Matto Fransen / m.j.fransen@rug.nl

Nieuwe privacyregels

Matto Fransen is de nieuwe security manager bij het CIT. Met deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen.

In de eerste twee maanden van dit jaar zijn in het kader van de wet meldplicht datalekken ongeveer zevenhonderd meldingen binnengekomen bij de Autoriteit Persoonsgegevens (AP), zo meldt een krant ons. Meldingen die bij de autoriteit binnenkomen hebben volgens het betreffende artikel vaak te maken met onversleutelde gegevens op externe datadragers, zoals USB-sticks en USB-schijven.

Per 1 januari dit jaar zijn de privacyregels strenger geworden met het van kracht worden van de wet meldplicht datalekken. Wie de nieuwe regels niet goed toepast, maakt kans op hoge boetes. Organisaties moeten zorgen voor passende technische en organisatorische maatregelen om datalekken van persoonsgegevens te voorkomen. De Autoriteit Persoonsgegevens kan boetes opleggen wanneer persoonsgegevens niet zorgvuldig zijn verwerkt, de beveiliging tekort schiet, het beheer van persoonsgegevens slecht is georganiseerd of gevoelige informatie over burgers is misbruikt.

Wat zijn persoonsgegevens?

Persoonsgegevens zijn al die gegevens die naar een natuurlijk persoon herleidbaar zijn of die directe of indirecte informatie over een persoon verschaffen. Een naam, personeelsnummer, geslacht, geboortedatum, Burgerservicenummer (BSN) en een telefoonnummer zijn hier voorbeelden van, maar dit kan ook gelden voor bijvoorbeeld een autokenteken, een netwerkadres. Audio- en video-opnamen van personen zijn ook persoonsgegevens.

De wet maakt onderscheid tussen persoonsgegevens en bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn onder andere gegevens over iemands ras, godsdienst of levensovertuiging, gezondheid, seksuele leven, of iemands lidmaatschap van een vakvereniging. Ook strafrechtelijke gegevens vallen onder bijzondere persoonsgegevens.

Omdat de verwerking van deze bijzondere persoonsgegevens kan zorgen voor een grote inbreuk op de privacy van betrokkenen gelden strenge regels en voorwaarden voor de verwerking er van. Bijvoorbeeld de verwerking van gegevens over iemands gezondheid is in principe uitsluitend toegestaan aan instellingen in de gezondheidszorg.

Up-to-date

Op verschillende plekken binnen de universiteit wordt met persoonsgegevens gewerkt, zoals gegevens over studenten en hun studieresultaten en gegevens over de medewerkers. Bij de universiteit werken ook veel mensen die niet in loondienst van de universiteit zijn, maar wel in diverse systemen geregistreerd zijn, bijvoorbeeld voor toegang tot het IT-netwerk

of toegang tot een of meer gebouwen van de universiteit. Daarnaast wordt in het onderzoek soms ook met persoonsgegevens gewerkt. Het kan zijn dat mensen vragenlijsten worden voorgelegd om in te vullen, of om opnames van interviews, et cetera.

Voor al deze gegevens geldt dat daarmee zorgvuldig moet worden omgegaan. De wet verlangt dat beveiliging van die gegevens conform de laatste stand van de techniek is. Verouderde besturingssystemen waar geen updates meer voor verschijnen, of besturingssystemen waar de laatste veiligheidspatches niet zijn aangebracht, zijn dus niet geschikt voor de opslag of verwerking van deze gegevens. Ook voor de softwarepakketten die op die systemen staan, geldt dat zij veilig en up-to-date moeten zijn. Maar techniek alléén is geen voldoende waarborg.

Het gaat er ook om, hoe de werkprocessen zijn georganiseerd en hoe men met deze gegevens omgaat. Het is verleidelijk om even een query op Peoplesoft te maken en die op een USB-stick op te slaan, om hiermee 's avonds thuis nog snel een rapportje voor het bestuur op te stellen.

Risico's inschatten

Wanneer het ons zelf betreft, zijn wij mensen snel geneigd om de risico's lager in te schatten. Bij andere mensen wordt ingebroken, maar bij ons niet, wij hebben immers die nieuwe tuinlamp. Andere mensen vergeten hun jas of tas in de trein, wij niet, dat is ons nog nooit overkomen omdat we daar goed op letten.

Wie gegevens op een USB-stick of op een USB-schijf zet, loopt altijd risico deze ergens te verliezen of te vergeten, of de tas of jas waarin deze zit wordt vergeten of verloren. Of de laptop, inclusief alle gegevens die daarop staan, wordt vergeten of gestolen. Daarom is het opslaan van persoonsgegevens (en andere gevoelige informatie) op deze informatiedragers geen goed idee, zeker niet wanneer daarbij geen sterke encryptie wordt toegepast.

