een strikte procedure volgen om dit aan te tonen *(zie verder)*. Als een conflict tot voor de arbeidsrechtbank komt, zal die onder meer bekijken of er een internet policy was, of die duidelijk was meegedeeld, hoe de (ex-)werknemer heeft gesurft en hoe de werkgever dit te weten is gekomen.

HOE KAN EEN WERKGEVER ONLINECOMMUNICATIE OP HET WERK CONTROLEREN?

Een werkgever mag controleren of medewerkers niet (te veel) surfen of e-mailen voor privédoeleinden of facebooken tijdens de werkuren. Maar er zijn **strakke spelregels** voor hoe hij die controle moet aanpakken, met een evenwicht tussen zijn controlerecht en de privacy van de werknemer.

Redenen om te controleren zijn: wangedrag voorkomen, de belangen van de onderneming vrijwaren, de goede werking van de IT-systemen garanderen of checken of de onlinegedragscode wordt nageleefd. Deze controles moeten een concreet doel hebben en zo minimaal mogelijk de privacy schenden.

De werkgever mag **niet continu kijken wat werknemers online doen**. Controles moeten aangekondigd worden. Als een werkgever individueel misbruik wil aantonen, moet hij eerst een algemene controle doen, waarbij hij zoekt naar afwijkingen zoals onverklaarbaar hoog dataverbruik. Als hij vreemde dingen opmerkt, moet hij werknemers eerst informeren over de resultaten van deze controle. Als na een nieuwe controle problemen worden vastgesteld en er een redelijk vermoeden van misbruik is, mag de werkgever gegevens van de individuele werknemer controleren.

MAG JE EEN WERKGEVER BEKRITISEREN OP SOCIALE MEDIA?

Een werkgever heeft recht op **de loyauteit, het respect en de discretie van zijn werknemers**. Als werknemer mag je niets doen om de onderneming in gevaar te brengen of te beschadigen. Een werkgever moet erop kunnen rekenen dat je geen vertrouwelijke of schadelijke informatie verspreidt.

Werkgevers moeten wel **een zekere mate van kritiek kunnen aanvaarden.** Maar dat is geen vrijgeleide, en zeker niet als je je gal spuwt op een publiek forum, zodat de potentieel schadelijke gevolgen veel groter zijn. Er zijn geregeld ex-werknemers die voor de arbeidsrechter hun ontslag wegens een digitaal slippertje aanvechten.

> *Een kaderlid van een beursgenoteerd bedrijf postte bij herhaling commentaar op zijn werkgever. Hij deed dat ook vlak na de bekendmaking van de (slechte) halfjaarlijkse resultaten, voorzien van commentaar. Toen de personeelsdirecteur dit ontdekte, werd het kaderlid aan de deur gezet. Hij beriep zich voor de arbeidsrechtbank op zijn privacy, maar die veegde dat argument van tafel. De posts waren volgens de rechter publiek. Hij hield ook rekening met het feit dat het bedrijf beursgenoteerd was en de man kaderlid, en met de timing van de posts.*

Als je iets post wat kritisch is voor je werkgever, voor een collega of leidinggevende, of als je je ziek meldt om een snipperdagje te nemen en foto's van je dagtrip online zet op een sociaal netwerk, ben je nooit zeker dat dit niet gesignaleerd zal worden. In wel meer gevallen waarbij posts uitmondden in ontslag, waren het **collega's en onlinevrienden die de kat de bel aanbonden.**

Een keukenhulp werd om dringende redenen ontslagen nadat ze op Facebook een onderhoudsmedewerkster beledigd had. De vrouw voerde voor de arbeidsrechtbank aan dat de post niet als bewijs mocht worden gebruikt, omdat een collega die een 'vriend' was op Facebook, het bericht had doorgespeeld aan hun werkgever. Volgens de rechter echter ging het om een 'publieke' uiting.

