Integritetsskyddsmyndigheten

Migrationsverket
Slottsgatan 82
602 22 Norrköping

Diarienummer:
DI-2019-13667

Ert diarienummer:
1.3.3-2019-43845

Datum:
2021-11-17

Beslut efter tillsyn enligt dataskyddsförordningen – Migrationsverkets behandling av personuppgifter i VIS

Innehåll

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

1. Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten utfärdar varningar, med stöd av 58.2 a dataskyddsförordningen, då Migrationsverkets behandling sannolikt kommer att bryta mot bestämmelserna i dataskyddsförordningen enligt följande.

1. Den fortsatta utvecklingen och förvaltningen av VIS kan, i strid med artikel 32 dataskyddsförordningen, komma att äventyras på grund av otydligheter kring IT-dokumentationens status, vilket kan leda till att Migrationsverket inte vidtar lämpliga tekniska och organisatoriska åtgärder som säkerställer en säkerhetsnivå som är lämplig.
2. Uppgifter i användarloggar kan, i strid med artikel 5.1 e dataskyddsförordningen om lagringsminimering, komma att sparas under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas, eftersom Migrationsverket saknar en rutin för gallring av användarloggar.

2. Redogörelse för tillsynsärendet

2.1 Granskningens syfte och avgränsning

Integritetsskyddsmyndigheten (IMY) har i enlighet med fastställd inspektionsplan granskat Migrationsverkets behandling av personuppgifter i den nationella delen av informationssystemet för viseringar (VIS). Syftet med granskningen har varit att kontrollera om behandlingen av personuppgifter är i överensstämmelse med gällande rätt, dvs. VIS-förordningen[1] och dataskyddsförordningen (GDPR)[2].

IMY har en skyldighet enligt artikel 41.2 i VIS-förordningen att granska behandlingen i den nationella delen av VIS minst en gång vart fjärde år. Granskningen ska genomföras i enlighet med internationella redovisningsstandarder.

Vid granskningen har IMY ställt frågor avseende personuppgiftsbehandlingen i VIS, personuppgiftsansvar, personuppgiftsbiträden, behöriga myndigheter, informationsutbyte med andra medlemsländer, gallring, överföring av personuppgifter till tredje land, registrerades rättigheter, utbildning av personal samt it-säkerhet.

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen)

[2] 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)

2.2 Genomförande och metod

IMY har vid tre tillfällen, den 16 januari 2020, den 21 februari 2020 och den 5 oktober 2021, på plats hos Migrationsverket granskat personuppgiftsbehandlingen i den nationella delen av VIS. Migrationsverket har vid det första tillfället förevisat VIS och de nationella IT-systemen Wilma, W2, VIS-mail och den centrala utlänningsdatabasen (CUD).

Efter det första inspektionstillfället har IMY skickat ett antal skriftliga frågor till Migrationsverket, som verket har besvarat före det andra inspektionstillfället.

Vid det andra inspektionstillfället har IMY ställt kompletterande frågor samt genomfört stickprovskontroller av avslutade viseringsärenden i Wilma samt pågående viseringsärenden i W2.

På grund av pandemin har det tredje inspektionstillfället, med fokus på användarloggar, fått skjutas upp till hösten 2021. Inför detta tillfälle har IMY skickat ett antal kompletterande frågor som Migrationsverket har fått besvara.

Vid det tredje inspektionstillfället har IMY granskat användarloggarna samt ställt kompletterande frågor. Migrationsverket har också fått möjlighet att informera om vad som kan ha förändrats sedan inspektion 2.

2.3 Om VIS

VIS är ett EU-gemensamt system för utbyte av uppgifter om viseringar för kortare vistelser mellan EU:s medlemsländer. Syftet med VIS är att underlätta förfarandet vid visumansökningar, förhindra ett kringgående av reglerna om vilket medlemsland som ansvarar för att pröva en visumansökan, underlätta kampen mot bedrägerier, underlätta kontroller vid gränsövergångar vid de yttre gränserna av Schengen och inom medlemsstaternas territorium och att bidra till att förebygga hot mot medlemsstaternas inre säkerhet.

VIS innehåller personuppgifter som samlats in och registrerats i samband med ansökan om visum. Vilka personuppgifter som får behandlas anges i VIS-förordningen och inkluderar bl.a. fingeravtryck och fotografier.

