nationale recht moet verrichten als enige verantwoordelijk is voor de inachtneming van de in artikel 5, lid 1, AVG bedoelde beginselen, tenzij uit dit recht voortvloeit dat hij daarvoor gezamenlijk met andere entiteiten verantwoordelijk is.

32

Een datalek betekent niet zonder meer een inbreuk op art. 24 en 32 AVG

Hof van Justitie EU
14 december 2023, C-340/21,
ECLI:EU:C:2023:986
(Jürimäe, Piçarra, Safjan, Jääskinen, Gavalec)
Noot mr. M. Moeskops, mr. J.G. Reus

NAP. Bulgarije. Immateriële schadevergoeding. Hacking. Informatiebeveiliging.

[VWEU art. 267; AVG art. 4, 5, 24, 32, 82]

Bij het nationaal agentschap voor overheidsinkomsten van Bulgarije (hierna: de NAP) vindt een datalek plaats. Verzoekster in het hoofdgeding stelt vervolgens een vordering tot schadevergoeding in wegens immateriële schade. De bestuursrechter in eerste aanleg verwerpt het beroep, waartegen verzoekster beroep instelt bij de hoogste bestuursrechter. Die rechter stelt in deze zaak prejudiciële vragen aan het Hof.
Ten eerste overweegt het Hof dat het feit dat een datalek heeft plaatsgevonden niet volstaat om aan te nemen dat de getroffen technische en organisatorische maatregelen niet passend zijn. Art. 24 en 32 AVG verplichten de verwerkingsverantwoordelijke enkel technische en organisatorische maatregelen te treffen om elke inbreuk in verband met persoonsgegevens zoveel mogelijk te voorkomen. Of de maatregelen passend zijn, moet worden beoordeeld door te onderzoeken of rekening is gehouden met de in de artikelen genoemde criteria en de specifieke behoeften van gegevensbescherming. Daarnaast moet de verwerkingsverantwoordelijke tegenbewijs kunnen leveren.
Ten tweede overweegt het Hof dat de nationale rechterlijke instanties moeten beoordelen of de getroffen maatregelen passend zijn. Blijkens art. 32 AVG moeten de risico's verbonden aan de verwerking en de eventuele gevolgen daarvan worden vastgesteld. Daarna moet worden nagegaan of de maatregelen zijn afgestemd op die risico's. Daarbij moet rekening worden gehouden met onder andere de aard, de omvang, de context en de doeleinden van de verwerking. Hoewel de verwerkingsverantwoordelijke beoordelingsruimte heeft om te bepalen welke maatregelen passend zijn, moet een nationale rechterlijke instantie die beoordeling kunnen evalueren.
Ten derde overweegt het Hof dat het in het kader van art. 82 AVG aan de verwerkingsverantwoordelijke is om aan te tonen dat de getroffen maatregelen passend zijn. Volgens het Hof blijkt dit ondubbelzinnig uit de bewoordingen van art. 5, 24 en 32 AVG en moet deze regel worden toegepast in het kader van art. 82 AVG. Vervolgens overweegt het Hof dat een deskundigenrapport niet een noodzakelijk en toereikend bewijsmiddel vormt om te beoordelen of de getroffen maatregelen passend zijn. Daarbij merkt het Hof op dat de AVG hierover geen voorschriften bevat, waardoor dit een zaak van de interne rechtsorde van de lidstaten is. Echter, een deskundigenrapport als een noodzakelijk en toereikend bewijsmiddel is in strijd met het doeltreffendheidsbeginsel, omdat een deskundigenonderzoek in sommige zaken overbodig is en een rechter niet automatisch uit een deskundigenrapport moet afleiden dat de maatregelen passend zijn.
Ten vierde overweegt het Hof dat de verwerkingsverantwoordelijke niet van zijn verplichting tot schadevergoeding wordt vrijgesteld op de enkele grond dat de schade het gevolg is van hacking door derden. De verwerkingsverantwoordelijke kan slechts van zijn aansprakelijkheid worden vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.
Tot slot overweegt het Hof dat de vrees die een betrokkene na een datalek heeft voor mogelijk misbruik van zijn persoonsgegevens, op zich immateriële schade ex art. 82 AVG kan vormen. De bewoordingen van art. 82 AVG sluiten dit in ieder geval niet uit. Daarvoor is steun te vinden in overweging 146 AVG dat het begrip 'schade' ruim moet worden uitgelegd.

VB
tegen
Natsionalna agentsia za prihodite.

Arrest

1. Het verzoek om een prejudiciële beslissing betreft de uitlegging van artikel 5, lid 2, de artikelen 24 en 32 en artikel 82, leden 1 tot en met 3, van 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 en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB 2016, L 119, blz. 1, met rectificaties in PB 2018, L 127, blz. 2, en PB 2021, L 74, blz. 35; hierna: "AVG").

2. Dit verzoek is ingediend in het kader van een geding tussen VB, een natuurlijke persoon, en de Natsionalna agentsia za prihodite (nationaal agentschap voor overheidsinkomsten, Bulgarije; hierna: "NAP") over de vergoeding van de immateriële schade die VB stelt te hebben geleden wegens de vermeende niet-nakoming door deze overheidsinstantie van de wettelijke verplichtingen die op haar als verantwoordelijke voor de verwerking van persoonsgegevens rusten.

Toepasselijke bepalingen

3. De overwegingen 4, 10, 11, 74, 76, 83, 85 en 146 AVG luiden als volgt:

"(4) [...] Deze verordening eerbiedigt alle grondrechten alsook de vrijheden en beginselen die zijn erkend in het Handvest [van de grondrechten van de Europese Unie] zoals dat in de Verdragen is verankerd, met name de eerbiediging van het privéleven en het familie- en gezinsleven, woning en communicatie, de bescherming van persoonsgegevens, [...] [en] het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht [...].

[...]

(10) Teneinde natuurlijke personen een consistent en hoog beschermingsniveau te bieden en de belemmeringen voor het verkeer van persoonsgegevens binnen de [Europese] Unie op te heffen, dient het niveau van bescherming van de rechten en vrijheden van natuurlijke personen op het vlak van verwerking van deze gegevens in alle lidstaten gelijkwaardig te zijn. Er moet gezorgd worden voor een in de gehele Unie coherente en homogene toepassing van de regels inzake bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens. [...]

(11) Doeltreffende bescherming van persoonsgegevens in de gehele Unie vereist de versterking en nadere omschrijving van de rechten van betrokkenen en van de verplichtingen van degenen die persoonsgegevens verwerken en van degenen die over die verwerking beslissen, [...].

[...]

(74) De verantwoordelijkheid en aansprakelijkheid van de verwerkingsverantwoordelijke moeten worden vastgesteld voor elke verwerking van persoonsgegevens die door of namens hem wordt uitgevoerd. Meer bepaald dient de verwerkingsverantwoordelijke te worden verplicht passende en effectieve maatregelen uit te voeren en te kunnen aantonen dat elke verwerkingsactiviteit overeenkomstig deze verordening geschiedt, ook wat betreft de doeltreffendheid van de maatregelen. Bij die maatregelen moet rekening worden gehouden met de aard, de omvang, de context en het doel van de verwerking en het risico voor de rechten en vrijheden van natuurlijke personen.

[...]

(76) De waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkene moeten worden bepaald onder verwijzing naar de aard, het toepassingsgebied, de context en de doeleinden van de verwerking. Het risico moet worden bepaald op basis van een objectieve beoordeling en vastgesteld moet worden of de verwerking gepaard gaat met een risico of een hoog risico.

[...]

(83) Teneinde de veiligheid te waarborgen en te voorkomen dat de verwerking inbreuk maakt op deze verordening, dient de verwerkingsverantwoordelijke of de verwerker de aan de verwerking inherente risico's te beoordelen en maatregelen, zoals versleuteling, te treffen om die risico's te beperken. Die maatregelen dienen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, te waarborgen, rekening houdend met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens. Bij de beoordeling van de gegevensbeveiligingsrisico's dient aandacht te worden besteed aan risico's die zich voordoen bij persoonsgegevensverwerking, zoals de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij on-

rechtmatig, hetgeen met name tot lichamelijke, materiële of immateriële schade kan leiden.
[...]
(85) Een inbreuk in verband met persoonsgegevens kan, wanneer dit probleem niet tijdig en op passende wijze wordt aangepakt, resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens of de beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie. Daarom moet de verwerkingsverantwoordelijke, zodra hij weet dat een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, de toezichthoudende autoriteit onverwijld [...] in kennis stellen van de inbreuk in verband met persoonsgegevens, [...].
[...]
(146) De verwerkingsverantwoordelijke of de verwerker [moet] alle schade vergoeden die iemand kan lijden ten gevolge van een verwerking die inbreuk maakt op deze verordening. De verwerkingsverantwoordelijke of de verwerker moet van zijn aansprakelijkheid worden vrijgesteld indien hij bewijst dat hij niet verantwoordelijk is voor de schade. Het begrip 'schade' moet ruim worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen van deze verordening. Dit laat eventuele eisen tot schadeloosstelling wegens inbreuken op andere regels in het Unierecht of het lidstatelijke recht onverlet. Onder verwerking die inbreuk maakt op deze verordening, valt eveneens een verwerking die inbreuk maakt op gedelegeerde handelingen en uitvoeringshandelingen die werden vastgesteld overeenkomstig deze verordening, alsmede het lidstatelijke recht waarin in deze verordening vervatte regels worden gespecificeerd. De betrokkenen dienen volledige en daadwerkelijke vergoeding van door hen geleden schade te ontvangen. [...]"
4. Artikel 4 ("Definities") van deze verordening bepaalt:
"Voor de toepassing van deze verordening wordt verstaan onder:
1) 'persoonsgegevens': alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); [...]
2) 'verwerking': een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, [...];
[...]
7) 'verwerkingsverantwoordelijke': een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; [...]
[...]
10) 'derde': een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;
[...]
12) 'inbreuk in verband met persoonsgegevens': een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
[...]"
5. Artikel 5 ("Beginselen inzake verwerking van persoonsgegevens") van die verordening bepaalt:
"1. Persoonsgegevens moeten:
a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is ('rechtmatigheid, behoorlijkheid en transparantie');
[...]
f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ('integriteit en vertrouwelijkheid');
2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen ('verantwoordingsplicht')."