Zware kritiek op de werkgever of het uiten van extremistische meningen op sociale media kan een reden zijn voor ontslag om dringende redenen. Als je dat ontslag aanvecht, kan een rechter oordelen dat de uitlatingen op sociale media een professionele fout zijn, omdat ze het **imago van het bedrijf schaden of ingaan tegen waar het bedrijf voor staat; of dat collega's of klanten er aanstoot aan kunnen nemen.**

Een boekhouder van een Luikse organisatie voor maatschappelijke integratie postte links naar video's van de Franse comedian Dieudonné, die in België veroordeeld is voor negationisme. Zijn werkgever had hem al gevraagd dit niet meer te doen en hij had schriftelijk beloofd zich daaraan te zullen houden. Toen hij nogmaals xenofobe berichten likete, werd hij aan de deur gezet. De boekhouder beriep zich op zijn vrijheid van meningsuiting. Het arbeidshof bevestigde het ontslag omdat volgens de rechter het imago van de vzw geschaad was.

Over het algemeen geldt: hoe publieker, hoe minder je je kan beroepen op je recht op privacy. Een rechter kan ook kijken of je eerder al intern je kritiek ventileerde maar bijvoorbeeld geen gehoor vond, hoe de kritiek geformuleerd werd – bijvoorbeeld met persoonlijke beledigingen – of je een leidinggevende bent en dus een voorbeeldfunctie hebt, of er veel collega's of klanten onder je onlinevrienden zijn.

Socialemedianetwerken zijn nu al meer ingeburgerd. De meeste mensen weten dat ze beter voorzichtig zijn. Toch is het nuttig om te herhalen: **privé op sociale media bestaat niet.** Je kan de privacy-instellingen zo instellen dat alleen onlinecontacten je berichten zien. Maar dan nog ben je nooit zeker dat jouw post niet verder verspreid wordt dan jij bedoeld had. Als je niet wil dat iets jouw collega of werkgever ter ore komt, zet je het best niet online.

WAT KAN JE DOEN TEGEN ONLINEHAATBOODSCHAPPEN?

De vrijheid van meningsuiting is een grondrecht, maar dit recht is niet absoluut. **Uitspraken die aanzetten tot haat of die haat verspreiden of verdedigen, zijn strafbaar.** Het is niet altijd gemakkelijk om de grens te trekken tussen vrije meningsuiting en haatboodschappen. Ook kritische, verontrustende, schokkende en zelfs kwetsende meningen moeten geuit kunnen worden. Strafbaar ben je, wanneer je aanzet tot discriminatie, haat, geweld of segregatie tegen anderen in het openbaar, doelbewust en met een duidelijke reden; wanneer je denkbeelden verspreidt over rassenhaat of rassensuperioriteit; als je de genocide door het naziregime ontkent; als je jouw racistische beledigingen schriftelijk verwoordt – dus ook online. België heeft ook een antiseksismewet, die gebaren of handelingen waarbij iemand zwaar publiek geminacht wordt omwille van haar of zijn geslacht, bestraft.

Je kan:

- **aan de paginabeheerder of moderator vragen om het bericht weg te halen.**
- **haatdragende of discriminerende posts signaleren aan Facebook of Twitter.** Zij kunnen ze verwijderen na een melding van een gebruiker. Ze beslissen of ze het bericht offline halen of het profiel tijdelijk of definitief schorsen.
- **zelf reageren**. Je kan het gesprek aangaan met de poster, op een correcte en beleefde manier, en onwaarheden weerleggen met feiten, je ongenoegen of ontzetting tonen of positieve berichten posten als tegenstem.

Meer informatie over wat te doen bij haatboodschappen:
www.unia.be/nl/actiedomeinen/internet/hoe-ga-je-met-haatboodschappen-om

KAN DE WERKGEVER E-MAILS VAN ZIJN WERKNEMERS CHECKEN?

Voor e-mails gelden dezelfde spelregels als voor andere online-gegevens. Als de **bedrijfspolicy** vermeldt dat je de mailbox op het werk niet mag gebruiken voor privéberichten, ga je in de fout als je dat toch doet. De werkgever heeft dus het **recht om toezicht te houden op de e-mails voor professionele doeleinden.**

Een werkgever mag **niet de inhoud van een persoonlijke mailbox bekijken**. Hij kan wel niet-gepersonaliseerde mailboxen als info@, verbonden aan een functie, inkijken. Bij ziekte moet een werkgever ook kunnen controleren of er in jouw mailbox documenten of berichten zitten die behandeld moeten worden.