Migrationsverket är utsedd att vara personuppgiftsansvarig enligt artikel 41.4 i VIS-förordningen för Sveriges behandling av personuppgifter i VIS. Personuppgiftsansvaret omfattar även utlandsmyndigheternas automatiska behandling vid hantering av visumansökningar. Även andra, särskilt utsedda, myndigheter använder VIS bl.a. i den brottsbekämpande verksamheten.

Huvudkomponenten i IT-systemet är den centrala databasen (C-VIS), som innehåller uppgifter om visumansökningar och beslut från medlemsländerna. Den centrala databasen hanteras av Europeiska byrån för den operativa förvaltningen av stora IT-system inom området frihet, säkerhet och rättvisa (eu-Lisa). Det finns också ett integrerat kommunikationssystem, ViSMail, som används för kommunikation mellan Schengenstaterna i aktuella och avslutade viseringsärenden.

Varje medlemsland har nationella system (N-VIS) som kommunicerar med den centrala databasen. I Sverige använder sig Migrationsverket av det processtyrda ärendehanteringssystemet W2 för att hantera pågående visumansökningar och Wilma

för att hantera avslutade ärenden. Nationell information sparas i den centrala utlänningsdatabasen (CUD).

3. Motivering av beslutet

3.1 Vad granskningen omfattat

IMY:s granskning har omfattat vilka personuppgifter som behandlas i den nationella delen av VIS, vem som är personuppgiftsansvarig för behandlingen, om det finns personuppgiftsbiträden och förutsättningarna för hur de behandlar personuppgifter, vilka som är behöriga myndigheter och vilka uppgifter de har åtkomst till, hur informationsutbytet med andra medlemsländer går till, hur länge personuppgifter sparas i den nationella delen, hur datakvaliteten säkerställs och registervården fungerar, om uppgifterna överförs till tredje land, hur de registrerades rättigheter säkerställs, vilken utbildning i hanteringen av personuppgifter som tillhandahålls personalen samt hur it-säkerheten fungerar. Av avsnitt 3.9.1 framgår närmare vad som ingått i granskningen av it-säkerheten.

Under motiveringen av beslutet tar IMY upp utvalda delar av det som granskats. I övrigt har IMY inga synpunkter på behandlingen.

3.2 VIS-förordningen i förhållande till dataskyddsförordningen

Dataskyddsförordningen infördes den 25 maj 2018 och är den primära rättsliga regleringen vid behandling av personuppgifter.

Dataskyddsförordningens bestämmelser gäller i den mån det inte finns en särreglering i VIS-förordningen. Det framgår av skäl 17 i VIS-förordningen och artikel 94.2 i dataskyddsförordningen.

3.3 Grundläggande förutsättningar för att behandla personuppgifter i VIS

3.3.1 Migrationsverkets syften med behandlingen av personuppgifter i VIS

I artikel 2 i VIS-förordningen anges de syften för vilka personuppgifter får behandlas. För Migrationsverkets del handlar det framförallt om att hantera och besluta i viseringsärenden. Det har inte framkommit något inom ramen för granskningen och de stickprovskontroller som IMY utfört som tyder på att Migrationsverket skulle behandla uppgifter i de nationella systemen för andra syften än vad som framgår av VIS-förordningen.

3.3.2 Uppgifter som får behandlas enligt VIS-förordningen

I VIS-förordningen finns det ett flertal artiklar (artiklarna 9-14) som uttryckligen anger vilka uppgifter som får behandlas i samband med en viseringsansökan.

IMY har granskat vilka uppgifter som har registrerats i Wilma och i W2. I mycket stor utsträckning är kategorierna av uppgifter fördefinierade dvs. det finns ett väldigt lite utrymme för en person med åtkomst till systemen att behandla andra kategorier av uppgifter i de nationella systemen. IMY:s stickprovskontroller har inte heller visat att Migrationsverket skulle behandla andra uppgifter än vad myndigheten har stöd att behandla enligt VIS-förordningen.

3.4 Personuppgiftsansvar

Enligt artikel 41.4 i VIS-förordningen ska varje medlemsstat utse en myndighet som ska vara personuppgiftsansvarig och ha ett centralt ansvar för denna medlemsstats behandling av uppgifter. Migrationsverket är den nationellt utpekade myndigheten, vilket framgår av 11 § punkten 3 förordning (2019:502) med instruktion för Migrationsverket.