6. Artikel 24 AVG, met als opschrift "Verantwoordelijkheid van de verwerkingsverantwoordelijke", luidt als volgt:
"1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen."
7. Artikel 32 AVG, "Beveiliging van de verwerking", bepaalt:
"1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
a) de pseudonimisering en versleuteling van persoonsgegevens;
b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.
[...]"
8. Artikel 79 ("Recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke of een verwerker") van deze verordening bepaalt in lid 1:
"Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, waaronder het recht uit hoofde van artikel 77 een klacht in te dienen bij een toezichthoudende autoriteit, heeft elke betrokkene het recht een doeltreffende voorziening in rechte in te stellen indien hij van mening is dat zijn rechten uit hoofde van deze verordening geschonden zijn ten gevolge van een verwerking van zijn persoonsgegevens die niet aan deze verordening voldoet."
9. Artikel 82 ("Recht op schadevergoeding en aansprakelijkheid") van die verordening bepaalt in de leden 1 tot en met 3:
"1. Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade.
2. Elke verwerkingsverantwoordelijke die bij verwerking is betrokken, is aansprakelijk voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op deze verordening. [...]
3. Een verwerkingsverantwoordelijke of verwerker wordt van aansprakelijkheid op grond van lid 2 vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit."

Hoofdgeding en prejudiciële vragen

10. De NAP is een instantie die ressorteert onder de Bulgaarse minister van Financiën. In het kader van haar taken, die onder meer bestaan in het vaststellen, veiligstellen en invorderen van vorderingen van openbare schuldeisers, is zij verant-

woordelijk voor de verwerking van persoonsgegevens in de zin van artikel 4, punt 7, AVG.
11. Op 15 juli 2019 hebben de media gemeld dat ongeoorloofde toegang tot het IT-systeem van de NAP had plaatsgevonden en dat er na die cyberaanval persoonsgegevens uit dat systeem op internet waren gepubliceerd.
12. Meer dan zes miljoen natuurlijke personen van Bulgaarse of buitenlandse nationaliteit zijn geraakt door deze gebeurtenissen. Enkele honderden van hen, waaronder verzoekster in het hoofdgeding, hebben tegen de NAP vorderingen ingesteld tot vergoeding van de immateriële schade die volgens hen uit de bekendmaking van hun persoonsgegevens is voortgevloeid.
13. Tegen deze achtergrond heeft verzoekster in het hoofdgeding op grond van artikel 82 AVG en bepalingen van Bulgaars recht een vordering ingesteld bij de Administrativen sad Sofia-grad (bestuursrechter in eerste aanleg Sofia, Bulgarije) om te verkrijgen dat de NAP haar een schadevergoeding van 1 000 Bulgaarse leva (BGN) (ongeveer 510 EUR) betaalt. Tot staving van dit verzoek heeft zij aangevoerd dat zij immateriële schade heeft geleden door een inbreuk in verband met persoonsgegevens in de zin van artikel 4, punt 12, AVG, meer in het bijzonder een inbreuk op de beveiliging die is veroorzaakt doordat de NAP haar verplichtingen uit hoofde van met name artikel 5, lid 1, onder f), en de artikelen 24 en 32 van deze verordening niet is nagekomen. Haar immateriële schade bestaat in de vrees voor toekomstig misbruik van haar persoonsgegevens die zonder haar toestemming zijn gepubliceerd of dat zij zelf het slachtoffer wordt van afpersing of agressie of zelfs wordt ontvoerd.
14. Ter verweer heeft de NAP om te beginnen aangevoerd dat verzoekster in het hoofdgeding haar niet had verzocht om informatie over welke gegevens precies waren verstrekt. Voorts heeft de NAP documenten overgelegd om aan te tonen dat zij eerder alle nodige maatregelen had genomen om een inbreuk in verband met de in haar IT-systeem vervatte persoonsgegevens te voorkomen en dat zij na de inbreuk alle nodige maatregelen had genomen om de gevolgen van deze inbreuk te beperken en de burgers gerust te stellen. Voorts bestaat er volgens de NAP geen causaal verband tussen de gestelde immateriële schade en die inbreuk. Ten slotte heeft zij gesteld dat zij niet verantwoordelijk kan worden gehouden voor de schadelijke gevolgen van die inbreuk, aangezien zij zelf het slachtoffer was geworden van misbruik door personen die geen werknemers van haar waren.
15. Bij beslissing van 27 november 2020 heeft de Administrativen sad Sofia-grad het beroep van verzoekster in het hoofdgeding verworpen. Deze rechter heeft ten eerste geoordeeld dat de ongeoorloofde toegang tot de databank van de NAP het gevolg was van hacking door derden en ten tweede dat verzoekster in het hoofdgeding niet had aangetoond dat de NAP had verzuimd veiligheidsmaatregelen vast te stellen. Voorts was die rechter van oordeel dat verzoekster geen immateriële schade had geleden die recht geeft op vergoeding.
16. Verzoekster in het hoofdgeding heeft tegen die beslissing cassatieberoep ingesteld bij de Varhoven administrativen sad (hoogste bestuursrechter, Bulgarije), de verwijzende rechter in de onderhavige zaak. Ter onderbouwing van haar cassatieberoep betoogt zij dat de rechter in eerste aanleg bij de verdeling van de bewijslast inzake de door de NAP genomen veiligheidsmaatregelen blijk heeft gegeven van een onjuiste rechtsopvatting en dat de NAP niet heeft aangetoond dat zij dienaangaande niet had verzuimd om op te treden. Voorts stelt verzoekster in het hoofdgeding dat de vrees voor toekomstig mogelijk misbruik van haar persoonsgegevens daadwerkelijke immateriële schade vormt, en geen hypothetische immateriële schade. In haar verweerschrift betwist de NAP elk van deze argumenten.
17. De verwijzende rechter acht het om te beginnen mogelijk dat louter op grond van de vaststelling van een inbreuk in verband met persoonsgegevens al kan worden geconcludeerd dat de maatregelen die door de verantwoordelijke voor de verwerking van deze gegevens zijn getroffen, niet "passend" waren in de zin van de artikelen 24 en 32 AVG.
18. Voor het geval dat deze vaststelling ontoereikend is om tot die conclusie te komen, vraagt hij zich echter, ten eerste, af wat de omvang is van de toetsing die nationale rechters moeten verrichten bij de beoordeling of de betrokken maatregelen passend zijn en, ten tweede, welke regels inzake de bewijsvoering in dat verband moeten worden toegepast ten aanzien van zowel de bewijslast als de bewijsmiddelen, met name wanneer die rechters zich moeten uitspreken over een vordering tot schadevergoeding op grond van artikel 82 van deze verordening.

19. Voorts wenst de verwijzende rechter te vernemen of de omstandigheid dat de inbreuk in verband met persoonsgegevens toe te schrijven is aan een handeling van derden, in casu een cyberaanval, in het licht van artikel 82, lid 3, van die verordening een factor is die de verantwoordelijke voor de verwerking van deze gegevens systematisch vrijstelt van zijn aansprakelijkheid voor de schade die de betrokkene is berokkend.
20. Ten slotte vraagt de verwijzende rechter zich af of de door een persoon gekoesterde vrees voor mogelijk misbruik van zijn persoonsgegevens in de toekomst, in het onderhavige geval na ongeoorloofde toegang tot die gegevens en bekendmaking ervan door cybercriminelen, op zich "immateriële schade" in de zin van artikel 82, lid 1, AVG kan vormen. Zo ja, dan hoeft deze persoon niet aan te tonen dat derden vóór zijn vordering tot schadevergoeding onrechtmatig gebruik hebben gemaakt van die gegevens, zoals misbruik van zijn identiteit.
21. In die omstandigheden heeft de Varhoven administratiyen sad de behandeling van de zaak geschorst en het Hof verzocht om een prejudiciële beslissing over de volgende vragen:
"1) Moeten de artikelen 24 en 32 [AVG] aldus worden uitgelegd dat het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens in de zin van artikel 4, punt 12, [AVG] heeft plaatsgevonden door personen die geen medewerkers van de verwerkingsverantwoordelijke zijn en niet onder zijn toezicht staan, volstaat om aan te nemen dat de getroffen technische en organisatorische maatregelen niet passend zijn?
2) Ingeval de eerste vraag ontkennend wordt beantwoord: waarop moet de rechterlijke toetsing van de rechtmatigheid bij het onderzoek van de vraag of de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen passend zijn in de zin van artikel 32 [AVG] betrekking hebben en welke omvang moet die toetsing hebben?
3) Ingeval de eerste vraag ontkennend wordt beantwoord: moet het beginsel van de verantwoordingsplicht op grond van artikel 5, lid 2, [AVG] en artikel 24 [van deze verordening] juncto overweging 74 [ervan] aldus worden uitgelegd dat in het kader van een beroep op grond van artikel 82, lid 1, van [die verordening] de bewijslast voor het feit dat de getroffen technische en organisatorische maatregelen passend zijn in de zin van artikel 32 [AVG], op de verwerkingsverantwoordelijke rust? Kan een deskundigenrapport als een noodzakelijk en toereikend bewijsmiddel worden beschouwd om vast te stellen dat de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen in een geval zoals het onderhavige passend waren, wanneer de ongeoorloofde toegang tot en de ongeoorloofde verstrekking van persoonsgegevens het gevolg zijn van een 'cyberaanval'?
4) Moet artikel 82, lid 3, [AVG] aldus worden uitgelegd dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens in de zin van artikel 4, punt 12, [AVG], in casu door middel van een 'cyberaanval' door personen die geen medewerkers van de verwerkingsverantwoordelijke zijn en niet onder zijn toezicht staan, een feit is waarvoor de verwerkingsverantwoordelijke niet verantwoordelijk is en dat bijgevolg een vrijstelling van aansprakelijkheid rechtvaardigt?
5) Moeten artikel 82, leden 1 en 2, [AVG] junctis de overwegingen 85 en 146 [van deze] verordening aldus worden uitgelegd dat wanneer er zoals in casu sprake is van een inbreuk op de beveiliging van persoonsgegevens die bestaat in de ongeoorloofde toegang tot en de verspreiding van persoonsgegevens door middel van een 'cyberaanval', alleen al de bezorgdheid en ongerustheid van de betrokkene en zijn vrees voor mogelijk misbruik van zijn persoonsgegevens in de toekomst, zonder dat een dergelijk misbruik is vastgesteld en/of de betrokkene verdere schade heeft geleden, onder het ruim uit te leggen begrip 'immateriële schade' vallen en een recht op schadevergoeding doen ontstaan?"