Maar wat als je de mailbox van het werk ook mag gebruiken om – in beperkte mate – privéberichten te versturen? De werkgever heeft geen vrijgeleide voor een permanente en onvoorwaardelijke controle op e-mails, al helt de weegschaal eerder over naar de werkgever dan naar de werknemer.

De Gegevensbeschermingsautoriteit raadt daarom aan om een **dubbele mailbox** te gebruiken: een voor professionele berichten en een voor privécommunicatie. Sommige werkgevers vragen hun medewerkers om **privémails in een aparte map te bewaren** als er geen aparte mailboxen zijn. De meeste mensen hebben nu ook een **smartphone**, zodat ze hun privéberichten kunnen controleren op hun eigen toestel.

4. GEZONDHEID

Onlinetoepassingen zorgen voor een revolutie in de gezondheidszorg. Via onlineplatformen tussen zorgverleners kunnen patiënten beter worden opgevolgd. Dankzij medische mobiele apps hoeven patiënten met bijvoorbeeld hartritmestoornissen niet langer voor elke flauwte naar de spoeddienst of kunnen diabetici hun bloedsuiker meten via een sensor in hun smartphone. Lifestyleapps helpen beter te slapen of meer te bewegen. Maar het is ook opletten. Want gegevens over je gezondheid wil je niet in de verkeerde handen zien vallen.

MEDISCHE GEGEVENS = GEVOELIGE GEGEVENS

Als jouw medische gegevens via onlineplatformen gedeeld worden, hebben zorgverleners meteen een overzicht van jouw gezondheid. Ze weten voor welke ziekten je behandeld wordt, welke onderzoeken gebeurd zijn, welke geneesmiddelen je neemt. Handig voor een huisarts van wacht of een spoeddienst.

Jouw medische gegevens zijn echter zeer gevoelige gegevens. De registratie en het gebruik ervan zijn strikt geregeld. Jij moet toestemming geven vooraleer deze gegevens verzameld, geregistreerd of meegedeeld mogen worden. De uitwisseling ervan moet streng beveiligd zijn.

JOUW ONLINE MEDISCHE GEGEVENS BEHEREN

De federale overheid garandeert dat jouw online medische gegevens veilig zijn. Ze zorgt ervoor dat alleen de juiste personen toegang kunnen vragen en krijgen tot jouw medische informatie en dat de informatie alleen leesbaar is voor wie die toestemming heeft.

Als patiënt moet je jouw **geïnformeerde toestemming** geven voor het delen van je online medische gegevens. Dit kan je doen via je huisarts, apotheker of ziekenhuis. Je kan dat ook zelf online regelen via het federale portaal www.mijngezondheid.belgie.be of via de Patient Health Viewer (Vlaanderen).

Je kan die toestemming **op elk moment intrekken**. Je kan bepaalde artsen toevoegen aan de lijst van zorgverleners die toegang hebben tot jouw medische gegevens. Je kan de toestemming voor een specifieke arts, bijvoorbeeld na een onaangename ervaring, intrekken.

Via **www.mijngezondheid.belgie.be** kan je ook te weten komen waar gezondheidsgegevens over jou bekend zijn en in veel gevallen kan je die ook online raadplegen. Je kan ook je therapeutische relaties (de artsen die jou behandelen) beheren en bijvoorbeeld zorgverleners de toegang weigeren tot bepaalde documenten. Het wordt ook mogelijk om via dit portaal te zien wie jouw gegevens heeft geraadpleegd.

De federale overheid ondersteunt **regionale platformen van eerstelijnsgezondheids- of welzijnswerkers**: Vitalink (Vlaanderen), BruSafe (Brussel) en Intermed (Wallonië). Zij slaan medische gegevens op. Ook hier hebben alleen zorgverleners met jouw toestemming toegang tot die informatie.

Met vragen hierover kan je terecht bij je ziekenfonds.