Av 9 § utlänningsdatalagen (2016:27) framgår också att Migrationsverket är personuppgiftsansvarig för myndighetens behandling av personuppgifter. Dessutom är Migrationsverket enligt nämnda bestämmelse även personuppgiftsansvarig för utlandsmyndigheterna automatiserade behandling av personuppgifter, vilket omfattar behandling av personuppgifter i VIS.

Migrationsverket har i ärendet bl.a. informerat om att heltidsanställda vid utlandsmyndigheter, som handlägger migrationsärenden, sedan den 1 januari 2020 är anställda av Migrationsverket medan deltidsanställda och lokalanställda även fortsättningsvis är anställda av Utrikesdepartementet (UD). Anställda vid UD i Stockholm handlägger inte migrationsärenden överhuvudtaget och har heller ingen access till VIS-systemet. I syfte att klargöra ansvarsförhållandet mellan Migrationsverket och UD har det tecknats en förvaltningsöverenskommelse mellan parterna.

IMY ser positivt på att Migrationsverket och UD har tecknat en förvaltningsöverenskommelse. Det är viktigt att gränserna för Migrationsverkets personuppgiftsansvar är klarlagt i förhållande till UD. IMY har inga synpunkter på vad som framkommit i ärendet avseende personuppgiftsansvaret.

3.5 Behandling av särskilda kategorier av personuppgifter

IMY har särskilt ställt frågor kring Migrationsverkets behandling av fingeravtryck och fotografier. Av artikel 9 i VIS-förordningen framgår att viseringsmyndigheten ska registrera såväl fotografi av den sökanden såsom fingeravtryck. Migrationsverket har beskrivit hur fingeravtryck och fotografier registreras och hanteras och hur kvaliteten på uppgifterna säkerställs.

Migrationsverket har informerat om att det från EU-nivå inte det inte ställs något uttryckligt krav på kvalitén på ett fingeravtryck och förklarat att det sannolikt beror på att det är bättre med ofullständiga eller i viss mån ”sämre” avtryck i det centrala VIS än inga alls. Det finns dock krav på upplösning och vissa andra krav i (2009/756/EG), vilken refereras till i ”Bilaga handledning för handläggning av viseringsansökningar och ändring av utfärdande viseringar” (handledning I om viseringskodexen). I stället har man uppmanat medlemsstaterna att säkra att man verkligen försöker att uppnå bästa möjliga kvalitet genom mätning vid upptagningstillfället och om möjligt applicera samma algoritm för mätning av kvalitet vid upptagning som används centralt vid lagring. Kvaliteten mäts vid lagring och medlemsstaterna delges statistik över uppnådd kvalitet på en summerad nivå.

Migrationsverket har informerat om att myndigheten valt att använda samma kvalitetsprogramvara för fingeravtryck som används i det centrala VIS i de biometristationer myndigheten använder. Med hjälp av denna programvara mäts upptagningen av enskilda fingrar och också summan av alla fingrar på en hand enligt en viktning. Operatören blir uppmanad att ta om avtrycken om kvaliteten är låg och

kan också välja att använda det bästa fingret om flera upptagningar gjorts, allt i syfte att skicka bästa möjliga avtryck till det centrala VIS. Uppföljning av kvalitet på upptagningar görs för att säkerställa att de avtryck som sänds till VIS håller en hög kvalitet, en faktor är operatörens utbildning/motivation/skicklighet. Andra viktiga faktorer är åldern för tredjelandsmedborgaren, yrke, etnicitet och individuella skillnader av annan art. Enligt Migrationsverket har myndigheten säkerställt att utrustningen är av god kvalitet, att processen för upptagning är god samt att mätning av fingeravtryckens kvalitet görs och följs upp.

IMY gör bedömningen att Migrationsverket vidtagit adekvata åtgärder för att säkerställa en god kvalitet på de fingeravtryck som registreras av Sverige i VIS och hanteringen föranleder därför inga synpunkter från IMY.

3.6 Radering av uppgifter i VIS när domstol ändrat ett tidigare avslagsbeslut

Av artikel 25.3 i VIS-förordningen framgår att om ett avslag på en ansökan om visering har upphävts av domstol eller överklagandeinstans ska den medlemsstat som avslog ansökan radera de uppgifter som avses i artikel 12 i VIS-förordningen så snart beslutet att upphäva avslaget har vunnit laga kraft.

