

**Mål C-340/21****Sammanfattning av begäran om förhandsavgörande i enlighet med artikel 98.1 i domstolens rättegångsregler****Datum för ingivande:**

2 juni 2021

**Domstol som begär förhandsavgörande:**

Varhoven administrativen sad (Bulgarien)

**Datum för beslutet att begära förhandsavgörande:**

14 maj 2021

**Klagande:**

VB

**Motpart:**

Natsionalna agentsia za prihodite (den nationella skattemyndigheten)

**Saken i det nationella målet**

Överklagande av en dom som innebar ogillande av en talan om ersättning för immateriell skada på grund av att motparten i egenskap av personuppgiftsansvarig underlåtit att i tillräcklig utsträckning fullgöra sina skyldigheter enligt Zakon za zashtita na lichnite dannii (lagen om skydd av personuppgifter) och enligt förordning 2016/679.

**Syfte med och rättslig grund för begäran om förhandsavgörande**

Begäran om förhandsavgörande i enlighet med artikel 267 FEUF avseende tolkningen av skälen 74, 85 och 146 samt artikel 4 led 12 och artiklarna 5.2, 24, 32 och 82 i förordning 2016/679.

## Tolkningsfrågor

1. Ska artiklarna 24 och 32 i förordning (EU) 2016/679 tolkas på så sätt att det är tillräckligt att personer som inte är anställda vid den personuppgiftsansvariga myndigheten och inte står under dennas kontroll har gjort sig skyldiga till obehörigt röjande av eller obehörig åtkomst till personuppgifter i den mening som avses i artikel 4 led 12 i förordning (EU) 2016/679, för att de tekniska och organisatoriska åtgärderna ska anses inte vara lämpliga?
2. Om fråga 1 besvaras nekande, vad ska vara föremål för domstolens laglighetsprövning och i vilken omfattning ska prövningen göras när domstolen undersöker huruvida de tekniska och organisatoriska åtgärder som den personuppgiftsansvariga myndigheten har vidtagit är lämpliga enligt artikel 32 i förordning (EU) 2016/679?
3. Om fråga 1 besvaras nekande, ska principen om ansvarsskyldighet enligt artiklarna 5.2 och 24 jämförda med skäl 74 i förordning (EU) 2016/679 tolkas på så sätt att när en talan väcks enligt artikel 82.1 i förordning (EU) 2016/679 har den personuppgiftsansvariga myndigheten bevisbördan för att de tekniska och organisatoriska åtgärder enligt artikel 32 i förordningen som har vidtagits är lämpliga? Kan ett sakkunnigutlåtande anses utgöra nödvändig och tillräcklig bevisning för att fastställa huruvida de tekniska och organisatoriska åtgärder som den personuppgiftsansvariga myndigheten vidtagit varit lämpliga i ett sådant fall som det förevarande, om den obehöriga åtkomsten till och det obehöriga röjandet av personuppgifter är en följd av ett "it-angrepp"?
4. Ska artikel 82.3 i förordning (EU) 2016/679 tolkas på så sätt att det obehöriga röjandet av eller den obehöriga åtkomsten till personuppgifter i den mening som avses i artikel 4 led 12 i förordning (EU) 2016/679, så som i förevarande fall genom ett it-angrepp som utförts av personer som inte är anställda vid den personuppgiftsansvariga myndigheten, utgör en omständighet för vilken den personuppgiftsansvariga myndigheten inte på något sätt är ansvarig och vilken gör det möjligt att undanta denna från ersättningsansvar.
5. Ska artikel 82.1 och 82.2 jämförd med skälen 85 och 146 i förordning (EU) 2016/679 tolkas på så sätt att, i ett sådant fall som det förevarande där det skett en kränkning av skyddet av personuppgifter, vilken tar sig uttryck i obehörig åtkomst till och spridning av personuppgifter genom ett it-angrepp, enbart den berörda personens oro, farhågor och rädsla för att personuppgifter kan missbrukas i framtiden omfattas av begreppet immateriell skada, vilket ska tolkas extensivt och därmed ger rätt till skadeersättning, om sådant missbruk inte har fastställts och/eller ingen ytterligare skada har åsamkats den berörda personen?