KAN JE GEZONDHEIDSAPPS VEILIG GEBRUIKEN?

MEDISCHE APPS

Stel dat je last hebt van hartritmestoornissen. Elke flauwte kan een alarmsignaal zijn. Je wil graag snel zekerheid: vals alarm of niet? Een bezoekje aan de spoeddienst bracht tot voor kort het snelst uitsluitsel. Nu zijn er medische apps die met één vingertop op je smartphone je hartritme meten, detecteren of alles normaal is, en de gegevens doorsturen naar de behandelende arts. Die kan reageren als dat nodig is.

Deze apps kunnen het leven van een patiënt radicaal veranderen. Ze kunnen behandelingen doelgerichter en efficiënter maken. Met deze apps kunnen artsen de toestand van hun patiënten vanop afstand op de voet volgen en sneller ingrijpen wanneer dat nodig is zodat eventuele gevolgen minder erg zijn. Overbodige doktersafspraken kunnen vermeden worden. De patiënt krijgt er gemoedsrust bovenop.

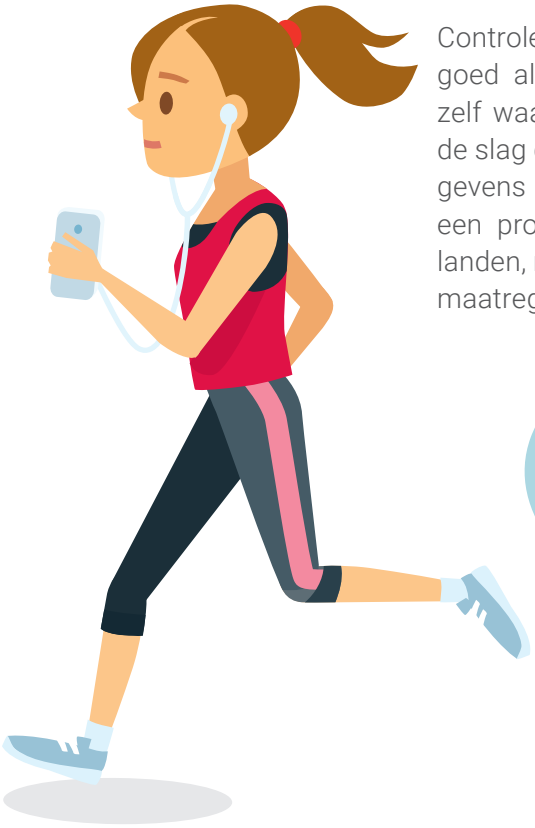
De federale overheid werkt aan een evaluatiemodel dat moet beoordelen of bepaalde apps in aanmerking komen om door een zorgverlener geadviseerd/voorgeschreven te worden en of ze al dan niet in aanmerking komen voor terugbetaling door de overheid via het ziekenfonds – steeds in het kader van een ruimere medische behandeling. De apps zullen onder andere moeten aantonen dat ze veilig zijn, dat ze de privacy van de patiënt strikt beschermen en dat ze een meerwaarde hebben voor de gezondheid.

LIFESTYLEAPPS

In appwinkels zijn daarnaast honderden lifestyleapps te vinden die beloven je mentaal en fysiek fitter te helpen worden. Vele zijn handig en nuttig. Ze kunnen je motiveren bij het sporten of diëten, helpen beter te slapen of je medicatie op tijd in te nemen.

Deze apps verzamelen ook zeer persoonlijke gegevens: je hartslag, je bloeddruk, je bewegingspatroon, je gewicht, je eetpatroon, je locatie. Gevoelige gegevens, die de privacywet extra beschermt, en die mensen soms bijna zonder nadenken toevertrouwen aan hun digitale gezondheidscoach.

Deze digitale coaches hebben commerciële bedoelingen. Ze hebben geen medisch beroepsgeheim. De apps zijn niet altijd wetenschappelijk of medisch onderbouwd. Onderzoek toont dat veel gezondheidsapps niet veilig omspringen met de gegevens van hun gebruikers en het niet altijd nauw nemen met de privacy. Gegevens worden doorgespeeld aan derden zonder dat de gebruiker op de hoogte is.