Migrationsverket har initialt uppgett att det finns en framtagen manuell rutin för att tillse att en ansökan raderas i enlighet med artikel 25.3 i VIS-förordningen men att det vid myndighetens kontroll framkommit att rutinen inte alltid följts. I september 2021 har Migrationsverket kompletterat med information om att det sedan tidigare finns en funktion i W2 där beslutsfattare vid utlandsmyndigheterna kan ta bort ett beslut från C-VIS. Migrationsverket har nu förtydligat rutinen för hur denna funktion ska användas i enlighet med artikel 25.3 VIS-förordningen. Migrationsverket har också tagits fram ett förslag till hur borttagandet kan automatiseras och informerat om att den it-utveckling som krävs för att införa automatiseringen förväntas kunna genomföras under Q1 2022.

IMY ser positivt på att Migrationsverket förtydligat den manuella rutinen för radering enligt artikel 25.3 i VIS-förordningen och planerna att ta fram en automatiserad rutin och har inga synpunkter på hanteringen.

3.7 Gallring av uppgifter i de nationella informationssystemen

3.7.1 Uppgifter i de nationella systemen

Enligt dataskyddsförordningen, se artiklarna 5.1 b, 5.1 e och 89.1, finns det möjligheter att spara uppgifter för arkivändmål med stöd av nationella bestämmelser. En myndighet är enligt arkivlagen (1990:782) och arkivförordningen (1991:446) skyldig att bevara sina allmänna handlingar och får endast, enligt 14 § arkivförordningen, gallra dessa i enlighet med föreskrifter eller beslut av Riksarkivet, om inte särskilda gallringsföreskrifter finns i lag eller förordning.

Av bilagan till Riksarkivets föreskrift RA-MS 2013:45 avsnitt 5.2.1.6 framgår att Migrationsverket får gallra handlingar i viseringsärenden fem år efter beslutsdatum

Enligt Migrationsverket säkerställer myndigheten, både genom automatisk gallring och manuella rutiner, att handlingar tas bort i nationella informationssystem. Enligt Migrationsverket gallras uppgifter från de nationella operativa systemen efter sex år. Det är viseringshandlingarna som gallras. Viss information, som personinformation och

övergripande information, förs över till ett nationellt e-arkiv, som är en separat databas avskilt från de nationella operativa systemen. Om det finns flera ärenden kopplade till en individ sker gallring när gallringsfristen utgått avseende samtliga viseringsärenden.

Migrationsverkets har uppgett att skälet till att uppgifter gallras efter sex år och inte fem år efter beslutsdatum, som gallringsföreskriften tillåter, är verksamhetsskäl.

IMY har inga synpunkter på det som framkommit i ärendet avseende hur Migrationsverket gallrar viseringsuppgifter respektive för över uppgifter till e-arkivet.

3.7.2 Uppgifter hämtade från C-VIS

Uppgifter som sparas i det nationella systemet kan antingen vara uppgifter som hämtats från den centrala databasen C-VIS och som andra medlemsstaters lagt in eller uppgifter som Sverige lagt in.

I artikel 30.1 VIS-förordningen anges att uppgifter från C-VIS endast får sparas i ett enskilt fall så länge som det är nödvändigt i enlighet med ändamålen med VIS och i enlighet med tillämpliga rättsliga bestämmelser. Av artikel 30.2 framgår att det inte påverkar medlemsstaternas rätt att lagra uppgifter som de har fört in i VIS i sina nationella informationssystem. All användning som inte är förenlig med punkterna 1 och 2 ska, enligt 30.3 VIS-förordningen, betraktas som missbruk enligt varje medlemsstats nationella lagstiftning.

Enligt Migrationsverket sparas inga hämtade uppgifter från C-VIS i de nationella systemen utöver den VisMail-korrespondens som kan finnas i enskilda viserings- och/eller asylärenden. Dessa uppgifter gallras samtidigt som ärendet i dess helhet gallras enligt nationella gallringsregler.

IMY har inga synpunkter på hanteringen.