## Anförda unionsbestämmelser och anförd praxis från EU-domstolen

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter

och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (nedan kallad förordningen): skälen 1, 4, 6, 74, 75, 76, 77, 83, 85 och 146 och artikel 4 leden 2, 7 och 12 samt artiklarna 5, 24, 32, 33, 79, 82.

EU-domstolens dom av den 30 maj 2013, Worten (C-342/12, EU:C:2013:355), punkterna 24 och 26.

### **Anförda nationella bestämmelser**

Administrativnoprotsesualen kodeks (förvaltningsprocesslagen), artiklarna 144.1, 203 och 208.

Grazhdanski protsesualen kodeks (civilprocesslagen), artikel 154.

Zakon za otgovornostta na darzhavata i obshtinite za vredi (lagen om statens och kommunernas skadeståndsansvar), artikel 1.

Zakon za zashtita na lichnite dannii (lagen om skydd av personuppgifter), artiklarna 39.1, 39.2 och 59.1.

### **Kortfattad redogörelse för de faktiska omständigheterna och förfarandet i det nationella målet**

- 1 Natsionalna agentsia za prihodite (den nationella skattemyndigheten) (nedan kallad skattemyndigheten) är personuppgiftsansvarig i den mening som avses i artikel 4 led 7 i förordningen. Enligt nationell rätt är skattemyndigheten en specialiserad myndighet som är underordnad finansministern och har ansvar för att fastställa, säkerställa och driva in offentliga fordringar och privatpersoners i lag föreskrivna skulder till staten. Skattemyndigheten behandlar personuppgifter när den utövar sina offentliga befogenheter.
- 2 Den 15 juli 2019 informerade de bulgariska medierna samhället som helhet om att det hade skett obehörig åtkomst till skattemyndighetens informationssystem och om att uppgifterna i dess databaser, vilka innehöll personuppgifter och uppgifter om skatter och avgifter och socialförsäkring, hade publicerats på internet. 4 057 328 bulgariska medborgare berördes, medan det totala antalet berörda fysiska personer, dit både bulgariska och utländska medborgare räknades, uppgick till 6 074 140. Klaganden, VB, finns också bland de berörda.
- 3 Det finns ännu inte någon lagakraftvunnen fällande dom mot de personer som (ska ha) gjort sig skyldiga till den obehöriga åtkomst som i medierna betecknades som ett it-angrepp
- 4 Efter åtkomsten väckte hundratals medborgare talan mot skattemyndigheten och yrkade ersättning för immateriell skada.

- 5 Den 16 september 2019 väckte VB talan mot skattemyndigheten vid Administrativen sad Sofia-grad (Förvaltningsdomstolen i Sofia) och yrkade skadeersättning med ett belopp på 1 000 lev (BGN) (cirka 511 euro) enligt artikel 82.1 i förordningen, artikel 1.1 lagen om statens och kommunernas skadeståndsansvar och artikel 39.1 lagen om skydd av personuppgifter.
- 6 I förfarandet i första instans gjorde VB gällande att skattemyndigheten ”inte på bästa möjliga sätt” hade fullgjort sin skyldighet att ”korrekt säkerställa sin it-säkerhet” och att ”i största möjliga utsträckning effektivt säkerställa säkerheten för de bulgariska medborgarnas personuppgifter”. Därigenom skedde en personuppgiftsincident i den mening som avses i artikel 4 led 12 i förordningen, och personuppgifter röjdes olagligt.
- 7 VB ansåg att ”den bristande omsorgen och den omständigheten att effektiva åtgärder för dataskydd inte hade vidtagits” skulle anses utgöra underlåtenhet från skattemyndighetens sida att fullgöra sina skyldigheter avseende medborgarnas personuppgifter och att detta utgjorde en överträdelse av artiklarna 24 och 32 i förordningen. I egenskap av personuppgiftsansvarig är skattemyndigheten skyldig att, genom att vidta lämpliga tekniska och organisatoriska åtgärder, behandla personuppgifterna på ett sätt som ”säkerställer lämplig säkerhet”.
- 8 VB gjorde gällande att hon, genom att skattemyndigheten åsidosatt sina skyldigheter, hade lidit immateriell skada som yttrade sig i oro och farhågor för att hennes personuppgifter skulle komma att missbrukas i framtiden, till exempel att hennes egendom skulle exproprieras, hennes bankkonton missbrukas, krediter avtalas i hennes namn, hennes civilstånd ändras eller hennes identitet bli stulen. Hon är upprörd över det ”omfattande intrånget i skattemyndighetens informationssystem” och känner sig inte skyddad av staten. Hon befärar att hon kommer att bli utpressad, attackerad eller kidnappad.
- 9 Skattemyndigheten ansåg att talan saknade grund. VB hade inte begärt någon information från skattemyndigheten om exakt vilka personuppgifter som hade utsatts för intrång.
- 10 Efter åtkomsten hade skattemyndigheten omedelbart vidtagit åtgärder för att skydda medborgarnas rättigheter och intressen. Det hade hållits möten med företrädare och experter vid säkerhetstjänsten, Notarialna kamara (kontoret för notarius publicus), Agentsia po vpisvaniata (registerbyrån), Asotsiatsia na targovskite banki (sammanslutningen av affärsbanker) med flera, för att samordna åtgärderna för att begränsa följderna av åtkomsten. På skattemyndighetens webbplats hade särskilda rubriker avseende it-angreppet lagts upp där aktuell information hade publicerats.
- 11 Enligt skattemyndigheten finns det inget orsakssamband mellan den påstådda immateriella skadan och den obehöriga åtkomsten till personuppgifterna. Skattemyndigheten hade utsatts för attacker som utförts av tredje parter som inte var anställda vid skattemyndigheten. Den var således inte ansvarig för skadorna.

