Samling af Afgørelser

DOMSTOLENS DOM (Tredje Afdeling)

14. december 2023*

»Præjudiciel forelæggelse – beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger – forordning (EU) 2016/679 – artikel 5 – principper for denne behandling – artikel 24 – den dataansvarliges ansvar – artikel 32 – foranstaltninger, der gennemføres for at sikre behandlingssikkerheden – vurdering af, om sådanne foranstaltninger er passende – domstolsprøvelsens rækkevidde – bevisførelse – artikel 82 – ret til erstatning og erstatningsansvar – eventuel ansvarsfritagelse for den dataansvarlige i tilfælde af en overtrædelse begået af tredjemand – påstand om erstatning for en immateriel skade støttet på frygten for et potentielt misbrug af personoplysninger«

I sag C-340/21,

angående en anmodning om præjudiciel afgørelse i henhold til artikel 267 TEUF, indgivet af Varhoven administrativen sad (øverste forvaltningsdomstol, Bulgarien) ved afgørelse af 14. maj 2021, indgået til Domstolen den 2. juni 2021, i sagen

VB

mod

Natsionalna agentsia za prihodite,

har

DOMSTOLEN (Tredje Afdeling),

sammensat af afdelingsformanden, K. Jürimäe, og dommerne N. Piçarra, M. Safjan, N. Jääskinen (refererende dommer) og M. Gavalec,

generaladvokat: G. Pitruzzella,

justitssekretær: A. Calot Escobar,

på grundlag af den skriftlige forhandling,

efter at der er afgivet indlæg af:

– Natsionalna agentsia za prihodite ved R. Spetsov,

* Processprog: bulgarsk.

– den bulgarske regering ved M. Georgieva og L. Zaharieva, som befuldmægtigede,

– den tjekkiske regering ved O. Serdula, M. Smolek og J. Vláčil, som befuldmægtigede,

– Irland ved Chief State Solicitor M. Browne samt A. Joyce, J. Quaney og M. Tierney, som befuldmægtigede, bistået af D. Fennelly, BL,

– den italienske regering ved G. Palmieri, som befuldmægtiget, bistået af avvocato dello Stato E. De Bonis,

– den portugisiske regering ved P. Barros da Costa, A. Pimenta, M.J. Ramos og C. Vieira Guerra, som befuldmægtigede,

– Europa-Kommissionen ved A. Bouchagiar, H. Kranenborg og N. Nikolova, som befuldmægtigede,

og efter at generaladvokaten har fremsat forslag til afgørelse i retsmødet den 27. april 2023,

afsagt følgende

Dom

1 Anmodningen om præjudiciel afgørelse vedrører fortolkningen af artikel 5, stk. 2, artikel 24 og 32 og artikel 82, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT 2016, L 119, s. 1, herefter »databeskyttelsesforordningen«).

2 Denne anmodning er blevet indgivet i forbindelse med en tvist mellem VB, der er en fysisk person, og Natsionalna agentsia za prihodite (det nationale agentur for offentlige indtægter, Bulgarien) (herefter »NAP«) vedrørende erstatningen for den immaterielle skade, som den nævnte person hævder at have lidt som følge af denne offentlige myndigheds angivelige tilsidesættelse af de lovbestemte forpligtelser, der påhviler den i dennes egenskab af ansvarlig for behandlingen af personoplysninger.

Retsforskrifter

3 4., 10., 11., 74., 76., 83., 85. og 146. betragtning til databeskyttelsesforordningen har følgende ordlyd:

»(4) […] Denne forordning overholder alle de grundlæggende rettigheder og følger de frihedsrettigheder og principper, der anerkendes i [Den Europæiske Unions charter om grundlæggende rettigheder] som forankret i traktaterne, navnlig respekten for privatliv og familieliv, hjem og kommunikation, beskyttelsen af personoplysninger, […] adgang til effektive retsmidler og til en retfærdig rettergang […].

[…]

(10) For at sikre et ensartet og højt niveau for beskyttelse af fysiske personer og for at fjerne hindringerne for udveksling af personoplysninger inden for [Den Europæiske Union] bør beskyttelsesniveauet for fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af sådanne oplysninger være ensartet i alle medlemsstater. Det bør sikres, at reglerne for beskyttelse af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger anvendes konsekvent og ensartet overalt i Unionen. […]

(11) For at sikre effektiv beskyttelse af personoplysninger i Unionen er det nødvendigt at styrke og præcisere de registreredes rettigheder og de forpligtelser, der påhviler dem, der behandler og træffer afgørelse om behandling af personoplysninger […].

[…]

(74) Der bør fastsættes bestemmelser om den dataansvarliges ansvar, herunder erstatningsansvar, for enhver behandling af personoplysninger, der foretages af den dataansvarlige eller på den dataansvarliges vegne. Den dataansvarlige bør navnlig have pligt til at gennemføre passende og effektive foranstaltninger og til at påvise, at behandlingsaktiviteter overholder denne forordning, herunder foranstaltningernes effektivitet. Disse foranstaltninger bør tage højde for behandlingens karakter, omfang, sammenhæng og formål og risikoen for fysiske personers rettigheder og frihedsrettigheder.

[…]

(76) Risikoens sandsynlighed og alvor for så vidt angår den registreredes rettigheder og frihedsrettigheder bør bestemmes med henvisning til behandlingens karakter, omfang, sammenhæng og formål. Risikoen bør evalueres på grundlag af en objektiv vurdering, hvorved det fastslås, om databehandlingsaktiviteter indebærer en risiko eller en høj risiko.

[…]

(83) For at opretholde sikkerheden og hindre behandling i strid med denne forordning bør den dataansvarlige eller databehandleren vurdere de risici, som en behandling indebærer, og gennemføre foranstaltninger, der kan begrænse disse risici, som f.eks. kryptering. Disse foranstaltninger bør under hensyntagen til det aktuelle tekniske niveau og implementeringsomkostningerne sikre et tilstrækkeligt sikkerhedsniveau, herunder fortrolighed, i forhold til risiciene og karakteren af de personoplysninger, der skal beskyttes. Ved vurderingen af datasikkerhedsrisikoen bør der tages hensyn til de risici, som behandling af personoplysninger indebærer, såsom hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, og som navnlig kan føre til fysisk, materiel eller immateriel skade.

