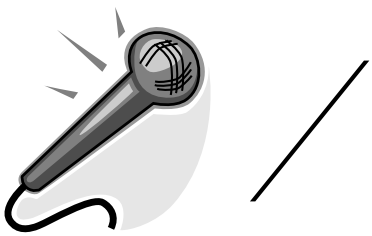
Hans Kuné /a.j.kune@rug.nl
Kristien Piersma / k.i.piersma@rug.nl

Foto's / Gerhard Lugard

Universiteit stelt privacytoezichthouder aan

De Algemene Verordening Gegevensbescherming staat voor de deur



Het staat vast. In mei volgend jaar wordt hij van kracht. De AVG, de Algemene Verordening Gegevensbescherming, oftewel de General Data Protection Regulation. Een Europese verordening, die in Nederland de Wet bescherming persoonsgegevens (Wbp) gaat vervangen. De verordening scherpt de bepalingen van de Wbp flink aan en . . . de boetes die in de AVG genoemd worden, zijn veel en veel hoger dan die van de Wbp. Kortom: werk aan de winkel.

Ook voor de RUG. Arjen Deenen weet daar alles van. Op 1 maart jl. is hij bij de RUG aangesteld als Functionaris Gegevensbescherming. Hij vertelt Pictogram wat de nieuwe wet zoal inhoudt en waar we in de komende periode op moeten letten en aan moeten werken.

Hogere boetes

Arjen is één van die zeldzame juristen, die niet alleen verstand heeft van wet- en regelgeving, maar ook van ICT. Hij heeft Nederlands Recht aan de RUG gestudeerd en hij heeft naast zijn studie een bedrijf voor webontwikkeling opge-

richt. ‘Dat bedrijf begon heel klein, maar het is in de loop van de tijd flink uitgegroeid. Ik vond het leuk om websites en applicaties te ontwerpen en er met technici over te praten hoe ze het beste gerealiseerd konden worden. Op die manier heb ik een goed inzicht gekregen in de mogelijkheden en beperkingen van ICT.

Op enig ogenblik heb ik het bedrijf verkocht en ben ik bij een klant van ons gaan werken, het advocatenkantoor Yspeert. Totdat ik deze vacature tegenkwam. Ik had en heb enorm veel zin in de werkzaamheden bij de RUG. Het is een klus waarin ik zowel mijn juridische kennis als mijn ICT-ervaring kan gebruiken. Op het ogenblik probeer ik met zoveel mogelijk mensen aan de RUG kennis te maken. Met ICT-mensen natuurlijk, maar ook met mensen die verantwoordelijk zijn voor administratieve procedures en met bestuurders.

Het belangrijkste is volgens mij dat iedereen zich ervan bewust wordt, dat we nog veel zorgvuldiger met persoonsgegevens moeten leren omgaan dan we al doen. Met persoonsgegevens is het altijd zo dat het enorm handig is om ze te hebben. Ze komen altijd van pas. Dat is onder de huidige wetgeving al niet toegestaan en de AVG is daar ook heel duidelijk over. Je moet precies weten voor welk doel je persoonsgegevens verzamelt en bewerkt. En je mag ze vervolgens ook alleen voor dat doel gebruiken. Dat is een van de principes van de AVG.’

Pictogram: En als je dat niet goed doet, volgen er dus hoge boetes?

Arjen: ‘Het is zeker zo, dat de boetes in de AVG veel hoger zijn dan in de WBP of in de andere nationale regelingen in Europa. De boetes kunnen nu tot in de honderdduizenden euro’s gaan lopen. Voor bedrijven als Facebook en Google, die geen publieke taak hebben, is dat zakgeld. Met de komst van de AVG kunnen de boetes, ook voor de RUG, in de miljoenen lopen. Dat is natuurlijk wel iets om even bij stil te staan.

Verantwoordelijkheid voor data

Maar ik heb liever niet dat mensen vanuit zo’n negatieve stimulans werken. Het is beter om vooraf goed naar je processen te kijken en er als het ware een eer in te stellen, dat die processen garanderen dat enkel persoonsgegevens worden verwerkt die noodzakelijk zijn voor het bereiken van het doel waarvoor ze verzameld zijn. Dat heet Privacy by Design.

Dus houd tijdens de ontwikkeling van je systemen rekening met de eisen die de wet stelt aan de privacybescherming, maar blijf vooral zelf nadenken, vraag jezelf af wat écht noodzakelijk is om te verwerken. De komst van de AVG moet zeker geen feestje van juristen worden.’

Pictogram: Geeft de AVG duidelijk aan wat onder privacy verstaan wordt?

Arjen: ‘Niet in die zin dat er een definitie gegeven wordt. Maar de AVG maakt heel duidelijk wat onder verantwoordelijkheid voor de data wordt verstaan. Die verantwoordelijkheid gaat veel verder dan tot nu toe gold. Voor alle verwerkingen van persoonsgegevens moet de organisatie aangeven met welk doel de data verwerkt worden en hoe ze verwerkt worden. Alle verwerkingen moeten in een register worden vastgelegd. Daaruit kan worden opgemaakt of een verwerking noodzakelijk is voor het behalen van het doel en of de verwerking op een veilige wijze gebeurt. Daarvoor is het nodig alle processen door te lichten, want het register is alleen op te stellen, als je die processen heel goed kent.