- 12 Skattemyndigheten gjorde gällande att den hade vidtagit ett stort antal åtgärder. Den hade nämligen infört processhanteringssystem och ledningssystem för informationssäkerhet, godkänt förfaranden som uppfyller de internationella kvalitetsstandarderna ISO 9000 och ISO 9001, och den tillämpar direktiv, regler, förfaranden, anvisningar och metoder enligt ledningssystemet för informationssäkerhet.
- 13 Skattemyndigheten lade fram bevisning, närmare bestämt olika interna dokument från perioden från januari 2013 till maj 2019 om innehållet, förfarandet för inrättande och underhåll och om åtkomst till databaserna, införandet av ledningssystem för informationssäkerhet, förebyggande förfaranden, de interna reglerna om nät- och informationssäkerhet, anvisningarna om hantering av information, riktlinjerna för skydd av personuppgifter, åtgärderna och medlen för skydd av personuppgifter och metoderna och förfarandet för riskbedömning.
- 14 I dom av den 27 november 2020 ogillade Administrativen sad Sofia-grad VB:s talan.
- 15 Administrativen sad Sofia-grad förklarade att den obehöriga åtkomsten till skattemyndighetens databas genom ett it-angrepp hade genomförts av personer mot vilka det hade inletts en förundersökning som ännu inte var avslutad.
- 16 Det lagstridiga resultatet ger enligt nämnda domstol inte anledning att förmoda att den personuppgiftsansvariga myndigheten inte fullgjort sin skyldighet att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa skyddet av databasen, så att ingen på något sätt och med några medel skulle kunna få åtkomst till denna databas.
- 17 Administrativen sad Sofia-grad ansåg att VB skulle redogöra för vilka (tekniska) åtgärder som skattemyndigheten faktiskt borde ha vidtagit, men inte hade vidtagit eller vidtagit bristfälligt, vilket hade lett till obehörig åtkomst till och röjande av personuppgifter eller bidragit till detta.
- 18 Enligt Administrativen sad Sofia-grad kunde det inte konstateras någon försummelse från den personuppgiftsansvariga myndighetens sida mot bakgrund av den bevisning som lagts fram. VB hade inte lidit någon ersättningsgill immateriell skada. De psykiska påfrestningar som VB hade upplevt och som hade orsakats av underrättelsen om den obehöriga åtkomsten till informationsdatabaserna är enligt domstolen normala, men utgör ingen faktisk skada i rättslig bemärkelse. VB hade inte visat något intresse av att få veta exakt vilka av hennes personuppgifter som hade kommits åt. Ett sådant beteende tyder inte på att det föreligger någon avsevärd emotionell stress.
- 19 Administrativen sad Sofia-grad fann att det offentliga tillkännagivandet beträffande den lagstridiga åtkomsten till skattemyndighetens databas inte hade påverkat VB:s liv när det gällde hennes självtillit, hennes självkänsla, hennes arbete, hennes relationer eller hennes hälsotillstånd. Det fanns inget

orsakssamband med de upplevda negativa känslorna, eftersom de inte var ett resultat av skattemyndighetens beteende.