[…]

(85) Et brud på persondatasikkerheden kan, hvis det ikke håndteres på en passende og rettidig måde, påføre fysiske personer fysisk, materiel eller immateriel skade, såsom tab af kontrol over deres personoplysninger eller begrænsning af deres rettigheder, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, uautoriseret ophævelse af pseudonymisering, skade på omdømme, tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt,

eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person. Så snart den dataansvarlige bliver bekendt med, at der er sket et brud på persondatasikkerheden, bør vedkommende derfor anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed uden unødig forsinkelse […]

[…]

(146) Den dataansvarlige eller databehandleren bør yde erstatning for enhver skade, som en person måtte lide som følge af behandling, der overtræder denne forordning. Den dataansvarlige eller databehandleren bør være fritaget for erstatningsansvar, hvis den pågældende beviser ikke at være ansvarlig for den forvoldte skade. Begrebet »skade« bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler formålene for denne forordning. Dette berører ikke eventuelle erstatningskrav for skade som følge af overtrædelse af andre bestemmelser i EU-retten eller medlemsstaternes nationale ret. Behandling, der overtræder denne forordning, omfatter også behandling, der overtræder delegerede retsakter og gennemførelsesretsakter vedtaget i henhold til denne forordning og til medlemsstaternes nationale ret, der præciserer bestemmelserne i denne forordning. Registrerede bør have fuld erstatning for den skade, som de har lidt. […]«

4 Denne forordnings artikel 4 med overskriften »Definitioner« bestemmer følgende:

»I denne forordning forstås ved:

1) »personoplysninger«: enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); […]

2) »behandling«: enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, […]

[…]

7) »dataansvarlig«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; […]

[…]

10) »tredjemand«: en anden fysisk eller juridisk person, offentlig myndighed eller institution eller ethvert andet organ end den registrerede, den dataansvarlige, databehandleren og de personer under den dataansvarliges eller databehandlerens direkte myndighed, der er beføjet til at behandle personoplysninger

[…]

12) »brud på persondatasikkerheden«: et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

[…]«

5 Den nævnte forordnings artikel 5 med overskriften »Principper for behandling af personoplysninger« fastsætter følgende:

»1. Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)

[…]

f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).«

6 Databeskyttelsesforordningens artikel 24 med overskriften »Den dataansvarliges ansvar« har følgende ordlyd:

»1. Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

2. Hvis det står i rimeligt forhold til behandlingsaktiviteter, skal de foranstaltninger, der er omhandlet i stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker.

3. Overholdelse af godkendte adfærdskodekser som omhandlet i artikel 40 eller godkendte certificeringsmekanismer som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af den dataansvarliges forpligtelser.«

7 Databeskyttelsesforordningens artikel 32, der har overskriften »Behandlingssikkerhed«, bestemmer følgende:

»1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger

b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

3. Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholde

[…]«

8 Denne forordnings artikel 79 med overskriften »Adgang til effektive retsmidler over for en dataansvarlig eller databehandler« bestemmer i stk. 1 følgende:

»Uden at det berører andre tilgængelige administrative eller udenretslige klageadgange, herunder retten til at indgive klage til en tilsynsmyndighed i henhold til artikel 77, skal den enkelte registrerede have adgang til effektive retsmidler, hvis vedkommende finder, at vedkommendes rettigheder i henhold til denne forordning er blevet krænket som følge af behandling af vedkommendes personoplysninger i strid med denne forordning.«

9 Den nævnte forordnings artikel 82 med overskriften »Ret til erstatning og erstatningsansvar« bestemmer i stk. 1-3 følgende:

»1. Enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren.

2. Enhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning. […]

3. En dataansvarlig eller databehandler er fritaget for erstatningsansvar i henhold til stk. 2, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden.«

Tvisten i hovedsagen og de præjudicielle spørgsmål

10 NAP er en myndighed, der er tilknyttet den bulgarske finansminister. Inden for rammerne af sine opgaver, der bl.a. består i identificering, sikring og inddrivelse af offentlige fordringer, er dette agentur ansvarlig for behandling af personoplysninger som omhandlet i databeskyttelsesforordningens artikel 4, nr. 7).

11 Den 15. juli 2019 afslørede medierne, at en uautoriseret adgang til NAP's IT-system havde fundet sted, og at en række personoplysninger indeholdt i dette system som følge af dette cyberangreb var blevet offentliggjort på internettet.

12 Over seks millioner fysiske personer, der var bulgarske eller udenlandske statsborgere, var berørt af disse begivenheder. Nogle hundrede af disse, herunder sagsøgeren i hovedsagen, anlagde søgsmål mod NAP med påstand om erstatning for immaterielle skader som følge af videregivelsen af deres personoplysninger.

13 I denne sammenhæng anlagde sagsøgeren i hovedsagen søgsmål ved Administrativen sad Sofia-grad (forvaltningsdomstolen i Sofia, Bulgarien) med påstand om, at NAP skulle betale hende et beløb på 1 000 bulgarske leva (BGN) (ca. 510 EUR) i erstatning på grundlag af databeskyttelsesforordningens artikel 82 og bestemmelser i bulgarsk ret. Til støtte for denne påstand gjorde hun gældende, at hun havde lidt en immateriel skade som følge af et brud på persondatasikkerheden som omhandlet i databeskyttelsesforordningens artikel 4, nr. 12), nærmere bestemt et brud på sikkerheden, der var fremkaldt af, at NAP havde tilsidesat sine forpligtelser i henhold til bl.a. denne forordnings artikel 5, stk. 1, litra f), og artikel 24 og 32. Hendes immaterielle skade bestod i frygten for, at hendes personoplysninger, der var blevet offentliggjort uden hendes samtykke, skulle blive misbrugt i fremtiden, eller for, at hun selv skulle blive udsat for afpresning, overfald eller endog bortførelse.

14 Til sit forsvar gjorde NAP indledningsvis gældende, at sagsøgeren i hovedsagen ikke havde anmodet dette agentur om informationer angående de præcise oplysninger, der var blevet videregivet. Dernæst fremlagde NAP en række dokumenter med henblik på at bevise, at agenturet havde truffet alle de nødvendige foranstaltninger, såvel forudgående for at forebygge et brud på datasikkerheden i forhold til de personoplysninger, der var indeholdt i dets IT-system, som efterfølgende for at begrænse virkningerne af dette brud og for at berolige borgerne. Desuden var der ifølge NAP ingen årsagsforbindelse mellem den hævdede immaterielle skade og det nævnte brud. Endelig anførte NAP, at eftersom dette agentur selv havde været udsat for en ondsindet angreb fra personer, der ikke var dets ansatte, kunne det ikke holdes ansvarligt for skadevirkningerne af dette angreb.

15 Ved afgørelse af 27. november 2020 frifandt Administrativen sad Sofia-grad (forvaltningsdomstolen i Sofia) NAP i det af sagsøgeren i hovedsagen anlagte søgsmål. Denne ret udtalte for det første, at den uautoriserede adgang til NAP's database skyldtes et hackerangreb begået af tredjemand, og for det andet, at sagsøgeren i hovedsagen ikke havde bevist, at NAP havde udvist forsømmelse med hensyn til vedtagelsen af sikkerhedsforanstaltninger. Endvidere fandt retten, at denne sagsøger ikke havde lidt nogen immateriel skade, der gav ret til erstatning.

16 Sagsøgeren i hovedsagen har iværksat kassationsanke til prøvelse af denne afgørelse ved Varhoven administrativen sad (øverste forvaltningsdomstol, Bulgarien), som er den forelæggende ret i den foreliggende sag. Hun har til støtte for sin appel gjort gældende, at retten i første instans har begået en retlig fejl ved fordelingen af bevisbyrden vedrørende de af NAP trufne sikkerhedsforanstaltninger, og at dette agentur ikke har påvist, at det ikke har udvist forsømmelse i denne forbindelse. Sagsøgeren i hovedsagen har desuden gjort gældende, at frygten for muligt misbrug af hendes personoplysninger i fremtiden udgør en reel og ikke hypotetisk immateriel skade. Til sit forsvar har NAP anfægtet hvert af disse argumenter.

