Richtlijnen Algemene Verordening Gegevensbescherming

1. Inleiding

Mensen staan niet zo vaak stil bij privacy. Als de buren niet zomaar binnen kunnen gluren, niemand meeleest over de schouder als je sms’t, Snapt of WhatsAppt en als de NSA niet elk telefoongesprek afluistert, denken veel mensen dat hun privacy goed is beschermd.

Dat is echter niet altijd zo. Alledaagse programma’s, sites en apps weten veel meer over mensen dan de gemiddelde NSA-medewerker. Hun winst komt daar immers van: Facebook verkoopt gegevens en voorkeuren aan reclamebureaus, zodat men gerichte reclame kan krijgen. Google registreert zoektermen, zodat YouTube (eigendom van Google) gerichte spotjes kan tonen, wat opnieuw inkomsten garandeert. Whatsapp, Tinder, Google Maps en Pokémon GO! verzamelen allemaal in meer of mindere mate gegevens, weliswaar om hun dienstverlening te verbeteren, maar men heeft ze toch maar gegeven.

Op zich kan men denken dat dit geen probleem is: programma’s lopen vlotter, reclames zijn interessanter en een spam-mail meer of minder maakt niet zoveel uit. Toch verstuurt iedereen, of men het nu weet of niet, nu en dan heel gevoelige informatie online. Denk maar aan creditcardgegevens bij een bestelling bij Bol.com, of medische gegevens bij het invullen van een online verzekeringsformulier. Dat uw brievenbus propvol reclame zit, is geen probleem. Dat de gemiddelde crimineel in Zuid-Amerika met uw creditcardgegevens uitgaven kan doen, kan voor velen een ramp zijn.

Vandaar dat de Europese Unie in 2016 een nieuwe verordening heeft uitgevaardigd om privacy en gegevensverwerking beter te beschermen. Deze verordening treedt op 25 mei 2018 in werking, wat inhoudt dat enkele zaken zullen veranderen. Deze verordening werkt immers onmiddellijk, het Belgisch of Vlaams parlement moeten zelf niet meer optreden, dus de bestaande regels uit 1992 worden, voor zover ze de nieuwe Algemene Verordening Gegevensbescherming (AVG) tegenspreken, geschrapt.

1. Veranderingen

Verandert er heel veel aan de privacyregelgeving? Op zich niet heel veel. Vroeger golden ook de principes dat niet alles zomaar aan iedereen doorgegeven mocht worden. Alleen stond daar vroeger geen boete op (of lag die boete veel lager), waardoor die verplichtingen dode letter bleven. Daarnaast is de AVG ook strenger: men spreekt veel sneller van een “persoonsgegeven” en van een “verwerking” dan voorheen.

Vallen vzw’s daar ook onder? In principe wel. Alle rechtspersonen die “niet-incidentele verwerkingen uitvoeren”, vallen onder de verordening. Dit betekent dat die geldt voor vzw’s die op regelmatige basis gegevens verwerken. Werkt u met een klantenbestand, een loonlijst of ledenadministratie, dan verwerkt u op regelmatige basis en valt u onder de verordening.

Wat voor uw vzw vooral van belang zal zijn, zijn de nieuwe informatieverplichtingen, de nieuwe regels rond toestemming, het dataregister, verwerkingsovereenkomsten en de procedure in geval van datalekken. Deze laatste zal in een apart luik behandeld worden.

* 1. Definities
* Wat zijn nu juist “persoonsgegevens” of “verwerkingen”?

Een *persoonsgegeven* is elk gegeven of combinatie van gegevens waarmee men iemand persoonlijk kan identificeren. Dit moet wel specifiek op 1 persoon slaan.

*Vb.: Iemand die een kaartje krijgt met daarop de naam “Donald Trump”, weet die persoon niet per se over wie het gaat. Er kunnen immers meerdere Donald Trumps in de wereld zijn. Als dat kaartje echter “Donald Trump, Witte Huis, Washington D.C.” vermeldt, is dit wel een persoonsgegeven, omdat de persoon hierin identificeerbaar is.*

*Vb.: Iemand die de naam van Romelu Lukaku op zich verwerkt, is niet bezig met een persoonsgegeven. Er zijn kunnen immers meerdere Romelu Lukaku’s op de wereld zijn. Indien diezelfde persoon echter de naam van Romelu Lukaku verwerkt in dienst is van de Rode Duivels, is het in die context wel duidelijk over welke “Romelu Lukaku” gaat, dus is dit wel een persoonsgegeven.*

Het is dus duidelijk dat, binnen de context van uw vzw, de meeste gegevens die u verwerkt, net omwille van de specifieke context, persoonsgegevens zullen zijn.