Encryptie

Het is onverstandig om geen encryptie op de harde schijf van de laptop toe te passen. Ook wanneer er geen persoonsgegevens mee verwerkt worden, staat op een laptop vaak vertrouwelijke informatie. Denk alleen maar aan opgeslagen wachtwoorden in bijvoorbeeld de browser of de e-mailapplicatie, nog even afgezien van de opgeslagen documenten.

De beste oplossing is om bij ingebruikname van de laptop de harde schijf te laten encrypten. Later, achteraf, alsnog encryptie toepassen is ingewikkelder, omdat er dan al allerlei gegevens op de harde schijf staan. Het is echter niet onmogelijk. Wie nog geen encryptie op zijn laptop toepast, raden wij daarom van harte aan, dat alsnog te regelen.

Bewerkersovereenkomsten

In een aantal gevallen zijn wij niet de enige die met bepaalde persoonsgegevens werken. Bijvoorbeeld wanneer die gegevens worden gedeeld met anderen die ook aan het onderzoek meewerken. Ook is hier sprake van wanneer een derde partij de software of het systeem beheert waarop wij met persoonsgegevens werken. Wellicht dat die derde partij niets met die gegevens doet, maar de mogelijkheid om die in te zien, bestaat wel. Zodra een andere rechtspersoon bij de verwerking betrokken is, vereist de wet dat een zogenoemde bewerkersovereenkomst wordt opgesteld en ondertekend. In de bewerkersovereenkomst is vastgelegd wie welke verantwoordelijkheden heeft tijdens de samenwerking, maar ook daarna.

In zo'n overeenkomst kan bijvoorbeeld staan, wat na afloop van het project of van het contract moet gebeuren. Wie wist welke gegevens, en hoe wordt dit vastgelegd zodat dit achteraf nog aan te tonen is? Een bewerkersovereenkomst is een belangrijk document en kan het beste in overleg met de juristen van de RUG worden opgesteld.

Melding van een lek

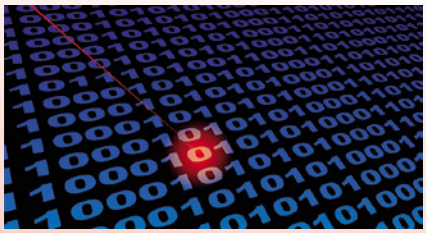
Mocht het onverhoopt toch gebeuren dat persoonsgegevens in handen van onbevoegden zijn gekomen, of de kans daarop is ontstaan, dan dient hiervan melding gemaakt te worden. In ieder geval dient de universiteit een register met deze incidenten bij te houden, en in een aantal situaties moet het incident gemeld worden bij de Autoriteit Persoonsgegevens of mogelijk zelfs bij betrokkenen. Deze melding bij de autoriteit dient binnen 72 uur plaats te vinden.

Om die reden heeft de universiteit een meldpunt ingericht. Bij een vermoeden dat er sprake is van een lek of onvoldoende beveiliging van persoonsgegevens, kan men dat bij dit meldpunt aangeven. Er vindt dan zo snel mogelijk nader onderzoek plaats.

Zorgvuldig omgaan

Wie met persoonsgegevens werkt, moet daar zorgvuldig mee omgaan. Technisch dient de omgeving op orde te zijn, met actuele software op een actueel besturingssysteem, waar alle updates zijn aangebracht. Ook de werkprocessen dienen op orde te zijn, waarbij de data alleen op het universiteitsnetwerk staat en niet op laptops, USB-sticks of USB-schijven. Maar dat hoeven wij u natuurlijk niet te vertellen, u heeft het allang op orde.

Meldpunt datalekken



Stel iemand vermoedt een datalek of heeft het idee dat de beveiliging of procedures rondom persoonsgegevens te kort zijn geschoten, wat kan die persoon dan het beste doen? Wat als een USB-stick of laptop is verloren? De universiteit heeft een speciaal meldpunt ingericht waar men dit kan melden. Stuur in dat geval een e-mail naar **cert@security.rug.nl** en beschrijf daarin kort de situatie. Vergeet ook niet contactgegevens op te nemen, zodat men snel contact kan opnemen.

Na een melding aan dit meldpunt wordt een protocol opgestart, waar verschillende personen bij betrokken zijn. Het kan zijn dat het noodzakelijk is, het incident bij de Autoriteit Persoonsgegevens of bij betrokkenen te melden. Die afweging is onderdeel van het protocol en binnen de RUG is vastgelegd wie een dergelijke melding doet. Het is zeker niet de bedoeling dat u daar zelf initiatief toe neemt.