17 Den forelæggende ret har indledningsvis nævnt muligheden for, at konstateringen af, at der er sket et brud på persondatasikkerheden, i sig selv gør det muligt at konkludere, at de foranstaltninger, som den dataansvarlige for disse oplysninger, har gennemført, ikke var »passende« som omhandlet i databeskyttelsesforordningens artikel 24 og 32.

18 Såfremt denne konstatering er utilstrækkelig til at nå frem til en sådan konklusion, er den forelæggende ret imidlertid i tvivl om dels rækkevidden af den prøvelse, som de nationale retter skal foretage for at vurdere, om de omhandlede foranstaltninger er passende, dels de regler om bevisførelse, der skal anvendes i denne forbindelse, både med hensyn til bevisbyrden og bevismidlerne, navnlig når der ved disse retter anlægges et erstatningssøgsmål på grundlag af databeskyttelsesforordningens artikel 82.

19 Dernæst ønsker den forelæggende ret oplyst, om den omstændighed, at bruddet på persondatasikkerheden skyldes en handling begået af tredjemand, i det foreliggende tilfælde et cyberangreb, i henhold til databeskyttelsesforordningens artikel 82, stk. 3, udgør en faktor, der systematisk fritager den dataansvarlige for disse oplysninger for sit ansvar for den skade, der er påført den registrerede.

20 Endelig ønsker den forelæggende ret oplyst, om en persons frygt for, at dennes personoplysninger vil kunne blive misbrugt i fremtiden – i det foreliggende tilfælde som følge af en uautoriseret adgang til disse oplysninger og cyberkriminelles videregivelse af oplysningerne – i sig selv kan udgøre en »immateriel skade« som omhandlet i databeskyttelsesforordningens artikel 82, stk. 1. I bekræftende fald ville denne person være fritaget for at godtgøre, at tredjemand forud for vedkommendes erstatningskrav har gjort ulovlig brug af disse oplysninger, såsom ved misbrug af dennes identitet.

21 På denne baggrund har Varhoven administrativen sad (øverste forvaltningsdomstol) besluttet at udsætte sagen og at forelægge Domstolen følgende præjudicielle spørgsmål:

»1) Skal [databeskyttelsesforordningens] artikel 24 og 32 […] fortolkes således, at det forhold, at en uautoriseret videregivelse eller en uautoriseret adgang til personoplysninger som omhandlet i [databeskyttelsesforordningens] artikel 4, nr. 12), […] er blevet foretaget af personer, som ikke er ansatte i den dataansvarliges administration og ikke er undergivet dennes kontrol, er tilstrækkeligt til at lægge til grund, at de iværksatte tekniske og organisatoriske foranstaltninger ikke er passende?

2) Såfremt det første spørgsmål besvares benægtende, hvilken genstand og hvilket omfang skal rettens legalitetskontrol da have ved vurderingen af, om de tekniske og organisatoriske foranstaltninger, som den dataansvarlige har truffet som omhandlet i [databeskyttelsesforordningens] artikel 32 […], er passende?

3) Såfremt det første spørgsmål besvares benægtende, skal ansvarlighedsprincippet som omhandlet i [databeskyttelsesforordningens] artikel 5, stk. 2, og artikel 24 […], sammenholdt med 74. betragtning hertil, da fortolkes således, at bevisbyrden for, at de iværksatte tekniske og organisatoriske foranstaltninger som omhandlet i [samme forordnings] artikel 32 […] er passende, påhviler den dataansvarlige i forbindelse med et søgsmål i henhold til forordningens artikel 82, stk. 1?

Kan indhentningen af en sagkyndig udtalelse anses for et bevismiddel, der er nødvendigt for og tilstrækkeligt til at fastslå, om de tekniske og organisatoriske foranstaltninger, som den dataansvarlige har truffet, i en sag som den foreliggende var passende, hvis den uautoriserede adgang til og den uautoriserede videregivelse af personoplysninger skyldtes et »hackerangreb«?

4) Skal [databeskyttelsesforordningens] artikel 82, stk. 3, […] fortolkes således, at den uautoriserede videregivelse af eller den uautoriserede adgang til personoplysninger som omhandlet i [databeskyttelsesforordningens] artikel 4, nr. 12), […] som i den foreliggende sag gennem et »hackerangreb« udført af personer, der ikke er ansatte i den dataansvarliges administration og ikke er undergivet dennes kontrol, udgør en omstændighed, som den dataansvarlige ikke er skyld i, og som kan begrunde en fritagelse for erstatningsansvar?

5) Skal [databeskyttelsesforordningens] artikel 82, stk. 1 og 2, […] sammenholdt med 85. og 146. betragtning hertil, fortolkes således, at det i en sag som den foreliggende, hvor tilsidesættelsen af beskyttelsen af personoplysninger kommer til udtryk ved en uautoriseret adgang til og formidling af personoplysninger gennem et »hackerangreb«, kun er den berørte persons bekymringer, frygt og angst for et muligt fremtidigt misbrug af personoplysninger, der er omfattet af begrebet immateriel skade, som skal fortolkes bredt, og dermed berettiger til erstatning, hvis der ikke er blevet konstateret et sådant misbrug og/eller den berørte person ikke er blevet påført nogen yderligere skade?«

Om de præjudicielle spørgsmål

Det første spørgsmål

22 Med sit første spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om databeskyttelsesforordningens artikel 24 og 32 skal fortolkes således, at en uautoriseret videregivelse af, eller en uautoriseret adgang til, personoplysninger foretaget af »tredjemand« som omhandlet i denne forordnings artikel 4, nr. 10), i sig selv er tilstrækkelig til at fastslå, at de tekniske og organisatoriske foranstaltninger, som den omhandlede dataansvarlige har truffet, ikke var »passende« som omhandlet i denne artikel 24 og 32.

23 Indledningsvis skal det bemærkes, at ifølge fast retspraksis skal ordlyden af en bestemmelse i EU-retten, der som databeskyttelsesforordningens artikel 24 og 32 ikke indeholder nogen udtrykkelig henvisning til medlemsstaternes ret med henblik på at fastlægge dens betydning og rækkevidde, normalt undergives en selvstændig og ensartet fortolkning i hele Unionen, som skal søges under hensyntagen til bl.a. den omhandlede bestemmelses affattelse, de formål, der forfølges med bestemmelsen, og den sammenhæng, hvori den indgår (jf. i denne retning dom af 18.1.1984, Ekro, 327/82, EU:C:1984:11, præmis 11, af 1.10.2019, Planet49, C-673/17, EU:C:2019:801, præmis 47 og 48, og af 4.5.2023, Österreichische Post (Immateriel skade i forbindelse med behandling af personoplysninger), C-300/21, EU:C:2023:370, præmis 29).

24 I første række og hvad angår affattelsen af de relevante bestemmelser skal det bemærkes, at databeskyttelsesforordningens artikel 24 fastsætter en generel forpligtelse for den dataansvarlige til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandlingen af personoplysninger er i overensstemmelse med denne forordning.