* Wanneer “verwerkt” u nu juist die persoonsgegevens? Dit houdt ongeveer alles in. Zowel het verzamelen, delen, doorgeven, analyseren, gebruiken, opslaan of onderzoeken van die gegevens is een verwerking, voor zover dit op systematische en professionele wijze gebeurt.

*Vb.: Als je een naam op een papiertje schrijft voor privégebruik, is dat geen verwerking. Schrijf je die naam op een papiertje om te gebruiken in het kader van uw vzw, is dat wel een verwerking.*

* 1. Informatieverplichting

Waar privacyregels vroeger goed verborgen zaten ergens middenin de “Algemene Voorwaarden” en waar niemand dus ooit de moeite deed om die te lezen, moet in geval van verwerking van persoonsgegevens de privacyverklaring duidelijk, begrijpelijk en expliciet worden meegedeeld.

Wat betekent dit concreet? Telkens u gegevens verzamelt van mensen, hetzij bij de inschrijving als lid, hetzij bij deelname aan een activiteit of wedstrijd, hetzij in het kader van direct marketing, u een privacyverklaring zal moeten voorzien. Deze verklaring is een standaarddocument dat reeds ter beschikking staat van S-Sport // Recreas vzw. U kan het als voorbeeld in bijlage vinden, verder aanvullen volgens uw behoeftes en dan plaatsen op uw website.

Hoe gaat dit dan in zijn werk? Als de gegevensverzameling schriftelijk gebeurt (vb. bij het invullen van een contract, formulier, lijst), moet daar een “disclaimer” bijgevoegd worden. Deze mag niet in kleine lettertjes vol met juridische termen zijn, maar moet in een leesbaar lettertype en een leesbare taal zijn. Als de gegevensverzameling online gebeurt (vb. onlineformulieren), moet een pop-up venster (of dergelijke) verschijnen met daarop deze verklaring.

Deze disclaimer is een kort tekstje met de belangrijkste gegevens (welke persoonsgegevens worden opgevraagd, waarom en voor wie en welke rechten de betrokkenen hebben), en dat uw vzw privacy hoog in het vaandel heeft staan. Daarna kunt u verwijzen naar de volledige verklaring op de website. Wij kunnen de nodige disclaimers voorzien indien u die niet ter beschikking heeft.

U kunt de mensen echter niet dwingen om uw disclaimers en verklaringen te lezen. Zolang u uw leden, klanten etc. voldoende mogelijkheden geeft om uw documenten te lezen, volstaat dit.

* 1. Toestemming

Vroeger volstond het om onderaan een contract, formulier of blad een korte zin toe te voegen in de trant van “ik geef hierbij toestemming voor het verwerken van mijn gegevens”. Veel mensen waren zich hier niet eens van bewust. In online formulieren stond ook vaak al vooraf aangekruist dat “ik akkoord ga met het verwerken van mijn persoonsgegevens”, of was het niet mogelijk om het formulier te vervolledigen zonder dat dit akkoord werd aangeklikt.

Ook dit is niet meer mogelijk. In de gevallen waar toestemming nodig is voor het verwerken van persoonsgegevens (indien de gegevens die u opvraagt niet noodzakelijk zijn voor het vervolledigen van een overeenkomst), moet die toestemming expliciet, duidelijk en geïnformeerd zijn.

Dit houdt 2 zaken in. Ten eerste is niet voor elke verwerking toestemming nodig. Zo is het opgeven van naam en adres bij een bestelling bij Bol.com een noodzakelijke verwerking van persoonsgegevens. Zonder naam en adres is het immers onmogelijk om te komen leveren. Leeftijd opvragen is echter niet noodzakelijk, daarvoor zou Bol.com wel toestemming moeten vragen (als ze dat zouden willen weten). Voor uw vzw is bijvoorbeeld geen toestemming vereist als u de naam, het adres en e-mailadres van nieuwe leden vraagt. Die gegevens zijn immers nodig om “de overeenkomst” (nl. het aansluiten van een nieuw lid) te volbrengen. Als u tegelijk ook de naam van hun grootouders zou vragen, is dit niet noodzakelijk en zal u daarvoor toestemming moeten vragen.