Controle op deze lifestyleapps is zo goed als onbestaande. Je moet dus zelf waakzaam zijn. Als je ermee aan de slag gaat, en zeker wil zijn dat je gegevens niet bij een verzekeraar of bij een producent in dieetproducten belanden, neem je best enkele voorzorgsmaatregelen.

CHECKLIST APPS
zie pagina 15

5. NA DE DOOD

We hebben allemaal een heel leven online. Tientallen wachtwoorden van rekeningen, accounts op sociale media, e-mailaccounts, een onlinemuziekbib of -boekenbib. Ons profiel op sociale media is een spiegel van ons leven, met herinneringen en notities van elke dag.

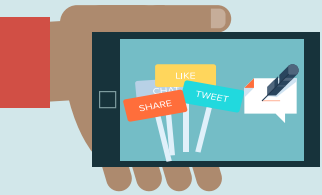
Wat gebeurt er met dat digitale leven nadat je je laatste adem hebt uitgeblazen? Steeds vaker denken mensen niet alleen na over wat ze met hun geld en goederen willen doen en wat ze willen voor hun uitvaart, maar ook over hoe het verder moet met al die digitale sporen die evenzeer een stuk van hun leven vertellen.

DIGITALE NALATENSCHAP: WELKE SPOREN LAAT JE NA?

Fragmenten van ons leven die we vroeger in huis bewaarden – dagboeken, brieven, fotoalbums, adresboekjes, boeken-, platen- of cd-collecties, rekeninguittreksels – zitten nu bij velen van ons online. We maken voortdurend digitale gegevens aan online en offline op onze computer.

Alles samen is dit jouw digitaal persoonlijk product (DPP). Als je overlijdt, wordt dit jouw digitale nalatenschap. Op dit digitaal persoonlijk product kunnen verschillende soorten rechten rusten: extrapatrimoniale rechten, vermogensrechten, persoonlijkheidsrechten, auteursrechten.

JE DIGITAAL PERSOONLIJK PRODUCT BESTAAT UIT VIJF SOORTEN DATA:



1. **documenten die je offline op computer of laptop hebt opgemaakt**
2. **inhoud online en via sociale media die je zelf hebt gecreëerd**, inclusief data in de cloud; je domeinnaamrechten en contracten met reclamebedrijven als je een blog hebt; muziek, presentaties, video, blogs, microblogs of bijdragen op een wiki (een website waaraan iedereen wijzigingen kan aanbrengen, zoals Wikipedia);
3. **communicatie**, bijvoorbeeld e-mail met onlineadresboek en -contactenlijst, internettelefonie met onlineadresboek en -contactenlijst of chat met een contactenlijst;
4. **elektronische handel en transacties, zoals e-financiën:** e-banking, e-verzekeringen, e-betalingen met afrekeningen en tegoeden of facturen van je telecomprovider of elektriciteitsleverancier, aandelen of effectendossiers die uitsluitend online consulteerbaar zijn of betaalmiddelen die exclusief online bestaan zoals bitcoins; e-government zoals Tax-on-web; onlineshopping, online boeken van reizen en transport, wat vaak gepaard gaat met een loyality-systeem;
5. **online lezen** via e-books, **onlinegaming** waarin (soms indirect) een virtueel vermogen wordt opgebouwd, een goksite of pokerapplicatie waar je over tegoeden beschikt; **onlinemuziek** of legaal gedownloade films of tv-programma's.

*Het is handig om een **digitale vingerafdruk** op te maken – een overzicht van al deze digitale sporen – en die af en toe te actualiseren.*

WAT GEBEURT ER MET DIE DIGITALE ERFENIS NA JE DOOD?

Als je zelf niets hebt geregeld, en je geen digitale vingerafdruk hebt gemaakt, is het een lastige klus voor erfgenamen om alle digitale bestanddelen en accounts op te sporen. Nabestaanden weten niet welke onlineaccounts je gebruikte of ze hebben de wachtwoorden niet. Ofwel blijven deze gegevens dan gewoon voortbestaan, ofwel worden ze na een periode van inactiviteit vernietigd door de aanbieders van de e-diensten.