25 Med henblik herpå opregnes i databeskyttelsesforordningens artikel 24, stk. 1, en række kriterier, der skal tages hensyn til ved vurderingen af sådanne foranstaltningers hensigtsmæssighed, nemlig behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder. Det tilføjes i denne bestemmelse, at de nævnte foranstaltninger om nødvendigt skal revideres og ajourføres.

26 I dette perspektiv præciserer databeskyttelsesforordningens artikel 32 den dataansvarliges og en eventuel databehandlers forpligtelser med hensyn til sikkerheden omkring denne behandling. Denne artikels stk. 1 bestemmer således, at den dataansvarlige og databehandleren skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er nævnt i nærværende doms foregående præmis, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål.

27 Det fremgår ligeledes af den nævnte artikels stk. 2, at der ved vurderingen af, hvilket sikkerhedsniveau der er passende, navnlig skal tages hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

28 Desuden er det angivet i både denne forordnings artikel 24, stk. 3, og artikel 32, stk. 3, at den dataansvarlige eller databehandleren kan påvise, at vedkommende har opfyldt kravene i disse artiklers stk. 1, ved at basere sig på, at vedkommende overholder et godkendt adfærdskodeks eller en godkendt certificeringsmekanisme, jf. den nævnte forordnings artikel 40 og 42.

29 Henvisningen i databeskyttelsesforordningens artikel 32, stk. 1 og 2, til »et sikkerhedsniveau, der passer til disse risici« og et »sikkerhedsniveau[,] der er passende« vidner om, at der med denne forordning indføres en risikostyringsordning, og at det på ingen måde hævdes, at risiciene for brud på persondatasikkerheden fjernes.

30 Det fremgår således af affattelsen af databeskyttelsesforordningens artikel 24 og 32, at disse bestemmelser begrænser sig til at pålægge den dataansvarlige at vedtage tekniske og organisatoriske foranstaltninger med henblik på i videst muligt omfang at undgå ethvert brud på persondatasikkerheden. Spørgsmålet om, hvorvidt sådanne foranstaltninger er passende, skal vurderes konkret, idet det skal undersøges, om den dataansvarlige har gennemført disse foranstaltninger under hensyntagen til de forskellige kriterier, der er omhandlet i de nævnte artikler, og til de behov for databeskyttelse, der specifikt er forbundet med den pågældende behandling, samt til de risici, som denne behandling indebærer.

31 Databeskyttelsesforordningens artikel 24 og 32 kan derfor ikke forstås således, at en uautoriseret videregivelse af, eller en uautoriseret adgang til, personoplysninger foretaget af tredjemand er tilstrækkelig til at konkludere, at de foranstaltninger, som den pågældende dataansvarlige har truffet, ikke var passende som omhandlet i disse bestemmelser, uden at det overhovedet gøres muligt for sidstnævnte at føre bevis for det modsatte.

32 En sådan fortolkning gælder så meget desto mere, som databeskyttelsesforordningens artikel 24 udtrykkeligt fastsætter, at den dataansvarlige skal kunne påvise, at de foranstaltninger, som vedkommende har gennemført, er i overensstemmelse med denne forordning, hvilken mulighed den dataansvarlige ville blive frataget, hvis en uafkræftelig formodning blev anerkendt.

33 I anden række understøtter elementer angående sammenhæng og formål denne fortolkning af databeskyttelsesforordningens artikel 24 og 32.

34 Hvad for det første angår den sammenhæng, hvori disse to artikler indgår, skal det bemærkes, at det fremgår af databeskyttelsesforordningens artikel 5, stk. 2, at den dataansvarlige skal kunne påvise, at vedkommende har overholdt de principper for behandling af personoplysninger, der er fastsat i denne artikels stk. 1. Denne forpligtelse gentages og præciseres i denne forordnings

artikel 24, stk. 1 og 3, og artikel 32, stk. 3, for så vidt angår forpligtelsen til at gennemføre tekniske og organisatoriske foranstaltninger for at beskytte sådanne oplysninger i forbindelse med den behandling, som denne dataansvarlige foretager. En sådan forpligtelse til at påvise, at disse foranstaltninger er passende, ville imidlertid ikke give mening, hvis den dataansvarlige var forpligtet til at forhindre ethvert brud på datasikkerheden i forhold til de nævnte oplysninger.

35 Det betones endvidere i 74. betragtning til databeskyttelsesforordningen, at den dataansvarlige bør have pligt til at gennemføre passende og effektive foranstaltninger og til at påvise, at behandlingsaktiviteter overholder denne forordning, herunder foranstaltningernes effektivitet, og at disse foranstaltninger bør tage højde for de kriterier, der er knyttet til den pågældende behandlings karakteristika og den risiko, som den udgør, hvilke kriterier også er fastsat i forordningens artikel 24 og 32.

36 Det fremgår ligeledes af 76. betragtning til denne forordning, at risikoens sandsynlighed og alvor afhænger af den pågældende behandlings særlige karakter, og at denne risiko bør evalueres på grundlag af en objektiv vurdering.

37 Det følger i øvrigt af databeskyttelsesforordningens artikel 82, stk. 2 og 3, at selv om en dataansvarlig hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning, er den pågældende ikke desto mindre fritaget for erstatningsansvar, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden.

38 For det andet bekræftes den fortolkning, der er anlagt i nærværende doms præmis 31, også af 83. betragtning til databeskyttelsesforordningen, hvor det i første punktum er angivet, at »[f]or at opretholde sikkerheden og hindre behandling i strid med denne forordning bør den dataansvarlige eller databehandleren vurdere de risici, som en behandling indebærer, og gennemføre foranstaltninger, der kan begrænse disse risici«. Herved har EU-lovgiver tilkendegivet sin hensigt om at »begrænse« risiciene for brud på persondatasikkerheden uden at hævde, at det ville være muligt at fjerne dem.

39 Henset til ovenstående begrundelser skal det første spørgsmål besvares med, at databeskyttelsesforordningens artikel 24 og 32 skal fortolkes således, at en uautoriseret videregivelse af, eller en uautoriseret adgang til, personoplysninger foretaget af »tredjemand« som omhandlet i denne forordnings artikel 4, nr. 10), ikke i sig selv er tilstrækkelig til at fastslå, at de tekniske og organisatoriske foranstaltninger, som den omhandlede dataansvarlige har truffet, ikke var »passende« som omhandlet i denne artikel 24 og 32.

Det andet spørgsmål

40 Med sit andet spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om databeskyttelsesforordningens artikel 32 skal fortolkes således, at spørgsmålet om, hvorvidt de tekniske og organisatoriske foranstaltninger, som den dataansvarlige i henhold til denne artikel har truffet, er passende, skal vurderes konkret af de nationale retsinstanser under hensyntagen til bl.a. de risici, der er forbundet med den pågældende behandling.