Ten tweede gelden voorwaarden voor die toestemming. Dit houdt in dat u het toestemmingsformulier zal moeten laten ondertekenen, waar duidelijk opstaat waarvoor de betrokkene toestemt. Dit formulier kan ter beschikking worden gesteld, maar moet natuurlijk aangepast worden naargelang de gegevens waarvoor u toestemming vraagt.

* 1. Dataregister

Om te verzekeren dat ondernemingen de regels van de AVG volgen, moet ieder land een controlerende autoriteit aanstellen. In België wordt dat een nieuwe taak voor de Privacycommissie. Die controle zal er komen in de vorm van het nalezen van het dataregister. Dit verplichte register is een overzicht van alle gegevens die worden verwerkt door een onderneming, wat het doel van de verwerking is, over wie die gaat, hoe lang de gegevens bewaard worden, hoe ze beveiligd worden, of ze al dan niet doorgegeven worden aan landen buiten de Europese Unie of de Europese Economische Ruimte en wie die gegevens ontvangt.

Als vzw zal u een eigen register moeten aanleggen, aangezien u een rechtspersoon bent. De Privacycommissie heeft een register voorzien, maar dit is zeer onhandig in het gebruik. U kan via ons een variant op dit register verkrijgen, dat heel wat bruikbaarder is.

* 1. Verwerkingsovereenkomst

Wanneer u samenwerkt met S-Sport // Recreas, zal de rolverdeling vaak als volgt verlopen:

* S-Sport // Recreas zal *verwerkingsverantwoordelijke* zijn. Dit is de rechtspersoon die het doel en de middelen van de verwerking aangeeft. Met andere woorden, dit is de entiteit die zegt welke gegevens verwerkt moeten worden, waarom dat moet en hoe dit moet gebeuren.
* Uw vzw zal de verwerker zijn. Dit is de rechtspersoon die in opdracht van de verwerkingsverantwoordelijke gegevens verwerkt. Met andere woorden, dit is de entiteit die de opdracht van de verantwoordelijke uitvoert.

Waarom is dit van belang? Zowel verwerkingsverantwoordelijke als verwerker hebben elk enkele verplichtingen wanneer zij gegevens verwerken. Op de niet-naleving van die verplichtingen kunnen zware boetes staan, dus is het belangrijk dat duidelijk wordt afgesproken wie wat mag doen.

S-Sport // Recreas doet beroep op uw diensten voor bepaalde verwerkingen, vb. het verkrijgen van gegevens, het doorsturen van gegevens voor het organiseren van activiteiten enz. U moet natuurlijk weten welke gegevens u al dan niet mag gebruiken en waarom dit gebeurt. Indien niet, is het heel goed mogelijk dat u, volledig te goeder trouw, meer gegevens opvraagt dan nodig en zo onnodig risico loopt.

Dit wordt verplicht opgelost via een verwerkersovereenkomst. Dit technisch-juridisch document is in feite een afspraak over het verwerken van gegevens en wordt bij het hoofdcontract gevoegd.

*Vb.: S-Sport // Recreas doet beroep op uw vzw om leden in te schrijven, of om een activiteit voor leden te organiseren. Daarvoor wordt een hoofdovereenkomst afgesloten (wie zijn de partijen, wat is de prijs enz.). Daarvoor moet u wel gegevens verwerken voor S-Sport // Recreas: zij geven de namen van hun leden door voor het organiseren van een activiteit, of namen en lidnummers van hun leden zodat u die kunt inschrijven. Voor die verwerking moet een contract worden opgesteld, waarin staat dat uw vzw enkel voor dit doel gegevens mag verwerken voor S-Sport // Recreas en welke gegevens dit juist zijn.*

Is dit een document bedoeld om uw vzw met hoge aansprakelijkheidskosten op te zadelen? Natuurlijk niet. Het is sowieso een verplichting, die tegelijk ook verwarring voorkomt. S-Sport // Recreas beschikt over een standaarddocument dat wij u gaan voorleggen. Dan kan natuurlijk onderhandeld worden over de precieze inhoud, nadat u het eens heeft gelezen.