3.8 Utbildning av personal vid utlandsmyndigheterna

Migrationsverket har under den pågående tillsynen driftsatt en interaktiv dataskyddsutbildning för anställda. Den tillhandahålls till den personal på utlandsmyndigheterna och på Migrationsverket som arbetar i VIS. Utbildningen har funnits tillgänglig sedan slutet av 2020. En uppföljning av vilka som gått utbildningen är planerad som en aktivitet för nästa år. Migrationsverkets dataskyddsombud har ansvaret för uppföljningen.

IMY ser positivt på att Migrationsverket tagit fram en interaktiv utbildning och har inga synpunkter.

3.9 VIS och it-säkerhet

3.9.1 Vad granskningen av it-säkerheten omfattat

Migrationsverket har beskrivit rutinerna för behörighetstilldelning, identifiering av användare, dokumentation över it-arkitekturen, policy för byte av lösenord, kontroller av behörigheter, hanteringen av användarloggar och datakvalitetsgranskningar.

3.9.2 Tillämpliga bestämmelser

De grundläggande principerna för behandling av personuppgifter anges i artikel 5 dataskyddsförordningen. En grundläggande princip är kravet på
säkerhet enligt artikel 5.1 f, som anger att personuppgifterna ska behandlas på ett sätt

som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Av artikel 5.2 dataskyddsförordningen framgår den s.k. ansvarsskyldigheten, dvs. att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna i punkt 1 efterlevs.

Artikel 32 dataskyddsförordningen reglerar säkerheten i samband med behandlingen. Enligt punkt 1 ska den personuppgiftsansvarige, med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken (...). Enligt punkt 2 ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

I artikel 32.2 VIS-förordningen anges närmare krav på it-säkerheten avseende det nationella gränssnittet. Även om artikeln enligt ordalydelsen i artikeln riktar sig till medlemsstaterna ger den vägledning vid tolkningen av artikel 32 dataskyddsförordningen av kravet på att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Migrationsverket är personuppgiftsansvarig för VIS i Sverige och är därmed den myndighet som ytterst ansvarar för att kraven i artikel 32 dataskyddsförordningen och 32.2 VIS-förordningen är uppfyllda.

3.9.3 Dokumentation av it-arkitekturen över VIS
En korrekt och uppdaterad dokumentation över it-arkitekturen är en viktig del i att skydda informationen och it-system och minska risker och sårbarhet t.ex. när personal byts ut eller slutar. Det är en sådan organisatorisk åtgärd som krävs enligt artikel 32 dataskyddsförordningen.

Vid inspektionstillfälle ett överlämnade Migrationsverket ett dokument över it-arkitekturen i VIS som enligt myndigheten inte var färdigställd. Vid inspektionstillfälle tre har Migrationsverket lämnat in en uppdaterad version, som föranletts av ett projekt med syfte att anpassa arkitekturen till ett kommande EU-system. Den uppdaterade versionen av dokumentet speglar enligt Migrationsverket det utseende som den nationella delen av VIS har just nu, men projektet kommer innebära att strukturen görs om.

Den senaste versionen av dokumentet som IMY tagit del av har status ”utkast” angiven i dokumentet och det saknas beslutsdatum i rutan ”beslutad av” och information i rutan ”godkänd av”. Enligt dokumenthistoriken uppdaterades det senast den 3-4 februari 2020.

IMY ifrågasätter inte Migrationsverkets uppgift om att dokumentet är uppdaterat och återger den nuvarande it-arkitekturen. Det finns dock inte någon information i rutan ”godkänd av” och rutan för datum för godkännande, vilket skulle kunna betyda att dokumentet inte formellt är beslutat av myndigheten. Det är inte heller tydligt för den som läser dokumentet att det är uppdaterat och återspeglar nuvarande it-arkitektur.

Enligt IMY är det sannolikt, på grund av oklarheten kring dokumentets status för läsaren, att det kan uppstå felaktigheter vid utvecklingen och förvaltning av VIS, vilket i sin tur kan leda till att Migrationsverket inte vidtar lämpliga tekniska och organisatoriska åtgärder som säkerställer en lämplig säkerhetsnivå enligt artikel 32 dataskyddsförordningen.

3.9.4 Loggning av användaraktiviteter och loggуppföljning

I artikel 32.2 i VIS-förordningen anges att varje medlemsstat ska, med avseende på sitt nationella gränssnitt, vidta de åtgärder som är nödvändiga, inbegripet anta en dataskyddsplan, för att se till att det finns möjlighet att verifiera och fastställa vilka uppgifter som har registrerats i VIS, när detta har gjorts, av vem, och i vilket syfte (kontroll av uppgiftsregistreringen).