41 Det skal i denne forbindelse påpeges, at databeskyttelsesforordningens artikel 32 – som fremhævet under besvarelsen af det første spørgsmål – kræver, at den dataansvarlige og, alt efter tilfældet, databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene, under hensyntagen til de vurderingskriterier,

der er angivet i artiklens stk. 1. Desuden gives i databeskyttelsesforordningens artikel 32, stk. 2, en ikke-udtømmende opregning af et vist antal faktorer, der er relevante for vurderingen af det passende sikkerhedsniveau i forhold til de risici, som den pågældende behandling frembyder.

42 Det fremgår af den nævnte artikel 32, stk. 1 og 2, at det skal vurderes i to faser, om sådanne tekniske og organisatoriske foranstaltninger er passende. For det første skal der ske en identificering af de risici for brud på persondatasikkerheden, der følger af den pågældende behandling, og deres eventuelle konsekvenser for fysiske personers rettigheder og frihedsrettigheder. Denne vurdering skal foretages konkret under hensyntagen til, hvor sandsynlige og alvorlige de identificerede risici er. For det andet skal det efterprøves, om de foranstaltninger, som den dataansvarlige har gennemført, er tilpasset disse risici under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og denne behandlings karakter, omfang, sammenhæng og formål.

43 Den dataansvarlige har ganske vist en vis skønsmargen til at fastlægge de passende tekniske og organisatoriske foranstaltninger med henblik på at sikre et sikkerhedsniveau, der passer til disse risici, således som det kræves i henhold til databeskyttelsesforordningens artikel 32, stk. 1. Det forholder sig ikke desto mindre således, at en national ret skal kunne evaluere den komplekse vurdering, som den dataansvarlige har foretaget, og herved sikre sig, at de foranstaltninger, som sidstnævnte har truffet, er egnede til at sikre et sådant sikkerhedsniveau.

44 En sådan fortolkning kan i øvrigt sikre dels effektiviteten af den beskyttelse af personoplysninger, som betones i 11. og 74. betragtning til denne forordning, dels den adgang til effektive retsmidler over for en dataansvarlig, som er beskyttet ved den nævnte forordnings artikel 79, stk. 1, sammenholdt med 4. betragtning til samme forordning.

45 For at efterprøve, om de tekniske og organisatoriske foranstaltninger, der er gennemført i henhold til databeskyttelsesforordningens artikel 32, er passende, skal en national ret derfor ikke begrænse sig til at fastslå, på hvilken måde den pågældende dataansvarlige har haft til hensigt at opfylde sine forpligtelser i henhold til denne artikel, men foretage en materiel undersøgelse af disse foranstaltninger ud fra alle de kriterier, der er nævnt i denne artikel, samt de særlige omstændigheder i den konkrete sag og de beviser, som denne ret råder over i denne henseende.

46 En sådan undersøgelse kræver, at der foretages en konkret analyse af både arten og indholdet af de foranstaltninger, som den dataansvarlige har gennemført, af den måde, hvorpå disse foranstaltninger er blevet gennemført, og af deres praktiske indvirkninger på det sikkerhedsniveau, som den dataansvarlige var forpligtet til at sikre, henset til de risici, der er forbundet med denne behandling.

47 Følgelig skal det andet spørgsmål besvares med, at databeskyttelsesforordningens artikel 32 skal fortolkes således, at spørgsmålet om, hvorvidt de tekniske og organisatoriske foranstaltninger, som den dataansvarlige i henhold til denne artikel har truffet, er passende, skal vurderes konkret af de nationale retsinstanser under hensyntagen til de risici, der er forbundet med den pågældende behandling, og idet de skal vurdere, om arten, indholdet og gennemførelsen af disse foranstaltninger er tilpasset disse risici.

Det tredje spørgsmål

Det tredje spørgsmåls første del

48 Med sit tredje spørgsmåls første del ønsker den forelæggende ret nærmere bestemt oplyst, om princippet om den dataansvarliges ansvar, der er fastsat i databeskyttelsesforordningens artikel 5, stk. 2, og konkretiseret i denne forordnings artikel 24, skal fortolkes således, at den dataansvarlige i forbindelse med et erstatningssøgsmål på grundlag af denne forordnings artikel 82 bærer bevisbyrden for, at de sikkerhedsforanstaltninger, som vedkommende har gennemført i henhold til den nævnte forordnings artikel 32, er passende.

49 I denne henseende skal det i første række bemærkes, at databeskyttelsesforordningens artikel 5, stk. 2, opstiller et princip om ansvar, hvorefter den dataansvarlige er ansvarlig for at overholde de principper for behandling af personoplysninger, der er fastsat i forordningens artikel 5, stk. 1, og bestemmer, at den dataansvarlige skal kunne påvise, at disse principper overholdes.

50 I henhold til princippet om personoplysningers integritet og fortrolighed, der er fastsat i denne forordnings artikel 5, stk. 1, litra f), skal den dataansvarlige navnlig sikre, at sådanne oplysninger behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger, og den dataansvarlige skal kunne påvise, at dette princip overholdes.

51 Det skal ligeledes bemærkes, at såvel databeskyttelsesforordningens artikel 24, stk. 1, læst i lyset af 74. betragtning hertil, som denne forordnings artikel 32, stk. 1, pålægger den dataansvarlige i forbindelse med enhver behandling af personoplysninger, der foretages af den pågældende selv eller på dennes vegne, at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og være i stand til at påvise, at behandlingen foretages i overensstemmelse med den nævnte forordning.

52 Det fremgår utvetydigt af ordlyden af databeskyttelsesforordningens artikel 5, stk. 2, artikel 24, stk. 1, og artikel 32, stk. 1, at bevisbyrden for, at personoplysningerne behandles på en måde, der sikrer tilstrækkelig sikkerhed for disse oplysninger som omhandlet i denne forordnings artikel 5, stk. 1, litra f), og artikel 32, påhviler den pågældende dataansvarlige (jf. analogt dom af 4.5.2023, Bundesrepublik Deutschland (Domstolenes elektroniske postkasse), C-60/22, EU:C:2023:373, præmis 52 og 53, og af 4.7.2023, Meta Platforms m.fl. (Almindelige betingelser for anvendelse af et socialt netværk), C-252/21, EU:C:2023:537, præmis 95).

53 Disse tre artikler fastsætter således en regel, der finder generel anvendelse, og som i mangel af oplysninger om det modsatte i databeskyttelsesforordningen ligeledes skal anvendes i forbindelse med et erstatningssøgsmål på grundlag af denne forordnings artikel 82.

54 I anden række skal det fastslås, at den ovenstående ordlydsfortolkning understøttes af en hensyntagen til de formål, der forfølges med databeskyttelsesforordningen.

55 Eftersom det beskyttelsesniveau, der tilstræbes med databeskyttelsesforordningen, afhænger af de sikkerhedsforanstaltninger, som de dataansvarlige for personoplysningerne træffer, skal disse, ved at de bærer bevisbyrden for, at disse foranstaltninger er passende, for det første tilskyndes til at gøre alt, hvad der står i deres magt, for at forebygge, at der finder behandlingsaktiviteter sted, som ikke er i overensstemmelse med denne forordning.