WAT GEBEURT ER MET JE SOCIALEMEDIAPAGINA NA JE DOOD? KAN JE DIE OPENHOUDEN?

Vele dienstaanbieders sluiten de account af zodra ze op de hoogte zijn van een overlijden of verwijderen accounts na een periode van inactiviteit. Dat is niet zo voor alle providers. Als je dan geen instructies hebt nagelaten, leef je verder als **'digitale zombie'** met felicitaties als je verjaart of verzoeken vanuit het graf.

Sommige socialemediabedrijven hebben een **'afwikkelings- en beheersmechanisme'**: je kan zelf bepalen hoe jouw account na je overlijden wordt beheerd.

FACEBOOK

Op Facebook hebben jij en je nabestaanden **drie opties:**

- nabestaanden kunnen de Facebookaccount laten **verwijderen**. Ze moeten bewijzen dat ze naaste familie zijn. Ze moeten een kopie van de overlijdensakte bezorgen. Facebook verwijdert dan de account, met alle foto's en posts.
- nabestaanden kunnen jouw pagina omvormen tot een **herdenkingspagina**. Je pagina wordt dan voorafgegaan met 'ter nagedachtenis'. De pagina blijft behouden zoals jij ze hebt nagelaten. Deze herdenkingsstatus kan door eender wie worden aangevraagd, maar die persoon moet wel jouw naam, sterfdatum en een onlineverwijzing naar je overlijden leveren. Aan een profiel met herdenkingsstatus kan niemand iets wijzigen.

- je kan zelf een **legacy contact** aanwijzen via jouw accountinstellingen. Die persoon krijgt na jouw overlijden toegang tot jouw account. Hij of zij kan dan bijvoorbeeld reageren op berichten of de profielfoto aanpassen. De pagina wordt zo een plek waar familie of vrienden elkaar kunnen vinden om herinneringen op te halen en jouw leven te herdenken. Jouw legacy contact moet ouder dan 18 jaar zijn om jouw account te kunnen beheren en zelf een Facebookaccount hebben. Deze contactpersoon kan ook gegevens zoals foto's en video's extern opslaan. Hij heeft echter geen toegang tot jouw privéberichten.

In het Help Centre van Facebook vind je meer informatie over het legacy contact.

GOOGLE

Google (Gmail en Google+, Blogger.com, Google Foto's) beschikt al langer over de Inactive Account Manager. Met deze inactiviteitsvoorkeuren kan je zelf bepalen wat er met je Google-account gebeurt wanneer je overlijdt. Je kan aangeven wanneer Google je account als inactief moet beschouwen en wat Google met je gegevens moet doen. Je kan je account delen met een vertrouwenspersoon die de afwikkeling kan doen (bijvoorbeeld nog bepaalde gegevens zoals mails of foto's downloaden) of Google vragen om je account te verwijderen.

Als je zelf op voorhand niets geregeld hebt, kunnen nabestaanden ook contact opnemen met Google. Ze moeten dan wel kunnen aantonen dat je overleden bent, dat ze familie van jou zijn en een verworven recht over de nalatenschap hebben.

Meer informatie onder Persoonlijke voorkeuren & Privacy bij Google.

TWITTER

Wanneer Twitter op de hoogte wordt gebracht van het overlijden van een gebruiker (met vermelding van de naam en contactgegevens van de verzoeker en zijn verwantschap met de overledene, de Twitter-naam van de overledene, en een officieel bericht van overlijden), zal het deze account afsluiten en/of de familie toelaten om de openbare tweets te downloaden.

YAHOO

Yahoo (inclusief Flickr en Tumblr) bewaakt de privacy van zijn gebruikers streng, ook als ze er niet meer zijn. Je account is niet overdraagbaar, en alle rechten op je Yahoo ID of de inhoud van je account vervallen na je dood. Zodra ze een kopie van de overlijdensakte ontvangen, wordt de account ingetrokken en de inhoud verwijderd.

Meer informatie in de algemene voorwaarden van Yahoo.

STOPT PRIVACY BIJ HET OVERLIJDEN?