Beantwoording van de prejudiciële vragen

Eerste vraag
22. Met zijn eerste vraag wenst de verwijzende rechter in essentie te vernemen of de artikelen 24 en 32 AVG aldus moeten worden uitgelegd dat het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens heeft plaatsgevonden door "derden" in de zin van artikel 4, punt 10, van deze verordening, op zich volstaat om aan te nemen dat de door de betrokken verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen niet

"passend" waren in de zin van de artikelen 24 en 32 AVG.
23. Vooraf zij eraan herinnerd dat de bewoordingen van een Unierechtelijke bepaling die, zoals de artikelen 24 en 32 AVG, voor de betekenis en de draagwijdte ervan niet uitdrukkelijk verwijst naar het recht van de lidstaten, volgens vaste rechtspraak normaal gesproken in de gehele Unie autonoom en uniform moeten worden uitgelegd, waarbij met name rekening moet worden gehouden met de bewoordingen van de betrokken bepaling, de daarmee nagestreefde doelstellingen en de context ervan [zie in die zin arresten van 18 januari 1984, Ekro, 327/82, ECLI:EU:C:1984:11, punt 11; 1 oktober 2019, Planet49, C-673/17, ECLI:EU:C:2019:801, punten 47 en 48, en 4 mei 2023, Österreichische Post (Immateriële schade ten gevolge van de verwerking van persoonsgegevens), C-300/21, ECLI:EU:C:2023:370, punt 29].
24. Wat in de eerste plaats de bewoordingen van de relevante bepalingen betreft, moet worden opgemerkt dat artikel 24 AVG voorziet in een algemene verplichting voor de verantwoordelijke voor de verwerking van persoonsgegevens om passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat die verwerking in overeenstemming met deze verordening wordt uitgevoerd.
25. Daartoe somt artikel 24 AVG in lid 1 een aantal criteria op waarmee rekening moet worden gehouden bij de beoordeling of dergelijke maatregelen passend zijn, namelijk de aard, de omvang, de context en het doel van de verwerking, alsook de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen. Deze bepaling voegt daaraan toe dat die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
26. In dit opzicht verduidelijkt artikel 32 AVG de verplichtingen van de verwerkingsverantwoordelijke en een eventuele verwerker met betrekking tot de beveiliging van deze verwerking. Zo is in artikel 32, lid 1, AVG bepaald dat laatstgenoemden passende technische en organisatorische maatregelen moeten treffen om een beveiligingsniveau te waarborgen dat afgestemd is op de in het vorige punt van het onderhavige arrest genoemde risico's, waarbij zij rekening moeten houden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de doeleinden van de betrokken verwerking.
27. Evenzo is in artikel 32, lid 2, AVG bepaald dat bij de beoordeling van het passende beveiligingsniveau met name rekening moet worden gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot persoonsgegevens, hetzij per ongeluk hetzij op onrechtmatige wijze.
28. Voorts is in zowel artikel 24, lid 3, van deze verordening als artikel 32, lid 3, daarvan aangegeven dat de verwerkingsverantwoordelijke of de verwerker kan aantonen dat hij de vereisten van lid 1 van die artikelen heeft nageleefd met een beroep op het feit dat hij aansluit bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme als bedoeld in respectievelijk artikel 40 en artikel 42 van die verordening.
29. Uit de verwijzing in artikel 32, leden 1 en 2, AVG naar "een op het risico afgestemd beveiligingsniveau" en een "passend veiligheidsniveau" blijkt dat deze verordening een risicobeheersysteem instelt en op geen enkele wijze beoogt de risico's van inbreuken in verband met persoonsgegevens weg te nemen.
30. Aldus blijkt uit de bewoordingen van de artikelen 24 en 32 AVG dat deze bepalingen de verwerkingsverantwoordelijke enkel verplichten technische en organisatorische maatregelen vast te stellen om elke inbreuk in verband met persoonsgegevens zoveel mogelijk te voorkomen. De vraag of dergelijke maatregelen passend zijn, moet concreet worden beoordeeld door te onderzoeken of deze verantwoordelijke bij de uitvoering van die maatregelen rekening heeft gehouden met de verschillende in die artikelen genoemde criteria en de behoeften van gegevensbescherming die specifiek inherent zijn aan de betrokken verwerking en de risico's daarvan.
31. Bijgevolg kunnen de artikelen 24 en 32 AVG niet aldus worden begrepen dat het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens heeft plaatsgevonden door een derde, volstaat om tot de slotsom te komen dat de door de betrokken verwerkingsverantwoordelijke getroffen maatregelen niet passend waren in de zin van deze bepalingen, zonder dat deze laatste ook maar de mogelijkheid wordt geboden het tegenbewijs te leveren.
32. Een dergelijke uitlegging is te meer geboden daar artikel 24 AVG uitdrukkelijk bepaalt dat de verwerkingsverantwoordelijke moet kunnen aantonen dat de door hem getroffen maatregelen in

overeenstemming zijn met deze verordening. Deze mogelijkheid zou hem worden ontnomen indien een onweerlegbaar vermoeden zou worden aanvaard.
33. In de tweede plaats is voor deze uitlegging van de artikelen 24 en 32 AVG steun te vinden in contextuele en teleologische elementen.
34. Wat ten eerste de context van deze twee artikelen betreft, zij opgemerkt dat uit artikel 5, lid 2, AVG volgt dat de verwerkingsverantwoordelijke moet kunnen aantonen dat hij de in artikel 5, lid 1, AVG geformuleerde beginselen inzake de verwerking van persoonsgegevens heeft geëerbiedigd. Deze verplichting is in artikel 24, leden 1 en 3, en in artikel 32, lid 3, van deze verordening overgenomen en verduidelijkt ten aanzien van de verplichting om technische en organisatorische maatregelen te treffen om dergelijke gegevens te beschermen wanneer zij door de verwerkingsverantwoordelijke worden verwerkt. Een dergelijke verplichting om aan te tonen dat die maatregelen passend zijn, zou geen zin hebben indien de verwerkingsverantwoordelijke verplicht was om elke inbreuk in verband met die gegevens te voorkomen.
35. Voorts wordt in overweging 74 AVG benadrukt dat de verwerkingsverantwoordelijke dient te worden verplicht passende en effectieve maatregelen uit te voeren en te kunnen aantonen dat elke verwerkingsactiviteit overeenkomstig deze verordening geschiedt, ook wat betreft de doeltreffendheid van de maatregelen, en dat bij die maatregelen rekening moet worden gehouden met de criteria die verband houden met de kenmerken van de betrokken verwerking en het daarmee gepaard gaande risico, die ook in de artikelen 24 en 32 AVG zijn opgenomen.
36. Evenzo staat in overweging 76 van deze verordening te lezen dat de waarschijnlijkheid en de ernst van het risico afhangen van de specifieke kenmerken van de betrokken verwerking en dat dit risico moet worden bepaald op basis van een objectieve beoordeling.
37. Daarnaast volgt uit artikel 82, leden 2 en 3, AVG dat een verwerkingsverantwoordelijke weliswaar aansprakelijk is voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op deze verordening, maar dat hij niettemin van zijn aansprakelijkheid wordt vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.
38. Ten tweede is voor de uitlegging in punt 31 van het onderhavige arrest ook steun te vinden in overweging 83 AVG, waarvan de eerste volzin vermeldt dat "[t]eneinde de veiligheid te waarborgen en te voorkomen dat de verwerking inbreuk maakt op deze verordening, [...] de verwerkingsverantwoordelijke of de verwerker de aan de verwerking inherente risico's [dient] te beoordelen en maatregelen [...] [dient] te treffen om die risico's te beperken". De Uniewetgever heeft daarmee blijk gegeven van zijn voornemen om de risico's van een inbreuk in verband met persoonsgegevens te "beperken", zonder te beweren dat zij kunnen worden weggenomen.
39. Gelet op een en ander dient op de eerste vraag te worden geantwoord dat de artikelen 24 en 32 AVG aldus moeten worden uitgelegd dat het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens heeft plaatsgevonden door "derden" in de zin van artikel 4, punt 10, van deze verordening, op zich niet volstaat om aan te nemen dat de door de betrokken verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen niet "passend" waren in de zin van die artikelen 24 en 32.

Tweede vraag
40. Met zijn tweede vraag wenst de verwijzende rechter in essentie te vernemen of artikel 32 AVG aldus moet worden uitgelegd dat de vraag of de door de verwerkingsverantwoordelijke op grond van dit artikel getroffen technische en organisatorische maatregelen passend zijn, concreet moet worden beoordeeld door de nationale rechterlijke instanties, met name door rekening te houden met de aan de betrokken verwerking verbonden risico's.
41. In dit verband zij eraan herinnerd dat, zoals in het antwoord op de eerste vraag is benadrukt, artikel 32 AVG vereist dat de verwerkingsverantwoordelijke en de verwerker, naargelang van het geval, passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen, rekening houdend met de beoordelingscriteria van artikel 32, lid 1, AVG. Voorts geeft artikel 32, lid 2, AVG een niet-uitputtende opsomming van een aantal factoren die relevant zijn bij de beoordeling welk beveiligingsniveau passend is in het licht van de risico's van de betrokken verwerking.

42. Blijkens artikel 32, leden 1 en 2, AVG moet in twee stappen worden beoordeeld of dergelijke technische en organisatorische maatregelen passend zijn. In de eerste plaats moeten de aan de betrokken verwerking verbonden risico's van een inbreuk in verband met persoonsgegevens en de eventuele gevolgen daarvan voor de rechten en vrijheden van natuurlijke personen worden vastgesteld. Bij deze concreet te verrichten beoordeling worden de mate van waarschijnlijkheid en de ernst van de vastgestelde risico's in aanmerking genomen. In de tweede plaats moet worden nagegaan of de door de verwerkingsverantwoordelijke getroffen maatregelen zijn afgestemd op die risico's, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de doeleinden van deze verwerking.
43. Het is juist dat de verwerkingsverantwoordelijke over een zekere beoordelingsmarge beschikt om te bepalen welke technische en organisatorische maatregelen passend zijn om een op het risico afgestemd beveiligingsniveau te waarborgen, zoals artikel 32, lid 1, AVG vereist. Dit neemt niet weg dat een nationale rechterlijke instantie de ingewikkelde beoordeling door de verwerkingsverantwoordelijke moet kunnen evalueren om er aldus voor te zorgen dat de door deze laatste gekozen maatregelen geschikt zijn om een dergelijk veiligheidsniveau te waarborgen.
44. Met een dergelijke uitlegging kunnen overigens de doeltreffendheid van de bescherming van persoonsgegevens, die in de overwegingen 11 en 74 van deze verordening wordt beklemtoond, en het recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke, zoals beschermd door artikel 79, lid 1, van die verordening, gelezen in samenhang met overweging 4 ervan, worden verzekerd.
45. Bijgevolg moet een nationale rechterlijke instantie bij de toetsing of de krachtens artikel 32 AVG getroffen technische en organisatorische maatregelen passend zijn, niet alleen vaststellen op welke wijze de betrokken verwerkingsverantwoordelijke heeft willen voldoen aan de krachtens dit artikel op hem rustende verplichtingen, maar moet hij deze maatregelen ook inhoudelijk onderzoeken in het licht van alle in dat artikel genoemde criteria, de omstandigheden van het betrokken geval en het bewijs waarover deze rechterlijke instantie dienaangaande beschikt.
46. Een dergelijk onderzoek vereist een concrete analyse van zowel de aard als de inhoud van de door de verwerkingsverantwoordelijke getroffen maatregelen, de wijze waarop deze maatregelen zijn toegepast en de praktische gevolgen ervan voor het veiligheidsniveau dat hij in het licht van de aan deze verwerking inherente risico's dient te waarborgen.
47. Bijgevolg dient op de tweede vraag te worden geantwoord dat artikel 32 AVG aldus moet worden uitgelegd dat de vraag of de door de verwerkingsverantwoordelijke op grond van dit artikel getroffen technische en organisatorische maatregelen passend zijn, door de nationale rechterlijke instanties concreet moet worden beoordeeld, door rekening te houden met de aan de betrokken verwerking verbonden risico's en door te beoordelen of de aard, de inhoud en de uitvoering van die maatregelen afgestemd zijn op die risico's.