56 Hvis det blev lagt til grund, at bevisbyrden for de nævnte foranstaltningers passende karakter påhvilede de registrerede, således som disse er defineret i databeskyttelsesforordningens artikel 4, nr. 1), ville resultatet heraf for det andet blive, at den i samme forordnings artikel 82, stk. 1, fastsatte ret til erstatning ville miste en stor del af sin effektive virkning, på trods af, at EU-lovgiver har ønsket at styrke både disse personers rettigheder og de dataansvarliges forpligtelser i forhold til de bestemmelser, der gjaldt forud for denne forordning, således som angivet i 11. betragtning hertil.

57 Det tredje spørgsmåls første del skal derfor besvares med, at princippet om den dataansvarliges ansvar, der er fastsat i databeskyttelsesforordningens artikel 5, stk. 2, og konkretiseret i denne forordnings artikel 24, skal fortolkes således, at den dataansvarlige i forbindelse med et erstatningssøgsmål på grundlag af denne forordnings artikel 82 bærer bevisbyrden for, at de sikkerhedsforanstaltninger, som vedkommende har gennemført i henhold til den nævnte forordnings artikel 32, er passende.

Det tredje spørgsmåls anden del

58 Med sit tredje spørgsmåls anden del ønsker den forelæggende ret nærmere bestemt oplyst, om databeskyttelsesforordningens artikel 32 og det EU-retlige effektivitetsprincip skal fortolkes således, at en retsligt udmeldt sagkyndig udtalelse udgør et bevismiddel, der er nødvendigt for og tilstrækkeligt til at vurdere, om de sikkerhedsforanstaltninger, som den dataansvarlige har gennemført i henhold til denne artikel, er passende.

59 I denne henseende bemærkes, at det fremgår af fast retspraksis, at det i mangel af EU-retlige bestemmelser på området i medfør af princippet om procesautonomi tilkommer hver enkelt medlemsstat i sin interne retsorden at regulere de processuelle aspekter vedrørende sagsanlæg til sikring af beskyttelsen af borgernes rettigheder, dog på den betingelse, at de pågældende regler ikke i situationer, der hører under EU-retten, er mindre gunstige end dem, som regulerer tilsvarende situationer, der er underlagt national ret (ækvivalensprincippet), og at de i praksis ikke umuliggør eller uforholdsmæssigt vanskeliggør udøvelsen af rettigheder, der er tillagt ved EU-retten (effektivitetsprincippet) (dom af 4.5.2023, Österreichische Post (Immateriel skade i forbindelse med behandling af personoplysninger), C-300/21, EU:C:2023:370, præmis 53 og den deri nævnte retspraksis).

60 I det foreliggende tilfælde skal det bemærkes, at databeskyttelsesforordningen ikke fastsætter nogen regler om anerkendelse og bevisværdi af et bevismiddel, såsom en retsligt udmeldt sagkyndig udtalelse, som skal anvendes af de nationale retter, for hvilke der er anlagt et erstatningssøgsmål på grundlag af denne forordnings artikel 82, og som i henhold til forordningens artikel 32 skal vurdere, om de sikkerhedsforanstaltninger, som den pågældende dataansvarlige har gennemført, er passende. I overensstemmelse med, hvad der er påpeget i nærværende doms foregående præmis, gælder det følgelig, at når der ikke findes EU-retlige regler på området, tilkommer det hver enkelt medlemsstat i sin nationale retsorden at fastsætte de nærmere regler for sager til sikring af beskyttelsen af borgernes rettigheder i henhold til artikel 82, og navnlig at fastsætte reglerne for de bevismidler, der gør det muligt at vurdere, om sådanne foranstaltninger i denne sammenhæng er passende, idet de nævnte principper om ækvivalens og effektivitet skal overholdes (jf. analogt dom af 21.6.2022, Ligue des droits humains, C-817/19, EU:C:2022:491, præmis 297, og 4.5.2023, Österreichische Post (Immateriel skade i forbindelse med behandling af personoplysninger), C-300/21, EU:C:2023:370, præmis 54).

61 I den foreliggende sag råder Domstolen ikke over nogen oplysninger, der kan give anledning til tvivl om, hvorvidt ækvivalensprincippet er overholdt. Det forholder sig anderledes med hensyn til overholdelsen af effektivitetsprincippet, for så vidt som selve ordlyden af det tredje spørgsmåls anden del præsenterer brugen af en sagkyndig udtalelse som et »bevismiddel, der er nødvendigt […] og tilstrækkeligt […]«.

62 Navnlig kan en national procedureregel, hvorefter det er systematisk »nødvendigt«, at de nationale retter anordner en sagkyndig udtalelse, støde an mod effektivitetsprincippet. En systematisk anvendelse af en sådan sagkyndig udtalelse kan nemlig vise sig at være overflødig, henset til de øvrige beviser, som den ret, for hvilken sagen er indbragt, er i besiddelse af, navnlig – således som den bulgarske regering har anført i sit skriftlige indlæg – henset til resultaterne af en kontrol af overholdelsen af de foranstaltninger til beskyttelse af personoplysninger, der er blevet gennemført af en uafhængig og ved lov oprettet myndighed, såfremt denne kontrol er af nyere dato, eftersom de nævnte foranstaltninger i henhold til databeskyttelsesforordningens artikel 24, stk. 1, om nødvendigt skal revideres og ajourføres.

63 Som Europa-Kommissionen har anført i sit skriftlige indlæg, kan effektivitetsprincippet desuden blive tilsidesat i det tilfælde, hvor ordet »tilstrækkeligt« skal forstås således, at en national ret af en rapport med en sagkyndig udtalelse udelukkende eller automatisk skal udlede, at de sikkerhedsforanstaltninger, som den pågældende dataansvarlige har gennemført, er »passende« som omhandlet i databeskyttelsesforordningens artikel 32. Beskyttelsen af de rettigheder, som denne forordning giver – hvilken beskyttelse er formålet med det nævnte effektivitetsprincip – og særligt adgangen til effektive retsmidler over for en dataansvarlig, som er sikret ved forordningens artikel 79, stk. 1, kræver imidlertid, at en upartisk ret foretager en objektiv vurdering af, om de pågældende foranstaltninger er passende, i stedet for at begrænse sig til en sådan udledning (jf. i denne retning dom af 12.1.2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, præmis 50).

64 Henset til ovenstående begrundelser skal det tredje spørgsmåls anden del besvares med, at databeskyttelsesforordningens artikel 32 og det EU-retlige effektivitetsprincip skal fortolkes således, at en retsligt udmeldt sagkyndig udtalelse ikke kan udgøre et bevismiddel, der er systematisk nødvendigt for og tilstrækkeligt til at vurdere, om de sikkerhedsforanstaltninger, som den dataansvarlige har gennemført i henhold til denne artikel, er passende.

Det fjerde spørgsmål

65 Med sit fjerde spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om databeskyttelsesforordningens artikel 82, stk. 3, skal fortolkes således, at den dataansvarlige er fritaget for sin forpligtelse efter denne forordnings artikel 82, stk. 1 og 2, til at erstatte den skade, som en person har lidt, alene fordi denne skade skyldes en uautoriseret videregivelse af, eller en uautoriseret adgang til, personoplysninger foretaget af »tredjemand« som omhandlet i denne forordnings artikel 4, nr. 10).