De persoonlijkheidsrechten (het recht op privacy, het briefgeheim, de bescherming van afbeelding, het recht op eer en goede naam) doven in beginsel uit na je dood. Jouw erfgenamen mogen dus je mails of andere digitale correspondentie lezen, net zoals ze je brieven of dagboeken mogen lezen – ook als je dat misschien niet wil.

Providers houden echter ook rekening met de privacy van derden die bijvoorbeeld een mail verstuurd of ontvangen hebben. Wat heeft er voorrang? Het recht van jouw erfgenamen om bijvoorbeeld jouw mails te lezen, of van de afzender van die mail om zijn privacy niet geschonden te zien?

Een aantal e-dienstenaanbieders deactiveert daarom je account automatisch na een periode van inactiviteit. Andere aanbieders deactiveren je account of zetten ze om in gedenkmodus zodra ze op de hoogte zijn van je overlijden. Je kan voor deze aanbieders kiezen als je wil vermijden dat erfgenamen je berichten lezen.

Je kan ook een vertrouwenspersoon aanstellen als digitale testamentuitvoerder *(zie verder)*. Die persoon kan dan jouw e-mails sorteren of vernietigen.

KAN JE JE MUZIEKCOLLECTIE IN DE CLOUD IN EEN ERFENIS STEKEN?

Dat hangt af van wie de eigenaar is van – en dus de controle heeft over – de gegevens of de account. Zoals bij de klassieke nalatenschap kan je je muziekcollectie of je blogarchief alleen overdragen als jij zelf de eigenaar of de houder van deze digitale nalatenschap bent.

Bij *software as a service* (software die als onlinedienst wordt aangeboden, bijvoorbeeld de

muziekbib van iTunes) verkrijg je een gebruiksrecht, geen eigendomsrecht. In de algemene voorwaarden van blogs, digitale bibliotheken en muziekcollecties staat meestal dat het om een persoonlijk, exclusief, tijdelijk en niet-overdraagbaar gebruiksrecht gaat. iTunescollecties bijvoorbeeld kan je niet overdragen. Wel kan je een overzicht of afschrift van de lijst van de aangekochte muziek of boeken vragen. Dit kan voor een nabestaande emotioneel waardevol zijn.

De toegang tot een account is persoonlijk en niet-overdraagbaar. Misschien overweeg je je paswoorden door te geven aan je erfgenamen, zodat ze van je persoonlijke muziekbib kunnen genieten. Dan schenden ze de gebruiksvoorwaarden.

KAN JE HET TESTAMENT GEBRUIKEN VOOR JE DIGITALE NALATENSCHAP?

De **commerciële initiatieven** rond digitale nalatenschap springen als paddenstoelen uit de grond. Ze hebben één ding gemeen: jij moet een vertrouwenspersoon aanduiden om jouw laatste wensen te vervullen en te doen naleven.

Het voordeel van deze initiatieven is dat zij een forum bieden om alle digitale identiteiten en accounts samen af te wikkelen. Na jouw overlijden krijgen de personen die jij als vertrouwenspersoon hebt aangewezen een overzicht van jouw laatste wensen voor je digitale erfenis, en de toegangscodes om die af te handelen.

Maar je kan deze wensen, net als de wensen voor de rest van jouw vermogen, ook gewoon vastleggen in een testament. Een notaris kan je daarbij adviseren. Je kan dan een 'testamentuitvoerder' aanstellen die na jouw dood jouw digitale gegevens zal beheren. Hij of zij kan bijvoorbeeld documenten wissen van je computer of bepaalde onlinegegevens die na verloop van tijd automatisch gedeactiveerd worden, toch redden voor het nageslacht.

Je laat hem of haar een document na met alle paswoorden en digitale accounts, zodat hij jouw digitale erfenis kan afhandelen. Je kan hem ook in je verschillende onlineaccounts aanwijzen als digitale

testamentuitvoerder. In sommige gevallen is dat zelfs niet nodig. Facebook bijvoorbeeld aanvaardt dat de testamentuitvoerder ook legacy contact kan zijn, zonder dat hij de procedure moet volgen *(zie hoger)*.