Derde vraag

Eerste deel van de derde vraag
48. Met het eerste deel van zijn derde vraag wenst de verwijzende rechter in essentie te vernemen of het beginsel van verantwoordelijkheid van de verwerkingsverantwoordelijke, dat is geformuleerd in artikel 5, lid 2, AVG en nader is uitgewerkt in artikel 24 ervan, aldus moet worden uitgelegd dat het in het kader van een vordering tot schadevergoeding op grond van artikel 82 van deze verordening aan de betrokken verwerkingsverantwoordelijke staat om aan te tonen dat de beveiligingsmaatregelen die hij op grond van artikel 32 van die verordening heeft getroffen, passend zijn.
49. In dit verband zij er in de eerste plaats aan herinnerd dat artikel 5, lid 2, AVG een verantwoordelijkheidsbeginsel formuleert, op grond waarvan de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de in artikel 5, lid 1, AVG genoemde beginselen inzake de verwerking van persoonsgegevens, en dat bepaalt dat die verantwoordelijke moet kunnen aantonen dat deze beginselen zijn nageleefd.
50. In het bijzonder moet de verwerkingsverantwoordelijke er overeenkomstig het in artikel 5, lid 1, onder f), van deze verordening bedoelde beginsel van integriteit en vertrouwelijkheid van persoonsgegevens op toezien dat die gegevens door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier

worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging, en moet hij kunnen aantonen dat dit beginsel is geëerbiedigd.
51. Voorts moet worden opgemerkt dat zowel artikel 24, lid 1, AVG, gelezen in het licht van overweging 74 ervan, als artikel 32, lid 1, van deze verordening de verwerkingsverantwoordelijke verplicht om voor elke verwerking van persoonsgegevens die door of namens hem wordt uitgevoerd, passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met die verordening wordt uitgevoerd.
52. Uit de bewoordingen van artikel 5, lid 2, artikel 24, lid 1, en artikel 32, lid 1, AVG blijkt ondubbelzinnig dat het aan de verwerkingsverantwoordelijke staat om te bewijzen dat de persoonsgegevens op een dusdanige manier worden verwerkt dat een passende beveiliging ervan in de zin van artikel 5, lid 1, onder f), en artikel 32 van deze verordening gewaarborgd is [zie naar analogie arresten van 4 mei 2023, Bundesrepublik Deutschland (Gerechtelijke elektronische postbus), C-60/22, ECLI:EU:C:2023:373, punten 52 en 53, en 4 juli 2023, Meta Platforms e.a. (Algemene gebruiksvoorwaarden van een online sociaal netwerk), C-252/21, ECLI:EU:C:2023:537, punt 95].
53. Deze drie artikelen bevatten dus een algemeen toepasselijke regel die, bij gebreke van andersluidende aanwijzingen in de AVG, ook moet worden toegepast in het kader van een vordering tot schadevergoeding op grond van artikel 82 van deze verordening.
54. In de tweede plaats moet worden vastgesteld dat voor de voorgaande letterlijke uitlegging steun is te vinden in de omstandigheid dat rekening wordt gehouden met de doelstellingen van de AVG.
55. Aangezien, ten eerste, het door de AVG beoogde beschermingsniveau afhangt van de beveiligingsmaatregelen die door de verantwoordelijken voor de verwerking van persoonsgegevens worden vastgesteld, moeten zij via de op hen rustende verplichting om aan te tonen dat deze maatregelen passend zijn, worden aangespoord om alles in het werk te stellen om verwerkingen te voorkomen die niet in overeenstemming zijn met deze verordening.
56. Indien, ten tweede, wordt geoordeeld dat het aan de betrokkenen, zoals omschreven in artikel 4, punt 1, AVG, staat om te bewijzen dat die maatregelen passend zijn, zou daaruit volgen dat het in artikel 82, lid 1, van deze verordening bedoelde recht op schadevergoeding een groot deel van zijn nuttig effect zou verliezen, ofschoon de Uniewetgever heeft beoogd zowel de rechten van deze personen als de verplichtingen van de verwerkingsverantwoordelijken te versterken ten opzichte van de bepalingen die vóór die verordening golden, zoals blijkt uit overweging 11 ervan.
57. Op het eerste deel van de derde vraag dient derhalve te worden geantwoord dat het beginsel van verantwoordelijkheid van de verwerkingsverantwoordelijke, dat is geformuleerd in artikel 5, lid 2, AVG en dat nader is uitgewerkt in artikel 24 ervan, aldus moet worden uitgelegd dat het in het kader van een vordering tot schadevergoeding op grond van artikel 82 van deze verordening aan de betrokken verwerkingsverantwoordelijke staat om aan te tonen dat de beveiligingsmaatregelen die hij op grond van artikel 32 van die verordening heeft getroffen, passend zijn.

Tweede deel van de derde vraag

58. Met het tweede deel van zijn derde vraag wenst de verwijzende rechter in essentie te vernemen of artikel 32 AVG en het Unierechtelijke doeltreffendheidsbeginsel aldus moeten worden uitgelegd dat een deskundigenrapport een noodzakelijk en toereikend bewijsmiddel vormt om te beoordelen of de beveiligingsmaatregelen die de verwerkingsverantwoordelijke op grond van dat artikel heeft getroffen, passend zijn.
59. In dit verband zij eraan herinnerd dat het volgens vaste rechtspraak, bij ontbreken van Unievoorschriften ter zake, krachtens het beginsel van procedurele autonomie een zaak van de interne rechtsorde van de lidstaten is om de procedureregels vast te stellen voor vorderingen in rechte die worden ingediend ter bescherming van de rechten van de justitiabelen, op voorwaarde evenwel dat die regels – in situaties die binnen de werkingssfeer van het Unierecht vallen – niet ongunstiger zijn dan die welke voor soortgelijke situaties naar nationaal recht gelden (gelijkwaardigheidsbeginsel) en de uitoefening van de door het Unierecht verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel) [arrest van 4 mei 2023, Österreichische Post (Immateriële schade ten gevolge

van de verwerking van persoonsgegevens), C-300/21, ECLI:EU:C:2023:370, punt 53 en aldaar aangehaalde rechtspraak].
60. In het onderhavige geval moet worden opgemerkt dat de AVG geen voorschriften bevat over de toelating en de bewijskracht van een bewijsmiddel, zoals een deskundigenrapport, die moeten worden toegepast door nationale rechters bij wie een vordering tot schadevergoeding op grond van artikel 82 van deze verordening is ingesteld en die in het licht van artikel 32 AVG moeten beoordelen of de door de betrokken verwerkingsverantwoordelijke getroffen beveiligingsmaatregelen passend zijn. Derhalve is het overeenkomstig hetgeen in het vorige punt van het onderhavige arrest in herinnering is gebracht en bij het ontbreken van Unievoorschriften ter zake, een zaak van de interne rechtsorde van de lidstaten om de regels vast te stellen voor vorderingen die worden ingediend ter bescherming van de rechten die de justitiabelen aan artikel 82 AVG ontlenen, en in het bijzonder voor de regels betreffende de bewijsmiddelen aan de hand waarvan kan worden beoordeeld of dergelijke maatregelen in deze context passend zijn, op voorwaarde dat de beginselen van gelijkwaardigheid en doeltreffendheid worden geëerbiedigd [zie naar analogie arresten van 21 juni 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, punt 297, en 4 mei 2023, Österreichische Post (Immateriële schade ten gevolge van de verwerking van persoonsgegevens), C-300/21, ECLI:EU:C:2023:370, punt 54].
61. Het Hof beschikt in de onderhavige procedure niet over gegevens die twijfel doen rijzen over de eerbiediging van het gelijkwaardigheidsbeginsel. Dit ligt anders voor de overeenstemming met het doeltreffendheidsbeginsel, aangezien het gebruik van een deskundigenrapport volgens de bewoordingen van het tweede deel van de derde vraag een "een noodzakelijk en toereikend bewijsmiddel" is.
62. In het bijzonder zou een nationale procedureregel op grond waarvan het systematisch "noodzakelijk" is dat de nationale rechterlijke instanties een deskundigenonderzoek gelasten, in strijd kunnen zijn met het doeltreffendheidsbeginsel. Het systematische gebruik van een dergelijk deskundigenonderzoek kan namelijk overbodig blijken in het licht van de andere bewijzen waarover de aangezochte rechter beschikt; zoals de Bulgaarse regering in haar schriftelijke opmerkingen heeft aangegeven, is dit met name het geval in het licht van de resultaten van een controle op de naleving van de maatregelen ter bescherming van persoonsgegevens die door een bij wet ingestelde onafhankelijke autoriteit is verricht, voor zover die controle recentelijk heeft plaatsgevonden, aangezien die maatregelen overeenkomstig artikel 24, lid 1, AVG moeten worden geëvalueerd en indien nodig geactualiseerd.
63. Voorts wordt het doeltreffendheidsbeginsel, zoals de Europese Commissie in haar schriftelijke opmerkingen heeft opgemerkt, mogelijkerwijs geschonden indien het woord "toereikend" aldus moet worden begrepen dat een nationale rechterlijke instantie uitsluitend of automatisch uit een deskundigenrapport moet afleiden dat de door de betrokken verwerkingsverantwoordelijke getroffen veiligheidsmaatregelen "passend" zijn in de zin van artikel 32 AVG. De bescherming van de bij deze verordening toegekende rechten, die met dat doeltreffendheidsbeginsel wordt beoogd, en in het bijzonder het door artikel 79, lid 1, van die verordening gewaarborgde recht om een doeltreffende voorziening in rechte in te stellen tegen de verwerkingsverantwoordelijke, verlangen dat een onpartijdig gerecht objectief beoordeelt of de betrokken maatregelen passend zijn, in plaats van zich te beperken tot een dergelijke deductie (zie in die zin arrest van 12 januari 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, ECLI:EU:C:2023:2, punt 50).
64. Gelet op een en ander moet op het tweede deel van de derde vraag worden geantwoord dat artikel 32 AVG en het Unierechtelijke doeltreffendheidsbeginsel aldus moeten worden uitgelegd dat een deskundigenrapport geen systematisch noodzakelijk en toereikend bewijsmiddel kan vormen voor de beoordeling of de beveiligingsmaatregelen die de verwerkingsverantwoordelijke op grond van dat artikel heeft getroffen, passend zijn.