1. Verplichtingen en verantwoordelijkheden

Als vzw heef u nog enkele andere verplichtingen. Die verplichtingen komen niet per se voort uit de AVG, maar vloeien in het algemeen voort uit het principe dat de verwerkingen zo veilig en discreet mogelijk moeten gebeuren:

* elke medewerker, zowel bezoldigd als vrijwilliger, van de afdeling moet een discretieplicht naleven. U kunt een voorbeeld van dergelijke discretieplicht achteraan dit document vinden, onder punt 9. Die kunt u dan bij vrijwilligersovereenkomsten, arbeidsovereenkomsten of het huishoudelijk reglement voegen, indien u deze wil gebruiken;
* indien u als vzw op uw beurt gebruik maakt van een derde (private persoon of onderneming) voor het verwerken van persoonsgegevens, moet u hier zelf voor een verwerkersovereenkomst afsluiten. Op die manier kan uw vzw haar aansprakelijkheid beperken en tegelijk controle uitoefenen op de activiteiten van de derde;
* elke medewerker moet ook deze discretieplicht vanzelfsprekend naleven. Dit betekent niet alleen dat de informatie/de gegevens waarover de medewerker beschikt, niet mondeling mogen worden doorgegeven, maar ook dat die medewerker deze gegevens niet verwerkt buiten de toegestane verwerkingen, met andere woorden het doel.

Als afdeling bent u verantwoordelijk voor het leveren van de informatie via de disclaimer. S-Sport // Recreas kan niet elke verwerking controleren, dus doet S-Sport // Recreas beroep op u om aan deze verplichtingen te voldoen.

1. Datalek

Werken met gegevens houdt onvermijdelijk het risico op datalekken in. Een datalek is niet alleen het spectaculaire hacken door cybercriminelen van gevoelige bankgegevens, maar kan er even goed bestaan uit het verliezen van een laptop of usb-stick met gegevens, uit het verkeerd versturen van een mail met gegevens, uit het meenemen naar huis van een dossier waar uw kinderen door het dossier bladeren.

Kort gezegd bestaat een datalek erin dat persoonsgegevens worden “ontvangen” (gelezen, geanalyseerd etc.) of kunnen worden ontvangen door een persoon of personen die hier niet toe bevoegd zijn, met andere woorden, door personen die niet betrokken zijn bij de verwerking of, in het slechtste geval, niet bij uw vzw zelf betrokken zijn. “Kunnen worden ontvangen” hoort hier ook bij, daar, in geval van verlies van een laptop versleuteld met een wachtwoord, het niet zeker is of iemand deze laptop vindt of kan openen, maar deze gegevens wel in gevaar zijn.

Deze lekken zijn quasi onvermijdelijk, hoe zorgvuldig iemand ook omspringt met persoonsgegevens. U dient wel, in geval een datalek optreedt, dit lek op te nemen in een eenvoudig Excel-bestandje, met daarbij mogelijke oplossingen om dergelijke lekken in de toekomst te vermijden. Als een lek ernstig is, d.w.z. gevaar voor de betrokkenen zelf, moet u dit lek aan de Privacycommissie melden, tot 72 uur na het ontdekken van het lek. In extreme gevallen, wanneer er acuut gevaar is voor de betrokkenen (m.a.w. dat ernstige financiële, lichamelijke of psychologische schade goed mogelijk is), moeten de betrokkenen ook ingelicht worden.

Dit is de theorie. Moet u voor elk mogelijk datalek de Privacycommissie opbellen? Natuurlijk niet. De vuistregel is nog steeds: gebruik uw gezond verstand. Als het waarschijnlijk is dat iemand die gegevens kan lezen, dan moet u het melden (vb. u verstuurt een lijst van gegevens naar een verkeerd e-mailadres). Is het zeer onwaarschijnlijk (vb. u neemt een dossier mee naar huis en uw kleinkinderen van 3 en 5 jaar oud bladeren erin), dan hoeft u dat niet te melden.

1. Rechten betrokkenen

Betrokkenen hebben ook rechten. Indien u over gegevens van personen beschikt, kunnen die personen onder andere vragen om:

* inzage te krijgen in die gegevens;
* te vragen de verwerking stop te zetten (indien die verwerking op toestemming is gebaseerd);
* toestemming in te trekken;
* hun gegevens te laten corrigeren;
* “vergeten te worden”, m.a.w. dat alle gegevens betreffende die persoon uit de databank worden gewist.

Deze rechten worden opgelijst in de privacyverklaring, waardoor de betrokkene deze rechten kent of zou moeten kennen.

Deze vraag moet normaal gezien schriftelijk aan de vzw worden gericht, die dan een maand de tijd heeft (soms 3 maand) om dit verzoek te beantwoorden. In slechts zeer uitzonderlijke gevallen zal uw vzw dit verzoek kunnen weigeren. Het is echter zeer onwaarschijnlijk dat u veel verzoeken zult ontvangen. Indien nodig, kan S-Sport // Recreas u advies en hulp verlenen wanneer dit nodig is.