WIE KAN DIGITALE TESTAMENTUITVOERDER ZIJN?

De digitale testamentuitvoerder moet in de eerste plaats een persoon zijn in wie je vertrouwen hebt. Vaak zal hij of zij namelijk vertrouwelijke documenten moeten behandelen of vernietigen. Hij moet soms persoonlijke documenten en foto's of digitale accounts, berichten of toegangscodes verdelen onder erfgenamen. Het is evident dat je iemand kiest die zijn weg kent online.

Ook al heb je alles opgelijst en de testamentuitvoerder aangesteld, dan kan het toch zijn dat deze geen toegang krijgt tot de accounts. In de meeste algemene voorwaarden wordt immers opgenomen dat de toegang tot de account strikt persoonlijk is. De provider kan dan de data vernietigen of bepaalde informatie geven (bijvoorbeeld laatste e-mail, blog of post) en dan beslissen om te vernietigen of te bewaren.

Met dank aan Hans Graux, Elke Boudry, Eva Lievens, Isabelle Marchand, Nel Broothaerts, Rika Ponnet, Elisabeth Adriaens en Yung Shin Van Der Sype voor het waardevolle advies en/of de aandachtige herlezing. Wij danken ook iedereen die de tijd genomen heeft voor interviews of research en die zo heeft bijgedragen aan de totstandkoming van deze brochure.

BIJKOMENDE BRONNEN

Sociale media. Actuele juridische aspecten. Peggy Valcke, Pieter Jan Valgaeren en Eva Lievens (eds.). Intersentia, 2013.

Privacywetgeving in de praktijk. Hans Graux en Jos Dumortier. UGA, 2009.

Privacy binnen de gezondheidssector: knelpunten door de ontwikkeling van nieuwe technologieën zoals mobile health. Sarah Gilson. Masterproef Faculteit Rechtsgeleerdheid Universiteit Gent, 2016-2017.

Sociale media tijdens en na de arbeidsrelatie: bespreking en rechtsvergelijkend onderzoek. Elisabeth Standaert. Masterproef Faculteit Rechtsgeleerdheid Universiteit Gent, 2015-2016.

CO2 NEUTRAL Printing Services

FSC www.fsc.org RECYCLED Papier gemaakt van gerecycled materiaal FSC® C015373

Deze publicatie werd klimaatneutraal geproduceerd en gedrukt op Circle Premium White Offset 100% FSC® gerecycled ongestreken papier. De productie van Circle Premium White Offset is gebaseerd op een concept van verregaande recycling. Dit houdt de impact op het milieu zo laag mogelijk en ondersteunt een groene en duurzame groei.

NOTITIES

COLOFON

MIJN LEVEN ONLINE
MOGELIJKHEDEN EN VALKUILEN

Cette publication est également disponible en français sous le titre: Internet & moi. Protection, limites, opportunités.

Een gezamenlijke uitgave van de
Koning Boudewijnstichting, Brederodestraat 21, 1000 Brussel
en de Federatie van het Notariaat, Bergstraat 30-32, 1000 Brussel

Auteur
Isa Van Dorsselaer, met de medewerking van Virginie De Potter

Coördinatie voor de Koning Boudewijnstichting
Dominique Allard & Brigitte Duvieusart

Coördinatie voor de Federatie van het Notariaat
Bart Azare & Sandra Ichertz

Grafisch concept
Welcome Back Victoria, victoria.be

Deze uitgave kan (gratis) geraadpleegd of gedownload worden van de website van de Koning Boudewijnstichting www.kbs-frb.be of van de website van de Federatie van het Notariaat www.notaris.be

Wettelijk depot D/2893/2018/32
Bestelnummer 3604
September 2018

Koning Boudewijnstichting

Samen werken aan een betere samenleving

NOTARIS.BE

Koning Boudewijnstichting
Brederodestraat 21, 1000 Brussel
info@kbs-frb.be
02-500 4 555

Federatie van het Notariaat (Fednot)
Bergstraat 30-32, 1000 Brussel
fednot@fednot.be
02-505 08 11