

Redactioneel

In het vijfde nummer van 2021 van het *Tijdschrift voor Ondernemingsbestuur* wordt als overkoepelend thema aandacht besteed aan (de openbaarheid van) informatie en bescherming daarvan, bijvoorbeeld uit het oogpunt van privacy en veiligheid.

In de eerste bijdrage gaat *Marieke Vervoorn* in op de invloed van de Algemene Verordening Gegevensbescherming ('AVG') in het kader van de fusie- en overnamepraktijk. Zij stelt de vraag aan de orde of in het eerste deel van de transactiefase, bijvoorbeeld in het kader van een due diligenceonderzoek, persoonsgegevens door de verkoper of de doelwitvennootschap mogen worden verstrekt aan een geïnteresseerde, potentiële koper. *Vervoorn* is van mening dat alle gegevens en informatie die zien op de doelwitvennootschap zonder aanvullende voorwaarden verstrekt mogen worden, behalve als sprake is van persoonsgegevens. Alvorens dergelijke gegevens aan een geïnteresseerde, potentiële koper te verstrekken, moet worden onderzocht voor welk doel de persoonsgegevens worden verwerkt en of dat past bij een van de in de AVG genoemde grondslagen. Daarnaast, zo stelt *Vervoorn* aan de orde, is het van belang te onderzoeken of de doelwitvennootschap aan de door de AVG gestelde eisen voldoet. De boetes die door de Autoriteit Persoonsgegevens kunnen worden opgelegd zijn namelijk hoog. Bovendien kunnen aan niet-naleving van de AVG ook andere gevolgen zitten. Grosso modo: des te meer persoonsgegevens een vennootschap verwerkt, des te groter de risico's zijn, aldus *Vervoorn*.

In de tweede bijdrage bespreken redactielid *Eva Eijkelenboom*, *Bernold Nieuwesteeg* en *Rens Hoogerwaard* cyberveiligheid van Nederlandse beursgenoteerde vennootschappen en de wenselijkheid van transparantie in dat kader, mede naar aanleiding van onder meer de hack van Colonial Pipeline in de zomer van 2021. Het is een voorbeeld dat de toenemende noodzaak voor aandacht voor cyberveiligheid schetst. Dat blijkt ook uit het voorstel voor een 'IT-auditverklaring'. Een dergelijke verklaring houdt in dat accountants een door de vennootschap opgestelde IT-verklaring controleren en hierover een verklaring openbaar maken. De IT-auditverklaring kan bijdragen aan het inzicht van de buitenwereld (bijvoorbeeld potentiële investeerders, klanten en leveranciers) in het cyberveiligheidsniveau van de vennootschap. In de bijdrage van *Eijkelenboom*, *Nieuwesteeg* en *Hoogerwaard* staat de huidige transparantie over cyberveiligheid van AEX-beursvennootschappen centraal. Welke transparantievereisten gelden er voor deze vennootschappen? En op welke wijze zijn zij transparant over hun cyberveiligheid? Eerst bespreken *Eijkelenboom*, *Nieuwesteeg* en *Hoogerwaard* de transparantieverplichtingen voor cyberveiligheid op grond van wet- en regelgeving. Daarna plaatsen zij de wenselijkheid van transparantie over cyberveiligheid in rechtseconomisch perspectief. Zij betogen dat transparantie over cyberveiligheid kan bijdragen aan het verhogen ervan. *Eijkelenboom*, *Nieuwesteeg* en *Hoogerwaard* maken inzichtelijk de mate waarin Nederlandse beursvennootschappen in hun jaarlijkse financiële verslaggeving transparant zijn over cyberveiligheid en concluderen dat uit hun onderzoek naar de financiële verslaggeving over de boekjaren 2018 en 2020 is gebleken dat er steeds meer aandacht voor cyberveiligheid is. Zij besluiten hun bijdrage met de conclusie dat, hoewel steeds meer beursvennootschappen aandacht besteden aan hun digitale veiligheid, er nog een slag te maken valt.

In de derde bijdrage staan *Laurens Kelterman* en *Emilie van Blokland* stil bij het (voorstel van een) Centraal Aandeelhoudersregister (CAHR). Het CAHR is sinds 2011 onderwerp van onderzoek, discussie, nota's en (wets)voorstellen. Het register zou moeten bijdragen aan de bestrijding van fraude, witwassen, terrorismefinanciering en andere criminele aangelegenheden. *Kelterman* en *Van Blokland* stellen de vraag aan de orde of het CAHR zou moeten bestaan naast het vennootschappelijk aandeelhoudersregister en pleiten ervoor om – zoals zij dat noemen – het 'klappertje', dat veelal kwijt, niet actueel, onvolledig of onjuist bijgehouden is, te vervangen door een digitaal register. Zij betogen dat het vennootschappelijk aandeelhoudersregister in het CAHR zou moeten worden opgenomen. *Kelterman* en *Van Blokland* bespreken eerst de huidige stand van zaken van het CAHR, wat de huidige status van het vennootschappelijk aandeelhoudersregister is en wat de relevantie van dat register voor de praktijk is. Er zijn goede argumenten om een CAHR in te stellen, zoals de bestrijding van terrorisme en het tegengaan van fraude. Het CAHR heeft toegevoegde waarde naast het UBO-register. *Kelterman* en *Van Blokland* stellen echter ook dat er een noodzaak is het vennootschappelijk aandeelhoudersregister te digitaliseren. Ook dat is een goede reden een CAHR in te stellen. Er zal dan één digitaal, centraal gehouden aandeelhoudersregister bestaan, waartoe de partijen toegang hebben die nu op basis van de wet ook toegang hebben tot het vennootschappelijk register. In dat register moeten alle voor de rechtspraktijk relevante gegevens opgenomen worden. Daarnaast kunnen opsporingsdiensten en Wwft-instellingen toegang tot het CAHR krijgen, zo betogen *Kelterman* en *Van Blokland*. Bij voorkeur krijgt het CAHR een wettelijke basis. Als het niet snel tot een wettelijke regeling komt, dan zal het CAHR op een andere wijze moeten worden vormgegeven. *Kelterman* en *Van Blokland* zijn van mening dat een digitaal gehouden vennootschappelijk aandeelhoudersregister op basis van bestaande wetgeving al mogelijk is, zij het dat daarbij aandachtspunten bestaan en waarborgen moeten worden gerealiseerd.

Redactioneel

Zo kan door een samenwerking tussen private partijen een CAHR opgezet worden. In die opzet houdt een niet-commerciële partij het CAHR bij en stelt dat tegen kostprijs beschikbaar, aldus *Kelterman* en *Van Blokland*.

Ik nodig u, als lezer, van harte uit te reageren op artikelen in *TvOB* en uw opmerkingen of suggesties kenbaar te maken aan Charlotte Helmer (redactiesecretaris) via: tijdschriftvob@gmail.com.

Namens de redactie, Rogier Wolf