1. Verhouding S-Sport // Recreas – vzw

S-Sport // Recreas doet beroep op uw vzw om haar te helpen bij haar activiteiten. Op die manier bent u, in verhouding tot S-Sport // Recreas, verwerker. Voor verwerkingen die u zelf uitvoert, uit eigen naam en met eigen doeleinden, blijft u zelf verwerkingsverantwoordelijke.

Vandaar dat S-Sport // Recreas u een verwerkersovereenkomst zal voorleggen, om te zorgen dat beide partijen zo veilig mogelijk zitten wat betreft aansprakelijkheid.

1. Wat verandert er concreet?

In feite verandert er niet zo veel. U moet vanaf nu een dataregister bijhouden, uw informatieverplichtingen zijn iets uitgebreider en u moet datalekken melden indien nodig. Vroeger konden betrokkenen ook al rechten uitoefenen, maar nu zijn die beter en duidelijker geformuleerd en staan er zwaardere sancties op.

Voor wat betreft uw samenwerking met S-Sport // Recreas verandert er heel weinig, behalve dat uw samenwerking door een extra contract, nl. de verwerkersovereenkomst, beheerst zal worden.

Om het even visueel voor te stellen:

|  |  |
| --- | --- |
| VROEGER | VANAF 25 MEI |
| Geen dataregister | Wel dataregister |
| Informatieverplichting | Informatieverplichting, maar beter |
| Geen antwoordplicht bij vragen | Antwoordplicht, binnen 1 maand |
| Geen meldplicht bij ernstige datalekken | Meldplicht, binnen 72 uur |
| Geen verwerkersovereenkomst met S-Sport // Recreas | Verwerkersovereenkomst met S-Sport // Recreas verplicht |

1. Contactpersonen

Indien u nog vragen heeft hierover, kunt u terecht bij:

* + Contactgegevens vzw

1. Discretieplicht

Elk lid van de afdeling verklaart zich aan de volgende bepalingen te houden bij het verwerken, opvragen of anderzijds behandelen van persoonsgegevens in opdracht van of in samenwerking met S-Sport // Recreas.

Het lid van de afdeling verbindt er zich hiermee toe:

* alles wat door haar/zijn werkzaamheden niet als “publieke” informatie of “publieke informatiesystemen” is toevertrouwd of wat als zodanig ter kennis is gekomen en alles waarvan redelijkerwijs aangenomen moet worden dat het andere dan als “publieke informatie” geclassificeerde informatie betreft, aan niemand buiten het kader van haar/zijn opdracht te verspreiden, reproduceren, zelf bijhouden of ter beschikking stellen aan derden;
* zich alleen toegang te verschaffen tot de gegevens die noodzakelijk zijn voor het uitvoeren van de haar/hem toevertrouwde opdracht, zich met andere woorden discreet en loyaal op te stellen bij het raadplegen van gegevens;
* de gegevens waarvan zij/hij kennis heeft genomen, alleen toe te vertrouwen aan anderen in de mate dat dit voor de uitvoering van haar/zijn opdracht noodzakelijk is en op voorwaarde dat de persoon aan wie deze gegevens kenbaar worden gemaakt bevoegd is er kennis van te nemen;
* de toegangscodes en/of wachtwoorden om zich toegang tot de gegevens te verschaffen niet kenbaar te maken;
* alle verbintenissen na te leven die zij/hij moet nakomen in overeenstemming met de Algemene Verordening Gegevensbescherming, zijnde *verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens*, indien persoonsgegevens betrokken zijn bij het uitvoeren van de haar/hem toevertrouwde opdracht;
* enkel, in het kader van de activiteiten in opdracht van of in samenwerking met S-Sport // Recreas, de gegevens op te vragen en/of te verwerken waar S-Sport // Recreas expliciete instructies over geeft. Deze instructies dienen ook opgevolgd te worden.

Deze vertrouwelijkheidsplicht blijft ook na beëindiging van het samenwerkingsverband tussen S-Sport // Recreas en het lid van de afdeling voortbestaan.

Het lid van de afdeling is zich ervan bewust dat (straf-)sancties kunnen worden opgelegd indien vertrouwelijke informatie wordt aangewend voor andere doeleinden dan voor de uitoefening van haar/zijn opdracht of ingeval van misbruik van deze vertrouwelijke informatie.