66 Det skal indledningsvis præciseres, at det følger af databeskyttelsesforordningens artikel 4, nr. 10), at især andre personer end dem, som står under den dataansvarliges eller databehandlerens direkte myndighed, og som er beføjet til at behandle personoplysninger, har status som »tredjemand«. Denne definition omfatter personer, der ikke er den dataansvarliges ansatte og ikke er underlagt den dataansvarliges kontrol, såsom dem, der er omhandlet i det forelagte spørgsmål.

67 Dernæst skal det for det første bemærkes, at databeskyttelsesforordningens artikel 82, stk. 2, bestemmer, at »[e]nhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning«, og at denne artikels stk. 3 fastsætter, at en dataansvarlig eller, alt efter tilfældet, en databehandler er fritaget for et sådant erstatningsansvar, »hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden«.

68 I 146. betragtning til databeskyttelsesforordningen, som specifikt angår forordningens artikel 82, angives det endvidere i første og andet punktum, at »[d]en dataansvarlige eller databehandleren bør yde erstatning for enhver skade, som en person måtte lide som følge af behandling, der overtræder denne forordning«, og »bør være fritaget for erstatningsansvar, hvis den pågældende beviser ikke at være ansvarlig for den forvoldte skade«.

69 Af disse bestemmelser følger dels, at den pågældende dataansvarlige i princippet skal erstatte en skade, der er forvoldt ved en tilsidesættelse af denne forordning i forbindelse med denne behandling, dels at den pågældende kun kan fritages for sit ansvar, hvis denne fører bevis for, at vedkommende ikke er skyld i den begivenhed, der medførte skaden.

70 Som det fremgår af den udtrykkelige formulering »ikke at være ansvarlig for«, der blev tilføjet under lovgivningsproceduren, skal de omstændigheder, hvorunder den dataansvarlige kan gøre krav på at blive fritaget for det civilretlige ansvar, som den pågældende ifalder efter databeskyttelsesforordningens artikel 82, således være strengt begrænset til de omstændigheder, hvor den dataansvarlige kan påvise, at skaden ikke kan tilregnes den pågældende.

71 Når et brud på persondatasikkerheden som omhandlet i databeskyttelsesforordningens artikel 4, nr. 12) – som i det foreliggende tilfælde – er blevet begået af cyberkriminelle og dermed af »tredjemand« som omhandlet i denne forordnings artikel 4, nr. 10), kan denne tilsidesættelse ikke tilregnes den dataansvarlige, medmindre denne har muliggjort det nævnte brud ved at tilsidesætte en forpligtelse, der er fastsat i databeskyttelsesforordningen, og navnlig den forpligtelse til at beskytte oplysninger, som påhviler den dataansvarlige i henhold til samme forordnings artikel 5, stk. 1, litra f), og artikel 24 og 32.

72 I tilfælde af et brud på persondatasikkerheden begået af en tredjemand kan den dataansvarlige således på grundlag af databeskyttelsesforordningens artikel 82, stk. 3, fritages for sit erstatningsansvar ved at bevise, at der ikke er nogen årsagsforbindelse mellem den pågældendes eventuelle tilsidesættelse af forpligtelsen til at beskytte oplysningerne og den skade, som den fysiske person har lidt.

73 For det andet er den ovenstående fortolkning af denne artikel 82, stk. 3, ligeledes i overensstemmelse med databeskyttelsesforordningens formål, der består i at sikre et højt beskyttelsesniveau for fysiske personer i forbindelse med behandling af deres personoplysninger, således som anført i 10. og 11. betragtning til denne forordning.

74 Henset til samtlige disse betragtninger skal det fjerde spørgsmål besvares med, at databeskyttelsesforordningens artikel 82, stk. 3, skal fortolkes således, at den dataansvarlige ikke kan fritages for sin forpligtelse efter denne forordnings artikel 82, stk. 1 og 2, til at erstatte den skade, som en person har lidt, alene fordi denne skade skyldes en uautoriseret videregivelse af, eller en uautoriseret adgang til, personoplysninger foretaget af »tredjemand« som omhandlet i denne forordnings artikel 4, nr. 10), idet den dataansvarlige i så fald skal bevise, at den pågældende ikke er skyld i den begivenhed, der har medført den pågældende skade.

Det femte spørgsmål

75 Med sit femte spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om databeskyttelsesforordningens artikel 82, stk. 1, skal fortolkes således, at den frygt, som en registreret nærer for, at dennes personoplysninger potentielt kan blive misbrugt af tredjemand som følge af en tilsidesættelse af denne forordning, i sig selv kan udgøre en »immateriel skade« som omhandlet i denne bestemmelse.

76 Hvad for det første angår ordlyden af databeskyttelsesforordningens artikel 82, stk. 1, skal det bemærkes, at denne bestemmelse fastsætter, at »[e]nhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren«.

77 I denne henseende har Domstolen bemærket, at det klart fremgår af ordlyden af databeskyttelsesforordningens artikel 82, stk. 1, at en af betingelserne for ret til erstatning som fastsat i denne bestemmelse er, at der foreligger »skade«, eller at der er »forvold[t] skade«, ligesom denne forordning skal være overtrådt, og der skal være en årsagsforbindelse mellem skaden og overtrædelsen, idet disse tre betingelser er kumulative (dom 4.5.2023, Österreichische Post (Immateriel skade i forbindelse med behandling af personoplysninger), C-300/21, EU:C:2023:370, præmis 32).

78 Domstolen har i øvrigt på grundlag af både ordlyds-, system- og formålsbetragtninger fortolket databeskyttelsesforordningens artikel 82, stk. 1, således, at denne bestemmelse er til hinder for en national regel eller praksis, hvorefter erstatning for en »immateriel skade« som omhandlet i den nævnte bestemmelse er betinget af, at den skade, som den registrerede har lidt, har en vis alvorsgrad (dom 4.5.2023, Österreichische Post (Immateriel skade i forbindelse med behandling af personoplysninger), C-300/21, EU:C:2023:370, præmis 51).

79 Når dette er sagt, skal det i det foreliggende tilfælde fremhæves, at databeskyttelsesforordningens artikel 82, stk. 1, ikke sondrer mellem tilfælde, hvor den »immaterielle skade«, som den registrerede hævder at have lidt som følge af en konstateret tilsidesættelse af denne forordnings bestemmelser, på den ene side er forbundet med tredjemands misbrug af den registreredes personoplysninger, som allerede er sket på tidspunktet for vedkommendes erstatningskrav, og på den anden side er knyttet til den frygt, som denne person nærer for, at et sådant misbrug kan finde sted i fremtiden.

80 Ordlyden af databeskyttelsesforordningens artikel 82, stk. 1, udelukker derfor ikke, at begrebet »immateriel skade«, der fremgår af denne bestemmelse, kan omfatte en situation som den, der er henvist til af den forelæggende ret, hvor den registrerede med henblik på at opnå erstatning på grundlag af denne bestemmelse påberåber sig sin frygt for, at den pågældendes personoplysninger i fremtiden vil blive misbrugt af tredjemand som følge af den skete tilsidesættelse af denne forordning.