Vierde vraag

65. Met zijn vierde vraag wenst de verwijzende rechter in essentie te vernemen of artikel 82, lid 3, AVG aldus moet worden uitgelegd dat de verwerkingsverantwoordelijke van zijn verplichting uit hoofde van artikel 82, leden 1 en 2, van deze verordening tot vergoeding van de door een persoon geleden schade wordt vrijgesteld op de enkele grond dat deze schade het gevolg is van het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens heeft

plaatsgevonden door "derden" in de zin van artikel 4, punt 10, van die verordening.
66. Vooraf moet worden gepreciseerd dat uit artikel 4, punt 10, AVG volgt dat met name andere personen dan die welke onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken, "derden" zijn. Deze definitie heeft betrekking op personen die geen medewerkers van de verwerkingsverantwoordelijke zijn en niet onder zijn toezicht staan, zoals die waarop de gestelde vraag betrekking heeft.
67. Vervolgens zij er in de eerste plaats aan herinnerd dat artikel 82, lid 2, AVG bepaalt dat "[e]lke verwerkingsverantwoordelijke die bij verwerking is betrokken, [...] aansprakelijk [is] voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op deze verordening" en dat artikel 82, lid 3, AVG bepaalt dat een verwerkingsverantwoordelijke of verwerker, naargelang van het geval, van die aansprakelijkheid wordt vrijgesteld "indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit".
68. Voorts vermeldt overweging 146 AVG, die specifiek betrekking heeft op artikel 82 ervan, in de eerste en de tweede volzin dat "[d]e verwerkingsverantwoordelijke of de verwerker [...] alle schade [moet] vergoeden die iemand kan lijden ten gevolge van een verwerking die inbreuk maakt op deze verordening" en "[...] van zijn aansprakelijkheid [moet] worden vrijgesteld indien hij bewijst dat hij niet verantwoordelijk is voor de schade".
69. Uit deze bepalingen volgt ten eerste dat de betrokken verwerkingsverantwoordelijke in beginsel de schade moet vergoeden die is veroorzaakt door verwerking die inbreuk maakt op deze verordening, en ten tweede dat hij slechts van zijn aansprakelijkheid kan worden vrijgesteld indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.
70. Zoals blijkt uit de uitdrukkelijke toevoeging van de woorden "op geen enkele wijze" tijdens de wetgevingsprocedure, moeten de omstandigheden waarin de verwerkingsverantwoordelijke aanspraak kan maken op vrijstelling van zijn wettelijke aansprakelijkheid uit hoofde van artikel 82 AVG, strikt worden beperkt tot de omstandigheden waarin deze verantwoordelijke kan aantonen dat de schade niet aan hem kan worden toegerekend.
71. Wanneer, zoals in casu, een inbreuk in verband met persoonsgegevens in de zin van artikel 4, punt 12, AVG is gepleegd door cybercriminelen, en dus door "derden" in de zin van artikel 4, punt 10, van deze verordening, kan deze inbreuk niet worden toegerekend aan de verwerkingsverantwoordelijke, tenzij deze die inbreuk mogelijk heeft gemaakt door niet te voldoen aan een verplichting van de AVG, en met name de verplichting tot gegevensbescherming die krachtens artikel 5, lid 1, onder f), en de artikelen 24 en 32 van die verordening op hem rust.
72. Wanneer er sprake is van een inbreuk in verband met persoonsgegevens door een derde, kan de verwerkingsverantwoordelijke zich derhalve op grond van artikel 82, lid 3, AVG bevrijden van zijn aansprakelijkheid door aan te tonen dat er geen causaal verband bestaat tussen zijn eventuele niet-nakoming van de verplichting tot gegevensbescherming en de door de natuurlijke persoon geleden schade.
73. In de tweede plaats is de voorgaande uitlegging van artikel 82, lid 3, AVG ook in overeenstemming met de in de overwegingen 10 en 11 ervan opgenomen doelstelling van de AVG om natuurlijke personen een hoog beschermingsniveau te bieden op het vlak van verwerking van hun persoonsgegevens.
74. Gelet op een en ander moet op de vierde vraag worden geantwoord dat artikel 82, lid 3, AVG aldus moet worden uitgelegd dat de verwerkingsverantwoordelijke niet van zijn verplichting uit hoofde van artikel 82, leden 1 en 2, van deze verordening tot vergoeding van de door een persoon geleden schade kan worden vrijgesteld op de enkele grond dat deze schade het gevolg is van het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens heeft plaatsgevonden door "derden" in de zin van artikel 4, punt 10, van die verordening. Die verantwoordelijke moet daartoe bewijzen dat hij op geen enkele wijze verantwoordelijk is voor het betrokken schadeveroorzakende feit.

Vijfde vraag

75. Met zijn vijfde vraag wenst de verwijzende rechter in essentie te vernemen of artikel 82, lid 1, AVG aldus moet worden uitgelegd dat de vrees die een betrokkene na een inbreuk op deze verordening koestert voor mogelijk misbruik van zijn persoonsgegevens door derden, op zich "immate-

riële schade" in de zin van deze bepaling kan vormen.
76. Wat in de eerste plaats de bewoordingen van artikel 82, lid 1, AVG betreft, moet worden opgemerkt dat volgens deze bepaling "[e]enieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, [...] het recht [heeft] om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade".
77. Het Hof heeft er in dit verband op gewezen dat uit de bewoordingen van artikel 82, lid 1, AVG duidelijk blijkt dat het bestaan van "geleden schade" een van de voorwaarden is voor het in die bepaling bedoelde recht op vergoeding, net zoals het bestaan van een inbreuk op deze verordening en een causaal verband tussen die schade en die inbreuk, waarbij deze drie voorwaarden cumulatief vervuld moeten zijn [arrest van 4 mei 2023, Österreichische Post (Immateriële schade ten gevolge van de verwerking van persoonsgegevens), C-300/21, ECLI:EU:C:2023:370, punt 32].
78. Voorts heeft het Hof artikel 82, lid 1, AVG op basis van zowel letterlijke als systemische en teleologische overwegingen aldus uitgelegd dat deze bepaling zich verzet tegen een nationale regel of praktijk op grond waarvan "immateriële schade" in de zin van die bepaling slechts kan worden vergoed indien de door de betrokkene geleden schade een bepaalde mate van ernst bereikt [arrest van 4 mei 2023, Österreichische Post (Immateriële schade ten gevolge van de verwerking van persoonsgegevens), C-300/21, ECLI:EU:C:2023:370, punt 51].
79. Niettemin moet in casu worden beklemtoond dat artikel 82, lid 1, AVG geen onderscheid maakt tussen gevallen waarin de door de betrokkene gestelde "immateriële schade" ten gevolge van een bewezen inbreuk op bepalingen van deze verordening in verband wordt gebracht met misbruik van zijn persoonsgegevens door derden dat zich op het moment van zijn vordering tot schadevergoeding reeds heeft voorgedaan, dan wel wordt gekoppeld aan de angst van die persoon dat dergelijk misbruik zich in de toekomst zou kunnen voordoen.
80. De bewoordingen van artikel 82, lid 1, AVG sluiten dus niet uit dat het begrip "immateriële schade" in deze bepaling een situatie als bedoeld door de verwijzende rechter omvat, waarin de betrokkene zich, met het oog op de verkrijging van schadevergoeding krachtens deze bepaling, beroept op zijn vrees voor mogelijk misbruik van zijn persoonsgegevens door derden in de toekomst als gevolg van de gepleegde inbreuk op deze verordening.
81. Voor deze letterlijke uitlegging is in de tweede plaats steun te vinden in overweging 146 AVG, die specifiek betrekking heeft op het in artikel 82, lid 1, AVG bedoelde recht op schadevergoeding en waarvan de derde volzin vermeldt dat "[h]et begrip 'schade' [...] ruim [moet] worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen" van deze verordening. Een uitlegging van het begrip "immateriële schade" in de zin van artikel 82, lid 1, AVG die niet de situaties omvat waarin de persoon die wordt getroffen door een inbreuk op die verordening, zich beroept op zijn vrees voor toekomstig misbruik van zijn eigen persoonsgegevens, zou niet beantwoorden aan een ruime opvatting van dit begrip, die de Uniewetgever voor ogen had [zie naar analogie arrest van 4 mei 2023, Österreichische Post (Immateriële schade ten gevolge van de verwerking van persoonsgegevens), C-300/21, ECLI:EU:C:2023:370, punten 37 en 46].
82. Voorts staat in overweging 85, eerste volzin, AVG dat "[e]en inbreuk in verband met persoonsgegevens [...], wanneer dit probleem niet tijdig en op passende wijze wordt aangepakt, [kan] resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens of de beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, [...] of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie". Uit deze illustratieve lijst van "schade" die betrokkenen kunnen lijden, blijkt dat de Uniewetgever met name het enkele "verlies van controle" over hun eigen gegevens als gevolg van een inbreuk op deze verordening onder die begrippen heeft willen opnemen, ook al heeft er geen concreet misbruik van de betrokken gegevens ten nadele van die personen plaatsgevonden.
83. In de derde en laatste plaats wordt de uitlegging in punt 80 van het onderhavige arrest geschraagd door de doelstellingen van de AVG, waarmee ten volle rekening moet worden gehouden bij de definitie van het begrip "schade", zoals in overweging 146, derde volzin, van deze verordening is aangegeven. Een uitlegging van artikel 82, lid 1, AVG, volgens welke het begrip "immate-

riële schade" in de zin van deze bepaling niet de situaties zou omvatten waarin een betrokkene zich uitsluitend beroept op zijn vrees voor toekomstig misbruik van zijn gegevens door derden, zou niet stroken met de door dat instrument beoogde waarborg van een hoog beschermingsniveau voor natuurlijke personen op het vlak van verwerking van persoonsgegevens binnen de Unie.

84. Het is echter van belang te benadrukken dat een persoon die wordt getroffen door een inbreuk op de AVG met negatieve gevolgen voor hem, dient te bewijzen dat die gevolgen immateriële schade in de zin van artikel 82 van deze verordening opleveren [zie in die zin arrest van 4 mei 2023, Österreichische Post (Immateriële schade ten gevolge van de verwerking van persoonsgegevens), C-300/21, ECLI:EU:C:2023:370, punt 50].