- 20 VB överklagade domen från Administrativen sad Sofia-grad till den hänskjutande domstolen, Varhoven administrativen sad (Högsta förvaltningsdomstolen).

### **Parternas huvudargument**

- 21 I överklagandet har VB gjort gällande att Administrativen sad Sofia-grad gjorde en felaktig uppdelning av bevisbördan när det gällde att bevisa en negativ omständighet, nämligen den personuppskyddsansvariga myndighetens underlåtenhet att vidta lämpliga tekniska och organisatoriska åtgärder.
- 22 VB anser att skattemyndigheten har utrymme för skönsmässig bedömning när det gäller att vidta effektiva åtgärder, varför det inte är möjligt att förklara vilka konkreta skyldigheter skattemyndighetens anställda borde ha fullgjort, men inte fullgjorde. Den bevisning som skattemyndigheten lagt fram visade inte att de tekniska och organisatoriska åtgärder som vidtagits var lämpliga.
- 23 VB gör gällande att oron för eventuellt framtida missbruk av personuppgifterna inte utgör någon hypotetisk, utan en faktisk immateriell skada som ska ersättas. Det är inte nödvändigt att bevisa en normal immateriell skada.
- 24 Skattemyndigheten gör gällande att Administrativen sad Sofia-grad gjorde en riktig bedömning när den utgick från att skattemyndigheten inte gjort sig skyldig till underlåtenhet i egenskap av personuppgiftsansvarig, utan hade vidtagit ett stort antal tekniska och organisatoriska åtgärder för skydd vid behandlingen av personuppgifter. Det har inte bevisats att en skada faktiskt har inträffat. Oron och rädslan för framtida händelser är inte ersättningsgill.

### **Kortfattad redogörelse för skälen till att förhandsavgörande begärs**

- 25 Liknande domstolsförfaranden mot skattemyndigheten har gett motstridiga resultat i första instans. Antingen har talan ogillats eller har den tagits upp till prövning i vissa delar eller i sin helhet. Lagstiftningen har tolkats och tillämpats motsägelsefullt när det gällt alla delar av den personuppgiftsansvariga myndighetens ansvar.
- 26 Varhoven administrativen sad anser att ansvaret enligt artikel 82 i förordningen omfattar följande: i) den personuppgiftsansvariges överträdelse av denna förordning, ii) en materiell eller immateriell skada som den berörda personen har lidit, och iii) ett orsakssamband mellan skadan och den konkreta överträdelsen.



**Fråga 1**

- 27 Enligt artikel 24.1 i förordningen ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.
- 28 Vad gäller säkerheten i samband med behandlingen föreskrivs i artikel 32 i förordningen skyldigheter för den personuppgiftsansvarige, vilka är relevanta för dennes ansvar enligt artikel 24 och medför detta ansvar. Här räknas de kriterier upp enligt vilka lämpliga tekniska och organisatoriska åtgärder ska vidtas för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Hit hör ”den senaste utvecklingen och genomförandekostnaderna, behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter”.
- 29 I förordningen definieras inte begreppet ”lämpliga tekniska och organisatoriska åtgärder”. I skäl 74 anges det att personuppgiftsansvariga särskilt bör vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet.
- 30 Av ovanstående följer att personuppgiftsansvariga ska genomföra en riskbedömning enligt de kriterier som anges i artikel 32 i förordningen, på grundval av vilka de ska vidta tekniska och organisatoriska åtgärder som är lämpliga med hänsyn till vad som krävs och den säkerhetsnivå för personuppgifterna som är lämplig i förhållande till risken. Genom att vidta lämpliga tekniska och organisatoriska åtgärder säkerställer de personuppgiftsansvariga att de behandlar personuppgifterna i enlighet med förordningen.
- 31 Av nämnda lagstiftning följer att valet av lämpliga tekniska och organisatoriska åtgärder är en fråga om ändamålsenlighet. Den personuppgiftsansvariges bedömning av ändamålsenligheten är emellertid inte underkastad någon domstolsprövning, eftersom domstolen kontrollerar lagligheten. Samtidigt ska behandlingen av personuppgifter, när det finns ett utrymme för skönsmässig bedömning vad gäller valet av tekniska och organisatoriska åtgärder, ske inom ramen för förordningen och med beaktande av syftet att skydda den grundläggande rätten till skydd av personuppgifter för fysiska personer.
- 32 Med hänsyn till det ovan anförda vill Varhoven administrativen sad få klarhet i huruvida artiklarna 24 och 32 i förordningen ska tolkas på så sätt att det är tillräckligt att en otillåten händelse ägt rum i form av obehörigt röjande eller obehörig åtkomst till personuppgifter i den mening som avses i artikel 4.12 i förordningen för att det ska anses visat att de tekniska och organisatoriska åtgärder som den personuppgiftsansvariga myndigheten vidtagit inte har varit lämpliga.