81 Denne ordlydsfortolkning understøttes for det andet af 146. betragtning til databeskyttelsesforordningen, som specifikt vedrører den ret til erstatning, der er fastsat i denne forordnings artikel 82, stk. 1, og som i tredje punktum nævner, at »[b]egrebet »skade« bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler formålene for denne forordning«. En fortolkning af begrebet »immateriel skade« som omhandlet i denne artikel 82, stk. 1, som ikke inkluderer de situationer, hvor den registrerede, der er berørt af en tilsidesættelse af den nævnte forordning, påberåber sig den frygt, som vedkommende nærer for,

at den pågældendes egne personoplysninger i fremtiden vil blive misbrugt, ville imidlertid ikke være i overensstemmelse med en bred opfattelse af dette begreb således som ønsket af EU-lovgiver (jf. analogt dom af 4.5.2023, Österreichische Post (Immateriel skade i forbindelse med behandling af personoplysninger), C-300/21, EU:C:2023:370, præmis 37 og 46).

82 Det fremgår i øvrigt af 85. betragtning, første punktum, til databeskyttelsesforordningen, at »[e]t brud på persondatasikkerheden kan, hvis det ikke håndteres på en passende og rettidig måde, påføre fysiske personer fysisk, materiel eller immateriel skade, såsom tab af kontrol over deres personoplysninger eller begrænsning af deres rettigheder, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, […] eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person«. Det fremgår af denne liste over eksempler på »skade«, som de registrerede kan lide, at EU-lovgiver har haft til hensigt, at dette begreb navnlig skulle omfatte det blotte »tab af kontrol« over deres egne oplysninger som følge af en tilsidesættelse af denne forordning, selv om et misbrug af de omhandlede oplysninger ikke konkret har fundet sted til skade for de nævnte personer.

83 For det tredje og endelig understøttes fortolkningen i nærværende doms præmis 80 af formålene med databeskyttelsesforordningen, som skal afspejles fuldt ud ved fastlæggelsen af begrebet »skade«, således som det fremgår af 146. betragtning, tredje punktum, til denne forordning. En fortolkning af databeskyttelsesforordningens artikel 82, stk. 1, hvorefter begrebet »immateriel skade« som omhandlet i denne bestemmelse ikke omfatter de situationer, hvor en registreret udelukkende påberåber sig sin frygt for, at den pågældendes oplysninger i fremtiden vil blive misbrugt af tredjemand, ville imidlertid ikke være i overensstemmelse med den garanti for et højt beskyttelsesniveau for fysiske personer i forbindelse med behandling af personoplysninger inden for Unionen, der er omhandlet i dette instrument.

84 Det skal imidlertid fremhæves, at en registreret person, der er berørt af en overtrædelse af databeskyttelsesforordningen, som har haft skadevirkninger for den pågældende, skal godtgøre, at disse virkninger udgør en immateriel skade som omhandlet i forordningens artikel 82 (jf. i denne retning dom af 4.5.2023, Österreichische Post (Immateriel skade i forbindelse med behandling af personoplysninger), C-300/21, EU:C:2023:370, præmis 50).

85 Når en person, der kræver erstatning på dette grundlag, påberåber sig en frygt for, at der i fremtiden vil ske et misbrug af den pågældendes personoplysninger som følge af en sådan tilsidesættelse, skal den nationale ret, hvor sagen anlægges, navnlig efterprøve, om denne frygt kan anses for at være velbegrundet under de pågældende specifikke omstændigheder og i forhold til den registrerede.

86 Henset til ovenstående begrundelser skal det femte spørgsmål besvares med, at databeskyttelsesforordningens artikel 82, stk. 1, skal fortolkes således, at den frygt, som en registreret nærer for, at dennes personoplysninger potentielt kan blive misbrugt af tredjemand som følge af en tilsidesættelse af denne forordning, i sig selv kan udgøre en »immateriel skade« som omhandlet i denne bestemmelse.

Sagsomkostninger

87 Da sagens behandling i forhold til hovedsagens parter udgør et led i den sag, der verserer for den forelæggende ret, tilkommer det denne at træffe afgørelse om sagsomkostningerne. Bortset fra de nævnte parters udgifter kan de udgifter, som er afholdt i forbindelse med afgivelse af indlæg for Domstolen, ikke erstattes.

På grundlag af disse præmisser kender Domstolen (Tredje Afdeling) for ret:

1) Artikel 24 og 32 i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

skal fortolkes således, at

en uautoriseret videregivelse af, eller en uautoriseret adgang til, personoplysninger foretaget af »tredjemand« som omhandlet i denne forordnings artikel 4, nr. 10), ikke i sig selv er tilstrækkelig til at fastslå, at de tekniske og organisatoriske foranstaltninger, som den omhandlede dataansvarlige har truffet, ikke var »passende« som omhandlet i denne artikel 24 og 32.

2) Artikel 32 i forordning 2016/679

skal fortolkes således, at

spørgsmålet om, hvorvidt de tekniske og organisatoriske foranstaltninger, som den dataansvarlige i henhold til denne artikel har truffet, er passende, skal vurderes konkret af de nationale retsinstanser under hensyntagen til de risici, der er forbundet med den pågældende behandling, og idet de skal vurdere, om arten, indholdet og gennemførelsen af disse foranstaltninger er tilpasset disse risici.

3) Princippet om den dataansvarliges ansvar, der er fastsat i artikel 5, stk. 2, i forordning 2016/679 og konkretiseret i denne forordnings artikel 24,

skal fortolkes således, at

den dataansvarlige i forbindelse med et erstatningssøgsmål på grundlag af denne forordnings artikel 82 bærer bevisbyrden for, at de sikkerhedsforanstaltninger, som vedkommende har gennemført i henhold til den nævnte forordnings artikel 32, er passende.

4) Artikel 32 i forordning 2016/679 og det EU-retlige effektivitetsprincip

skal fortolkes således, at

en retsligt udmeldt sagkyndig udtalelse ikke kan udgøre et bevismiddel, der er systematisk nødvendigt for og tilstrækkeligt til at vurdere, om de sikkerhedsforanstaltninger, som den dataansvarlige har gennemført i henhold til denne artikel, er passende.

5) Artikel 82, stk. 3, i forordning 2016/679

skal fortolkes således, at

den dataansvarlige ikke kan fritages for sin forpligtelse efter denne forordnings artikel 82, stk. 1 og 2, til at erstatte den skade, som en person har lidt, alene fordi denne skade skyldes en uautoriseret videregivelse af, eller en uautoriseret adgang til, personoplysninger foretaget af »tredjemand« som omhandlet i denne forordnings artikel 4, nr. 10), idet den dataansvarlige i så fald skal bevise, at den pågældende ikke er skyld i den begivenhed, der har medført den pågældende skade.

6) Artikel 82, stk. 1, i forordning 2016/679

skal fortolkes således, at

den frygt, som en registreret nærer for, at dennes personoplysninger potentielt kan blive misbrugt af tredjemand som følge af en tilsidesættelse af denne forordning, i sig selv kan udgøre en »immateriel skade« som omhandlet i denne bestemmelse.

Underskrifter