85. Wanneer een persoon die op grond daarvan schadevergoeding vordert, zich beroept op de vrees voor toekomstig misbruik van zijn persoonsgegevens wegens het bestaan van een dergelijke inbreuk, moet de aangezochte nationale rechter met name nagaan of deze vrees in de betrokken specifieke omstandigheden en ten aanzien van de betrokkene gegrond kan worden geacht.

86. Gelet op een en ander dient op de vijfde vraag te worden geantwoord dat artikel 82, lid 1, AVG aldus moet worden uitgelegd dat de vrees die een betrokkene na een inbreuk op deze verordening koestert voor mogelijk misbruik van zijn persoonsgegevens door derden, op zich "immateriële schade" in de zin van deze bepaling kan vormen.

Kosten

87. Ten aanzien van de partijen in het hoofdgeding is de procedure als een aldaar gerezen incident te beschouwen, zodat de verwijzende rechter over de kosten heeft te beslissen. De door anderen wegens indiening van hun opmerkingen bij het Hof gemaakte kosten komen niet voor vergoeding in aanmerking.

Het Hof (Derde kamer) verklaart voor recht:

1) De artikelen 24 en 32 van 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 en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming)
moeten aldus worden uitgelegd dat
het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens heeft plaatsgevonden door "derden" in de zin van artikel 4, punt 10, van deze verordening, op zich niet volstaat om aan te nemen dat de door de betrokken verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen niet "passend" waren in de zin van die artikelen 24 en 32.

2) Artikel 32 van verordening 2016/679
moet aldus worden uitgelegd dat
de vraag of de door de verwerkingsverantwoordelijke op grond van dit artikel getroffen technische en organisatorische maatregelen passend zijn, door de nationale rechterlijke instanties concreet moet worden beoordeeld, door rekening te houden met de aan de betrokken verwerking verbonden risico's en door te beoordelen of de aard, de inhoud en de uitvoering van die maatregelen afgestemd zijn op die risico's.

3) Het beginsel van verantwoordelijkheid van de verwerkingsverantwoordelijke, dat is geformuleerd in artikel 5, lid 2, van verordening 2016/679 en dat nader is uitgewerkt in artikel 24 ervan,
moet aldus worden uitgelegd dat
het in het kader van een vordering tot schadevergoeding op grond van artikel 82 van deze verordening aan de betrokken verwerkingsverantwoordelijke staat om aan te tonen dat de beveiligingsmaatregelen die hij op grond van artikel 32 van die verordening heeft getroffen, passend zijn.

4) Artikel 32 van verordening 2016/679 en het Unierechtelijke doeltreffendheidsbeginsel
moeten aldus worden uitgelegd dat
een deskundigenrapport geen systematisch noodzakelijk en toereikend bewijsmiddel kan vormen voor de beoordeling of de beveiligingsmaatregelen die de verwerkingsverantwoordelijke op grond van dat artikel heeft getroffen, passend zijn.

5) Artikel 82, lid 3, van verordening 2016/679
moet aldus worden uitgelegd dat
de verwerkingsverantwoordelijke niet van zijn verplichting uit hoofde van artikel 82, leden 1 en 2, van deze verordening tot vergoeding van de door een persoon geleden schade kan worden vrijgesteld op de enkele grond dat deze schade het gevolg is van het feit dat de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot

persoonsgegevens heeft plaatsgevonden door "derden" in de zin van artikel 4, punt 10, van die verordening. Die verantwoordelijke moet daartoe bewijzen dat hij op geen enkele wijze verantwoordelijk is voor het betrokken schadeveroorzakende feit.
6) Artikel 82, lid 1, van verordening 2016/679 moet aldus worden uitgelegd dat
de vrees die een betrokkene na een inbreuk op deze verordening koestert voor mogelijk misbruik van zijn persoonsgegevens door derden, op zich "immateriële schade" in de zin van deze bepaling kan vormen.

NOOT

Inleiding
1. In deze uitspraak beantwoordt het Hof van Justitie van de Europese Unie ('HvJ EU' of 'Hof') een aantal prejudiciële vragen over de verantwoordelijkheid en aansprakelijkheid van een verwerkingsverantwoordelijke naar aanleiding van een datalek. Het Hof geeft zowel verdere duiding aan de bewijslastverdeling met betrekking tot de vereiste beveiligingsmaatregelen, als aan de uitleg van het immateriële schadebegrip in de zin van art. 82 Verordening (EU) nr. 2016/679 ('AVG').
2. Deze uitspraak kan, ten aanzien van uitleg van het immateriële schadebegrip van art. 82 AVG, worden gezien als een vervolg op het arrest Österreichische Post AG (HvJ EU 4 mei 2023, ECLI:EU:C:2023:370, «JBP» 2023/101, m.nt. Walree (*Österreichische Post*)). In dat arrest gaf het Hof voor het eerst uitleg aan dit schadebegrip.
3. In deze noot geven we eerst een achtergrond van de zaak die aanleiding gaf tot het stellen van vijf prejudiciële vragen en daarna bespreken we achtereenvolgens de door het Hof gegeven antwoorden.

Achtergrond
4. De Natsionalna agentsia za prihodite (de belastingdienst van Bulgarije; hierna: de 'NAP') is getroffen door een hackaanval. Fiscale en sociale zekerheidsgegevens van meer dan zes miljoen betrokkenen zijn door hackers verkregen en op het internet gepubliceerd (hierna: het 'datalek'). Meerdere betrokkenen, waaronder 'VB', vorderen schadevergoeding van de NAP.
5. VB vordert op grond van art. 82 AVG een schadevergoeding van 1000 Bulgaarse leva (ongeveer € 510). VB stelt dat zij immateriële schade heeft geleden als gevolg van het datalek. Die schade bestaat uit de vrees voor toekomstig misbruik van haar persoonsgegevens en haar vrees dat zij slachtoffer kan worden van afpersing, agressie of ontvoering. Verdere bijzondere omstandigheden omtrent de persoon van de betrokkene zijn niet bekend.
6. Nadat de Bulgaarse bestuursrechter de vorderingen afwijst gaat VB in hoger beroep bij de hoogste bestuursrechter van Bulgarije, die vijf prejudiciële vragen aan het Hof stelt.

Datalek niet zonder meer een inbreuk op de AVG
7. De eerste vraag is of het feit dat de ongeoorloofde verstrekking van of toegang tot persoonsgegevens heeft plaatsgevonden door 'derden', op zich al genoeg is om aan te nemen dat de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen niet passend zijn in de zin van art. 24 en 32 AVG. Met andere woorden: betekent een succesvolle hackaanval automatisch dat de verwerkingsverantwoordelijke geen passende beveiligingsmaatregelen heeft getroffen?
8. Het Hof beantwoordt deze vraag ontkennend. Het Hof wijst erop dat dat de in art. 32 AVG opgenomen begrippen 'een op het risico afgestemd beveiligingsniveau' en 'passend beveiligingsniveau' erop duiden dat de AVG een risicobeheersysteem instelt en op geen enkele wijze beoogt de risico's van datalekken weg te nemen, waarbij uit de Engelse versie van het arrest duidelijker blijkt dat het Hof bedoelt: *geheel* weg te nemen (r.o. 29: 'that regulation establishes a risk management system and that it in no way purports to eliminate the risks of personal data breaches'). Het Hof vervolgt dat art. 24 en 32 AVG de verwerkingsverantwoordelijke alleen verplichten om beveiligingsmaatregelen te treffen die datalekken *zoveel mogelijk* moeten voorkomen. Deze uitleg is volgens het Hof des te meer geboden omdat de verwerkingsverantwoordelijke op grond van art. 24 AVG moet kunnen aantonen dat de getroffen beveiligingsmaatregelen passend waren. Deze mogelijkheid zou een verwerkingsverantwoordelijke worden ontnomen indien een onweerlegbaar vermoeden wordt aanvaard dat de maatregelen niet passend zijn indien een (succesvolle) externe hackaanval plaatsvindt.
9. Ten slotte (r.o. 33-38) wijst het Hof op enkele contextuele en teleologische elementen die deze

uitleg ondersteunen, waaronder overwegingen 74, 76, 83 en art. 82 lid 3 AVG, die kort gezegd eveneens verwijzen naar een risico-gebaseerde aanpak en aansprakelijkheid van de verwerkingsverantwoordelijke en verwerker kunnen uitsluiten, indien zij bewijzen op geen enkele wijze verantwoordelijk te zijn voor het schadeveroorzakende feit.
10. Het antwoord van het Hof is weinig verrassend. Algemeen wordt aangenomen dat de beveiligingsplicht uit de AVG (en diens voorloper, Richtlijn 95/46/EG) een inspanningsverplichting behelst, en geen resultaatsverplichting. Een andere uitleg zou in wezen voor de verwerkingsverantwoordelijke een risicoaansprakelijkheid voor hackaanvallen in het leven roepen.
11. De tweede vraag is hoe de nationale rechter moet beoordelen of de getroffen beveiligingsmaatregelen passend zijn in de zin van art. 32 AVG. Volgens het Hof moet de nationale rechter met betrekking tot een verwerking eerst vaststellen welk risico's een potentieel datalek kunnen meebrengen, en wat de gevolgen daarvan voor betrokkenen zouden zijn. Daarna moet de nationale rechter nagaan of de getroffen maatregelen zijn afgestemd op die risico's en mogelijke gevolgen. De nationale rechter moet dus niet alleen kijken welke beveiligingsmaatregelen zijn getroffen, maar ook een inhoudelijk onderzoek doen naar de getroffen maatregelen in het licht van de in art. 32 AVG genoemde omstandigheden (namelijk: stand van de techniek, uitvoeringskosten, alsmede de aard, omvang en context van de verwerkingsdoeleinden en de risico's voor betrokkenen), de omstandigheden van het geval en het bewijs waarover de rechter beschikt. Dat onderzoek vereist een concrete analyse van zowel de aard als de inhoud van de door de verwerkingsverantwoordelijke getroffen maatregelen, de toepassing en de praktische gevolgen ervan voor het beveiligingsniveau dat hij dient te waarborgen. Dit antwoord van het Hof sluit aan bij de risico-gebaseerde benadering van art. 32 AVG.