Het zal naar mijn idee veel werk met zich meebrengen om het register binnen de RUG op te stellen, maar daar staat tegenover dat er ook een efficiencyslag gemaakt kan worden. Als je meer inzicht hebt in je processen, merk je wellicht dat er soms dubbel werk verricht wordt, of dat procedures gestroomlijnd kunnen worden. Wat in deze context trouwens ook heel belangrijk is, is dat het niet alleen om de procedures gaat die zich binnen de muren van de RUG

‘Het moet geen feestje van juristen worden’

afspelen. De RUG is ook verantwoordelijk voor de verwerking van haar persoonsgegevens door derden, waar verwerkersovereenkomsten mee zijn afgesloten. Die contracten zullen ook tegen het licht gehouden moeten worden. ‘

Pictogram: Pff, complex allemaal hoor.

Arjen: ‘Ja , dat is misschien wel zo, maar beveiligingsmaatregelen kunnen gelukkig ook best simpel zijn. Een klein voorbeeldje: het windowsknopje op het toetsenbord. Als je dat samen met de L indrukt, heb je je computer gelockt. Dat weet lang niet iedereen. Ik zeg: zet er een taartje op. Of zoiets. Spreek in de afdeling af: als we een onbeheerde computer aantreffen die niet gelockt is: trakteren. Dat hebben we binnen de afdeling ABJZ al gedaan. Er is drie keer getrakteerd. En nu sluit iedereen zijn of haar computer af.’

Pictogram: Dat opstellen van het register en dat opsporen en doorlichten van al die contracten, dat wordt een giga-project.

Arjen: ‘Dat klopt. Vandaar dat er een echte projectorganisatie in de steigers gezet wordt. Hierbij is ook de security officer van de RUG, Matto Fransen, nauw betrokken. Er zal een projectleider komen en er zullen in alle faculteiten coördinatoren privacy en security worden aangewezen. Dat zullen mensen zijn die hun faculteit goed kennen. Die zullen gaan helpen met de opzet van het register. En tegelijk zal er beleid gemaakt worden: wat doen we wel, wat niet, waar liggen de prioriteiten?

Datalekken

Het project zal ook een privacy portal in de lucht brengen. Daarop vertellen we waar we precies mee bezig zijn, de beleidsstukken komen er natuurlijk op, we zullen voorbeelden van ‘best practices’ laten zien en mensen zullen er op kunnen vinden wat ze moeten doen als er sprake is van bijvoorbeeld een datalek. De wet is er heel duidelijk over, dat ieder datalek gemeld moet worden aan de AP, de Autoriteit Persoonsgegevens. Ook daar moeten mensen zich van bewust worden.

Kijk, met die boetes is het zo: je krijgt niet gelijk duizenden of honderdduizenden euro’s boete als er iets misgaat, maar als je niet aan kunt tonen dat je er alles aan doet om te voorkomen dat er iets misgaat of als blijkt dat je fouten verdoezelt, dan zal de Autoriteit ingrijpen. Mensen moeten dus goed weten wat een datalek is. Een laptop die kwijt is, gestolen of verloren: melden. Dus niet alleen een nieuwe kopen, maar ook: het datalek melden. En: laptops en andere gegevensdragers versleutelen.

Verder is een datalek ook het per ongeluk verwijderen van persoonsgegevens zonder en back-up te hebben. Denk aan de bewijzen van behaalde diploma’s van alumni. Een dergelijke verwijdering kan grote gevolgen hebben wanneer een alumnus zijn eigen diploma niet meer heeft.‘

Pictogram: Wie controleert dat eigenlijk, dat alles wel goed gaat?

Arjen: ‘Er worden in de gehele universiteit PIA’s uitgevoerd, Privacy Impact Assessments. Die worden onder de nieuwe verordening verplicht. Met een PIA doorlicht een individu of groep een systeem of proces. Je kijkt wat er aan persoonsgegevens wordt verwerkt en bekijkt of je met minder gegevens hetzelfde doel kan bereiken. Daarnaast stel je de risico’s vast en bepaal je welke technische en organisatorische maatregelen nodig zijn om de risico’s zoveel mogelijk te beperken.

En er zullen zeker ook audits gehouden gaan worden, processen worden dan getoetst aan de hand van bekende certificering en gemaakte afspraken.

Mijn rol zal steeds meer in de sfeer van het toezicht komen te liggen, terwijl ik momenteel ook hands-on werkzaamheden verricht. Vooreerst zullen we druk bezig zijn er voor te zorgen dat de RUG voor mei volgend jaar AVG-bestendig is. Dat is nu het belangrijkste.

Toewerken naar compliance met de AVG moet echter geen afvink-exercitie worden. Het zal integraal onderdeel uit moeten gaan maken van ons professionele gedrag’