**Fråga 2 (om fråga 1 besvaras nekande)**

- 33 Eftersom valet och tillämpningen av tekniska och organisatoriska åtgärder har överlåtits åt den personuppgiftsansvariga myndighetens subjektiva bedömning och omfattas av dess utrymme för skönmässig bedömning, ställer sig Varhoven administrativen sad frågan vad som ska vara föremål för domstolens laglighetsprövning och i vilken omfattning prövningen ska göras när domstolen undersöker huruvida de tekniska och organisatoriska åtgärder som den personuppgiftsansvariga myndigheten har vidtagit är lämpliga och förenliga med artiklarna 24 och 32 i förordningen.
- 34 Varhoven administrativen sad är osäker på om det räcker att den nationella domstolen fastställer på vilket sätt den personuppgiftsansvariga myndigheten har fullgjort de skyldigheter som följer av de nämnda bestämmelserna, eller om denna domstol ska undersöka innehållet i de tekniska och organisatoriska åtgärder som har vidtagits, men som endast nämns som exempel i förordningen och ska vidtas om det är ändamålsenligt.

**Fråga 3 (om fråga 1 besvaras nekande)**

- 35 Enligt artikel 5.2 i förordningen ska den personuppgiftsansvarige ansvara för och kunna visa att de principer i punkt 1 i samma bestämmelse som avser behandling av personuppgifter efterlevs. Enligt artikel 24.1 i förordningen ska den personuppgiftsansvarige ”genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning.”
- 36 Artikel 82.3 i förordningen gör det möjligt för den personuppgiftsansvarige eller personuppgiftsbiträdet att undgå ansvar enligt punkt 2 ”om den visar att den inte på något sätt är ansvarig för den händelse som orsakade skadan”. Enligt nämnda punkt 2 ska den personuppgiftsansvarige som medverkat vid behandlingen ansvara för skada som orsakats av behandling som strider mot denna förordning.
- 37 Enligt den nationella lagstiftningen är varje part i ett mål när talan har väckts skyldig att bevisa de omständigheter som ligger till grund för dennes yrkanden eller invändningar. I liknande mål har domstolarna i första instans delat upp bevisbördan mellan käranden och svaranden på olika sätt.
- 38 I det nu aktuella fallet är det relevant att ställa frågan huruvida principen om ansvarsskyldighet enligt artikel 5.2 jämförd med skäl 74 och artikel 24.1 i förordningen ska tolkas på så sätt att bevisbördan blir omvänd och den personuppgiftsansvarige, mot vilken skadeståndstalan har väckts på grund av en överträdelse av förordningen, i egenskap av motpart är skyldig att visa att de tekniska och organisatoriska åtgärder som har vidtagits är lämpliga.
- 39 Förutom frågan om föremålet för och omfattningen av domstolens prövning av huruvida skyldigheterna enligt förordningen har fullgjorts är det också



problematiskt hur och med vilken bevisning det ska prövas huruvida skyldigheterna har fullgjorts och särskilt huruvida alla lämpliga tekniska och organisatoriska åtgärder har vidtagits.