Bewijs(lastverdeling)
12. Het eerste deel van de derde vraag is of het in de context van een vordering tot schadevergoeding op grond van art. 82 AVG aan de verwerkingsverantwoordelijke is om aan te tonen dat de getroffen beveiligingsmaatregelen passend waren. Het Hof oordeelt dat dit het geval is. Het Hof komt tot deze uitleg door allereerst te wijzen op het accountability-beginsel van art. 5 lid 2 AVG, op grond waarvan de verwerkingsverantwoordelijke moet aantonen dat hij passende beveiligingsmaatregelen heeft getroffen (in de zin van art. 5 lid 1 sub f AVG). Dit beginsel is verder uitgewerkt in art. 24 en 32 AVG. Op basis daarvan oordeelt het Hof dat art. 5, 24 en 32 AVG een algemeen toepasselijke regel bevatten die, bij gebreke aan een andersluidende bepaling in de AVG, ook van toepassing is op art. 82 AVG. Ten slotte oordeelt het Hof ook dat deze uitleg steun vindt in de doelstelling van de AVG om een hoog beschermingsniveau van persoonsgegevens te waarborgen. Dit beschermingsniveau zou worden ondergraven indien de betrokkene bij een beroep op art. 82 AVG de bewijslast zou dragen met betrekking tot de passendheid van de beveiligingsmaatregelen. Advocaat-generaal (hierna: A-G) Pitruzzella wijst in zijn conclusie ook nog op het feit dat het voor betrokkenen in de praktijk bijna onmogelijk is om te bewijzen dat de maatregelen niet passend zijn, gelet op de informatieasymmetrie tussen de betrokkene en de verwerkingsverantwoordelijke (nr. 52, concl. A-G).
13. Dit oordeel van het Hof is wat ons betreft begrijpelijk en ook in lijn met eerdere jurisprudentie. Zo oordeelde het Hof al eerder dat de verwerkingsverantwoordelijke de bewijslast draagt met betrekking tot de naleving van de beginselen genoemd in art. 5 lid 1 AVG (HvJ EU 4 mei 2023, ECLI:EU:C:2023:373, r.o. 53 (*UZ/Bundesrepublik Deutschland*), met verwijzing naar HvJ EU 24 februari 2022, ECLI:EU:C:2022:124, r.o. 77, 78 en 81 (*Valsts ieņēmumu dienests*)).
14. Het oordeel van het Hof vormt naar Nederlands bewijsrecht een uitzondering op de hoofdregel die is neergelegd in art. 150 Rv. Volgens art. 150 Rv draagt de partij die zich beroept op rechtsgevolgen van door haar gestelde feiten of rechten daarvan de bewijslast, tenzij uit enige bijzondere regel of uit de eisen van redelijkheid en billijkheid een andere bewijslastverdeling voortvloeit. De in dit arrest van het Hof tot uitdrukking gekomen regel dat de verwerkingsverantwoordelijke de bewijslast draagt van de passendheid van de door hem getroffen beveiligingsmaatregelen in het kader van een beroep op schadevergoeding op grond van art. 82 AVG, vormt dus een bijzondere regel waaruit een andere bewijslastverdeling voortvloeit (vgl. rb. Amsterdam 15 maart 2023, ECLI:NL:RBAMS:2023:1407, «JOR» 2023/225, m.nt. Reus en Van der Kooij, r.o. 11.20

(*DPS/Meta*), ten aanzien van de AVG-transparantieverplichtingen). Zoals Walree opmerkt is het wel aan de betrokkene om gemotiveerd te stellen dat de verwerkingsverantwoordelijke een inbreuk heeft gemaakt op art. 32 AVG, maar draagt de verwerkingsverantwoordelijke vervolgens de bewijslast dat de beveiligingsmaatregelen passend waren (T.F. Walree, 'Datalek HAN; Annotatie bij Rechtbank Gelderland 4 oktober 2023', *TvI* 2024/1, p. 23).

15. Het tweede deel van de derde vraag is of uit art. 32 AVG en het Unierechtelijke doeltreffendheidsbeginsel volgt dat een deskundigenrapport een noodzakelijk en toereikend bewijsmiddel vormt om te beoordelen of de beveiligingsmaatregelen passend zijn. Het Hof merkt op dat de AVG geen voorschriften bevat over de toelating en de bewijskracht van een bewijsmiddel. Bij het ontbreken van dergelijke regels is het volgens vaste jurisprudentie van het Hof een zaak van de interne rechtsorde van de lidstaten om dergelijke regels vast te stellen, mits die regels voor EU-rechtelijke situaties niet ongunstiger zijn dan die welke voor soortgelijke situaties naar nationaal recht gelden (gelijkwaardigheidsbeginsel) en de uitoefening van de door het Unierecht verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel) (*Österreichische Post,* r.o. 53 en 54, met verwijzing naar HvJ EU 13 juli 2006, ECLI:EU:C:2006:461 (*Manfredi*), r.o. 92 en 98).

16. Het Hof beantwoordt dit deel van de vraag dan ook ontkennend. Het doeltreffendheidsbeginsel wordt volgens het Hof mogelijk geschonden als een deskundigenrapport systematisch 'noodzakelijk' zou zijn, omdat een dergelijk rapport overbodig kan zijn als er andere bewijsmiddelen voorhanden zijn, bijvoorbeeld als er een recente (onafhankelijke) audit is gedaan. Daarnaast acht het Hof het ook in strijd met vernoemd beginsel als de toevoeging van het woord 'toereikend' zou betekenen dat een nationale rechter uitsluitend of automatisch uit een deskundigenrapport afleidt of de beveiligingsmaatregelen passend zijn. Volgens het Hof moet de nationale rechter op onpartijdige en objectieve wijze beoordelen of de maatregelen passend zijn, en kan hij zich niet uitsluitend baseren op een deskundigenrapport.

17. Dit oordeel is begrijpelijk. Hoewel een rechter (doorgaans) geen uitgebreide technische kennis zal hebben over cybersecurity en het heel gebruikelijk is dat hiervoor een deskundige wordt ingeschakeld, blijft het aan de onpartijdige rechter om in het licht van alle omstandigheden te oordelen of de maatregelen passend zijn. Het beoordelingskader van art. 32 AVG is immers in hoge mate ook normatief, en niet uitsluitend technisch. De vraag van de verwijzende rechter was dus in die zin te strikt geformuleerd en zou ook naar Nederlands recht in strijd komen met het uitgangspunt van de vrije bewijswaardering door de rechter zoals vervat in art. 152 lid 2 Rv. De rechter is niet gebonden aan conclusies van deskundigen en de waardering van een deskundigenrapport is overgelaten aan zijn oordeel, waarbij hij een grote mate van vrijheid heeft (T&C Rv bij art. 198 Rv, aantekening 7).

Schadevergoeding

18. De vierde vraag is of art. 82 lid 3 AVG zo moet worden uitgelegd dat de verwerkingsverantwoordelijke is vrijgesteld van zijn verplichting tot schadevergoeding op de enkele grond dat een ongeoorloofde verstrekking van of toegang tot persoonsgegevens heeft plaatsgevonden door een 'derde'. Derden in de zin van de AVG zijn personen die geen medewerkers van de verwerkingsverantwoordelijke zijn en niet onder zijn toezicht staan.

19. Het Hof beantwoordt deze vraag ontkennend. Art. 82 lid 3 AVG bepaalt dat de verwerkingsverantwoordelijke niet aansprakelijk is als hij aantoont dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit. Volgens het Hof moeten de begrippen 'op geen enkele wijze' strikt worden beperkt tot de omstandigheden waarin de verwerkingsverantwoordelijke kan aantonen dat de schade niet aan hem kan worden toegerekend. Een hackaanval door derden kan in beginsel niet worden toegerekend aan de verwerkingsverantwoordelijke, tenzij hij de hackaanval mogelijk heeft gemaakt door een inbreuk op de AVG, bijvoorbeeld door het nalaten van het treffen van passende beveiligingsmaatregelen in de zin van art. 24 en 32 AVG. Het Hof voegt daaraan toe dat wanneer er sprake is van een hackaanval door een derde de verwerkingsverantwoordelijke niet aansprakelijk is op grond van art. 82 AVG, indien hij kan bewijzen dat er geen causaal verband bestaat tussen zijn eventuele inbreuk op de AVG en de door de betrokkene geleden schade (r.o. 72).

20. A-G Pitruzzella is op dit punt iets explicieter in zijn motivering en geeft een beschrijving van de aard van de aansprakelijkheid van art. 82 AVG, waarover debat was ontstaan in de literatuur (nr. 61, concl. A-G). De vraag was of art. 82 AVG dient te worden gekwalificeerd als een schuldaansprakelijkheid of een risicoaansprakelijkheid (Van der Jagt ging nog uit van een risicoaansprakelijkheid; zie: F.C. van der Jagt, 'Schadevergoeding onder de AVG', *MvV* 2019/7&8, p. 290). Volgens de A-G heeft art. 82 AVG het karakter van een verruimde aansprakelijkheid voor veronderstelde schuld. De betrokkene hoeft de toerekenbaarheid van de verwerkingsverantwoordelijke dus niet te bewijzen; die wordt vermoed (anders dan bij een reguliere schuldaansprakelijkheid). Maar de verwerkingsverantwoordelijke kan wel ontsnappen aan aansprakelijkheid als hij bewijst dat het schadeveroorzakende feit hem niet te verwijten valt (anders dan bij een risicoaansprakelijkheid). Ten aanzien van de toerekenbaarheid geldt dus in feite een omgekeerde bewijslast, in lijn met de bewijslast voor de passendheid van de beveiligingsmaatregelen. In een later arrest heeft het Hof deze uitgangspunten expliciet bevestigd (HvJ EU 21 december 2023, ECLI:EU:C:2023:1022, r.o. 94 en 103 (*Krankenversicherung Nordrhein*)).
21. De vijfde en meest interessante vraag is of de vrees van een betrokkene voor mogelijk misbruik van zijn persoonsgegevens immateriële schade in de zin van art. 82 AVG kan vormen. In Österreichische Post AG heeft het Hof al geoordeeld dat voor een beroep op schadevergoeding op grond van art. 82 AVG drie vereisten gelden: een inbreuk op de AVG, schade en causaal verband (*Österreichische Post,* r.o. 32). De loutere inbreuk opde AVG volstaat niet (*Österreichische Post*, r.o. 42). Daarnaast heeft Hof geoordeeld dat er voor het bestaan van immateriële schade geen drempel van een bepaalde ernst geldt. Ten slotte heeft het Hof overwogen dat de schadevergoeding op grond van art. 82 AVG een compensatoire functie heeft en geen punitieve functie (*Österreichische Post*, r.o. 58; herhaald in *Krankenversicherung Nordrhein*, r.o. 85).
22. Het Hof beantwoordt de vijfde vraag bevestigend. De vrees voor toekomstig misbruik kan dus immateriële schade vormen. Daarvoor stelt het Hof allereerst vast dat de bewoordingen van art. 82 AVG niet uitsluiten dat die vrees onder het begrip immateriële schade valt. Daarnaast motiveert het Hof zijn uitleg met een verwijzing naar overweging 146, waarin een ruime opvatting van het begrip schade wordt voorgestaan. Ook is in overweging 85 het enkele 'verlies van controle' over persoonsgegevens opgenomen als (mogelijk) nadelig gevolg van een datalek.
23. Het Hof merkt ten slotte echter op dat het aan de betrokkene is om te bewijzen dat de negatieve gevolgen ook immateriële schade in de zin van art. 82 AVG opleveren. Wanneer een betrokkene zich beroept op de vrees voor toekomstig misbruik van zijn persoonsgegevens als gevolg van een inbreuk op de AVG, moet de nationale rechter *met name* nagaan of deze vrees in de *specifieke omstandigheden* en *ten aanzien van de betrokkene* gegrond kan worden geacht.
24. Hiermee brengt het Hof tot uitdrukking dat de betrokkene zijn immateriële schade concreet en op zijn persoon toegespitst moet kunnen onderbouwen. De A-G was op dit punt nog iets helderder en formuleerde het als volgt: 'de betrokkene moet bewijzen dat de vrees voor misbruik hem in concreet en specifiek opzicht reële en zekere emotionele schade heeft berokkend' (concl. A-G, nr. 82). Dit maakt dat wij aannemen dat algemene stellingen van betrokkenen dat zij vrezen voor toekomstig misbruik van hun persoonsgegevens als gevolg van een datalek, zonder nadere onderbouwing, niet voldoende zullen zijn om immateriële schade aan te nemen.
25. De Nederlandse praktijk ten aanzien van immateriële schadevergoeding bij inbreuken op de AVG lijkt in lijn te zijn met het oordeel van het Hof. Op de voet van art. 6:106 aanhef en onder b BW en de invulling daarvan in het *EBI-arrest* (HR 15 maart 2019, ECLI:NL:HR:2019:376, *NJ* 2019/162*,* m.nt. Lindenbergh (*EBI*)) wordt beoordeeld of sprake is van een aantasting van de persoon op andere wijze, gelet op de aard en ernst van de normschending en de gevolgen daarvan, waarvan de betrokkene in beginsel de nadelige gevolgen met concrete gegevens moet onderbouwen, tenzij die nadelige gevolgen gelet op de aard en ernst van de normschending voor de hand liggen (voor een uitvoerige uiteenzetting van deze praktijk zie S.D. Lindenbergh & M.C. Samson, *NJB* 2023/1621; T.F.E. Tjong Tjin Tai, *NJ* 2023/244; T.F. Walree, 'Datalek HAN; Annotatie bij Rechtbank Gelderland 4 oktober 2023', *TvI* 2024/1). De Nederlandse praktijk vereist dus ook, in overeenstemming met dit arrest van het Hof, dat de betrokkene in beginsel de nadelige gevolgen van de inbreuk op de AVG moet onderbouwen (en moet