Migrationsverket har beskrivit hur loggningen av användaraktiviteter går till. IMY har även vid inspektionstillfälle tre granskat vilka uppgifter som har registrerats i användarloggen avseende två avslutade viseringsärenden.

Migrationsverkets information och IMY:s stickprovskontroll visar att det går att verifiera och fastställa vilka uppgifter som har registrerats i VIS, när detta har gjorts, av vem, och i vilket syfte. IMY har mot den bakgrunden inga synpunkter på loggningen av användaraktiviteter.

3.9.5 Gallring av användarloggar

En användarlogg som sparas längre än vad som är nödvändigt för ändamålet kan i sig innebära en säkerhetsrisk. I bedömningen, enligt artikel 32 dataskyddsförordningen, av lämpliga säkerhetsåtgärder och användarloggar ligger att ta ställning till hur länge det finns ett behov av att spara dessa ur ett it-säkerhetsperspektiv. Enligt principen om lagringsminimering i artikel 5 c dataskyddsförordningen ska personuppgifter inte sparas längre än vad som är nödvändigt för ändamålet.

Enligt Migrationsverket ska användarloggarna gallras efter 10 år, vilket motsvarar preskriptionstiden för grovt dataintrång. Vid inspektion 2 uppgav Migrationsverket att myndigheten ännu inte fått igång någon rutin för gallring av användarloggar. IMY har därefter begärt in uppgift om hur gammal den äldsta loggposten är och fått svar från Migrationsverket att den registrerades 2012-09-01.

På befintligt underlag ifrågasätter inte IMY den valda tidsperioden att spara loggar. IMY konstaterar dock att valet av tidsperiod främst synes bygga på ett informationssäkerhetsperspektiv och inte ett integritetsperspektiv och vill därför understryka att båda perspektiven ska tas i beaktande vid bedömningen.

Vidare kan IMY konstatera att det ännu inte skett någon gallring av användarloggar, vilket förklaras av att den äldsta loggposten registrerades för lite drygt nio år sedan dvs. tiden för gallring har ännu inte passerat. En avsaknad av en rutin för gallring av användarloggar kan, nu när tidpunkten att börja gallra loggar närmar sig, sannolikt leda till en felaktig behandling av personuppgifter dvs. att uppgifter i användarloggar sparas för länge i strid med artikel 5 e dataskyddsförordningen.

4. Val av ingripande

4.1 Rättslig reglering

IMY har ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 dataskyddsförordningen. Om en behandling sannolikt kommer att bryta mot bestämmelserna i dataskyddsförordningen eller kompletterande författningar kan IMY enligt artikel 58.2 a dataskyddsförordningen utfärda en varning.

Övriga korrigerande åtgärder i artikel 58.2 b-j dvs. framförallt reprimand, föreläggande eller administrativa sanktionsavgifter, förutsätter att IMY konstaterat att den personuppgiftsansvarige behandlar personuppgifter i strid med dataskyddsförordningen eller kompletterande författningar.

4.2 Migrationsverket ska tilldelas två varningar

I avsnitt 3.9.3 och 3.9.5 har IMY bedömt att det är sannolikt att Migrationsverkets behandling kan komma att leda till felaktig behandling av personuppgifter. Det är inte fråga om konstaterade brister som kan föranleda reprimand, föreläggande eller administrativa sanktionsavgifter. I övrigt har IMY inte konstaterat någon överträdelse av dataskyddsförordningen. Det innebär att den korrigerande befogenhet som är möjlig för IMY att använda inom ramen för den här tillsynen är varningar.

Båda sannolikheterna är av sådan karaktär att det enligt IMY är motiverat att tilldela en varning för att kommande behandlingar kan komma att stå i strid med artikel 5 e dataskyddsförordningen respektive artikel 32 dataskyddsförordningen.

Detta beslut har fattats av enhetschefen Charlotte Waller Dahlberg efter föredragning av juristen Jonas Agnvall. Vid den slutliga handläggningen av ärendet har även juristerna Lisa Zettervall och It-säkerhetsspecialisten Johan Ma medverkat.

Charlotte Waller Dahlberg, 2021-11-17 (Det här är en elektronisk signatur)

Kopia till:
Dataskyddsombudet