- 40 I förfarandet lade skattemyndigheten fram bevisning avseende säkerställandet av skyddet av datanäten enligt de standarder som anges i dokumenten, men det inhämtades inget forensiskt sakkunnigutlåtande för att fastställa huruvida de tekniska och organisatoriska åtgärderna varit lämpliga i den mening som avses i förordningen. Varhoven administrativen sad är medveten om att en sådan personuppgiftsansvarig som skattemyndigheten är skyldig att vidta organisatoriska, teknologiska och tekniska åtgärder för nät- och informationssäkerhet som står i rimlig proportion till hoten i form av it-brottslighet, för att minimera risken för att de förverkligas. Om kriminaltekniska experter fick åtkomst i varje mål för vilket artikel 82 i förordningen utgör rättslig grund, skulle det kunna få nya negativa konsekvenser för skyddet av personuppgifter.
- 41 Med hänsyn till den senaste tekniska utvecklingen, befintliga standarder för skydd av datanät och den obehöriga åtkomsten genom ett it-angrepp som genomförts av personer som befinner sig utanför den personuppgiftsansvariga myndigheten ställer sig Varhoven administrativen sad frågan huruvida domstolens inhämtande av ett forensiskt sakkunnigutlåtande kan anses utgöra nödvändig och tillräcklig bevisning för att fastställa huruvida de tekniska och organisatoriska åtgärder som vidtagits och tillämpats har kunnat säkerställa skyddet av personuppgifterna.

#### Fråga 4

- 42 I egenskap av personuppgiftsansvarig som medverkar vid behandling av personuppgifter är skattemyndigheten ansvarig, men den kan undgå ansvar enligt artikel 82.3, om den visar att den inte i något avseende är ansvarig för den omständighet genom vilken skadan har uppkommit.
- 43 I förfarandet är det ostridigt att åtkomsten till personuppgifterna ägde rum genom ett it-angrepp mot skattemyndigheten. Den obehöriga åtkomsten till och röjandet av personuppgifter skedde däremot inte när eller med anledning av att skattemyndighetens personal behandlade personuppgifterna.
- 44 Varhoven administrativen sad vill få klarhet i huruvida det i det nu aktuella fallet kan antas att det föreligger en omständighet för vilken den personuppgiftsansvariga myndigheten inte på något sätt är ansvarig och att den följaktligen undgår ansvar genom denna omständighet.

#### Fråga 5

- 45 Den berörda personen yrkar ersättning för den immateriella skadan, som på olika sätt som hon har beskrivit tar sig uttryck i oro, rädsla, stress, en känsla av

osäkerhet och fruktan för framtida missbruk av hennes personuppgifter. Det finns inget som tyder på VB:s personuppgifter har missbrukats.

- 46 Såsom framgår av skälen 75 och 85 i förordningen beaktas typen av personuppgifter och de negativa effekterna för de berörda personerna i uppräknningen av exempel på materiella och immateriella skador, och inte enbart personernas subjektiva känsla.
- 47 I skäl 146 i förordningen fastställs gränsen för ansvaret. Den personuppgiftsansvarige ska ersätta ”all skada” som en person kan komma att lida till följd av behandling som strider mot förordningen.
- 48 Efter det att åtkomst redan har ägt rum kan den berörda personens personuppgifter bli föremål för ett stort antal fall av missbruk av immateriell och materiell art med avsevärda konsekvenser. Sådana fall av missbruk har blivit kända bland allmänheten, vilket kan motivera en ökad oro hos den person som berörs av it-angreppet. Eftersom det saknas uppgifter om missbruk som redan har ägt rum rör det sig i det nu aktuella fallet endast om en förmodan om framtida missbruk, en hypotes med en möjlig, men osäker risk för den berörda personens rättigheter.
- 49 Av nämnda skäl uppkommer frågan huruvida den berörda personens negativa känslor i detta sammanhang, det vill säga huruvida enbart den omständigheten att det föreligger risk för eventuellt framtida missbruk av personuppgifterna, omfattas av begreppet immateriell skada och ger rätt till ersättning enligt artikel 82.1 jämförd med skäl 146 i förordningen.
- 50 Det är emellertid möjligt att artikel 82.1 jämförd med skäl 146 i förordningen inte kan tolkas på så sätt att varje negativ känsla, rädsla eller oro hos den berörda personen ger rätt till ersättning för den immateriella skadan, om det inte dessförinnan förekommit olaglig användning, som till exempel genom expropriation av tillgångar, avtal om krediter i den berörda personens namn eller identitetsstöld.