onderbouwen waarom die leiden tot immateriële schade). Een uitzondering hierop geldt als de nadelige gevolgen voor de hand liggen, wat tot nu toe is aangenomen in zaken waarbij bijzondere persoonsgegevens zijn gelekt (zie bijvoorbeeld: ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, «JBP» 2020/56, m.nt. Baas en Groen, r.o. 36 (*Pieter Baan Centrum*)). Dat voor het beoordelen van immateriële schade in een concreet geval rekening moet worden gehouden met iemands specifieke persoonlijke situatie, zoals psychische klachten, en dat dit kan leiden tot (grotere) immateriële schade, heeft de rechtbank Den Haag al eens geoordeeld (rb. Den Haag 21 september 2023, ECLI:NL:RBDHA:2023:14359 (*X/UWV*)).
26. In een arrest dat op dezelfde dag is gewezen heeft het Hof ook geoordeeld over het verlies van controle van persoonsgegevens. In dat arrest oordeelt het Hof dat de bekendmaking van persoonsgegevens op internet en het daaropvolgende verlies van zeggenschap daarover gedurende een korte tijdspanne immateriële schade kan veroorzaken, maar dat de betrokkene nog wel moet aantonen dat hij daadwerkelijk dergelijke schade heeft geleden, hoe miniem ook. De schade moet zich onderscheiden van de enkele inbreuk op de AVG (HvJ EU 14 december 2023, ECLI:EU:C:2023:988, r.o. 22 en 23 (*Gemeinde Ummendorf*)).
27. Voorts heeft het Hof in een nog recenter arrest geoordeeld dat een zuiver hypothetisch risico dat een onbevoegde derde misbruik zal maken van persoonsgegevens geen aanleiding kan geven tot (immateriële) schadevergoeding. Dat is het geval wanneer geen enkele derde kennis heeft genomen van de betreffende persoonsgegevens (HvJ EU 25 januari 2024, ECLI:EU:C:2024:72, r.o. 68-69 (*MediaMarktSaturn*)).

Conclusie
28. Wij sluiten deze noot af met de constatering dat het recht op (immateriële) schadevergoeding op grond van art. 82 AVG volop in ontwikkeling is. In een relatief korte tijdspanne zijn veel prejudiciële vragen door het Hof over dit onderwerp beantwoord.
29. Op basis van dit arrest is duidelijk dat het Hof vereist dat de betrokkene zijn vrees voor toekomstig misbruik van zijn persoonsgegevens concreet en op de persoon toegespitst moet onderbouwen, maar dat niet categorisch uitgesloten is dat een dergelijke vrees tot immateriële schade kan leiden. Wat ons betreft kan dit criterium ook breder worden toegepast op de onderbouwing van alle soorten immateriële schade als gevolg van een inbreuk op de AVG. Dit is ook in lijn met de Nederlandse praktijk, die vereist dat de betrokkene de nadelige gevolgen met concrete gegevens moet onderbouwen, tenzij de nadelige gevolgen gelet op de aard en ernst van de normschending voor de hand liggen.
30. De antwoorden van het Hof met betrekking tot de bewijslastverdeling bij de beoordeling van de passendheid van beveiligingsmaatregelen en de toerekenbaarheid in de zin van art. 82 AVG zijn goed te volgen. Duidelijk is dat de verwerkingsverantwoordelijke moet aantonen dat de beveiligingsmaatregelen passend waren als hij een (degelijk onderbouwde) schadeclaim van een betrokkene krijgt als gevolg van een datalek. Als een inbreuk op de AVG vervolgens wordt vastgesteld, wordt vermoed dat die inbreuk toerekenbaar is aan de verwerkingsverantwoordelijke, tenzij hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor de inbreuk. Al met al zijn we met dit arrest weer wat wijzer geworden.

mr. M. Moeskops
Advocaat bij Houthoff te Amsterdam.

mr. J.G. Reus
Advocaat bij Houthoff te Amsterdam.

33

Inzageverzoek onterecht afgewezen

Gemeenschappelijk Hof van Justitie van Aruba, Curaçao, Sint Maarten en van Bonaire, Sint Eustatius en Saba
16 februari 2024, AUA2023H00063, ECLI:NL:OGHACMB:2024:21
(mr. Bel, mr. Drop, mr. Soffers)

Inzageverzoek.

[Landsverordening administratieve rechtspraak art. 19, 20; Landsverordening persoonsregistraties art. 2, 4, 12; Landsverordening op het aanleggen en bijhouden van het bevolkingsregister art. 1, 2, 3; Kiesverordening art. 2, 6, 7]

Verzoeker heeft de Dienst Burgerlijke Stand en Bevolkingsregister (hierna: DBSB) verzocht om een kopie van alle sinds 2016 verwerkte persoonsgegevens met daarbij een toelichting, op grond van de Landsverordening persoonsregistraties (hierna: Lvp). DBSB heeft op het verzoek gereageerd met de mededeling dat de gegevens van verzoeker hoogstwaarschijnlijk zijn opgenomen in het bevolkingsregister op basis van de Landsverordening op het aanleggen en bijhouden van het bevolkingsregister (hierna: Lvb) en het Landsbesluit bevolkingsregister (hierna: Lbb). Volgens DBSB wordt het verzoek op grond van de Lvp om deze reden niet als de juiste weg beschouwd. In eerste aanleg heeft het Gerecht geoordeeld dat verzoeker niet correct werd gehoord in bezwaar, en dat de motivering van de bestreden beschikking van DBSB onvoldoende is.
In hoger beroep betoogt DBSB dat hem niet kan worden verweten dat verzoeker niet in bezwaar is gehoord, omdat de bezwaaradviescommissie de hoorzitting tot nader order heeft uitgesteld. Omdat de bezwaaradviescommissie de hoorzitting voor de tweede keer had uitgesteld, kon DBSB op het bezwaarschrift beschikken zonder dat het advies hoefde worden afgewacht. DBSB bood verzoeker tweemaal de gelegenheid om gehoord te worden, maar daarvan is geen gebruik gemaakt. Volgens het hof heeft het Gerecht in eerste aanleg terecht geoordeeld dat DBSB niet op verzoekers bezwaarschrift mocht beslissen zonder het advies van de bezwaaradviescommissie af te wachten, omdat geen van de uitzonderingsgronden in art. 17 lid 4 Landsverordening administratieve rechtspraak van toepassing was. Het Gerecht heeft de bestreden beschikking dan ook terecht vernietigd. Als laatste wordt door het hof de vraag beantwoord of DBSB heeft voldaan aan het verzoek. Dit is niet het geval. Op grond van art. 12 lid 2 Lvp geldt dat de houder van de persoonsgegevens de verzoeker een volledig overzicht verstrekt van de persoonsgegevens. Het slechts in globale zin vermelden welke typen persoonsgegevens worden gehouden zonder die persoonsgegevens daadwerkelijk te verstrekken, is daarmee in strijd. Het verzoek van verzoeker is niet gericht op het verkrijgen van een uittreksel, maar op een schriftelijk overzicht van zijn persoonsgegevens in het register van DBSB. Het hof oordeelt dat DBSB aan verzoeker een volledig overzicht moet verstrekken, inclusief informatie over de herkomst van de gegevens.

Het Hoofd van de Dienst Burgerlijke Stand en Bevolkingsregister (hierna: DBSB),
appellant,
tegen
de uitspraak van het Gerecht in eerste aanleg van Aruba (hierna: het Gerecht), van 15 maart 2023 in zaak nr. AUA202202297, in het geding tussen
[verzoeker]
en
DBSB.

Procesverloop
Bij beschikking van 23 december 2021 heeft DBSB geantwoord op een verzoek van [verzoeker] om toezending van een kopie van alle persoonsgegevens.
Bij beschikking van 14 juni 2022 heeft DBSB het door [verzoeker] daartegen gemaakte bezwaar ongegrond verklaard (hierna: bestreden beschikking).
Bij uitspraak van 15 maart 2023 heeft het Gerecht het door [verzoeker] daartegen ingestelde beroep gegrond verklaard, de bestreden beschikking vernietigd en bepaald dat DBSB binnen drie maanden opnieuw moet beschikken.
Tegen deze uitspraak heeft DBSB hoger beroep ingesteld.
[verzoeker] heeft een verweerschrift ingediend.