Integritetsskyddsmyndigheten

Vklass AB

Smedjegatan 2c, 1 tr
13154 NACKA

Diarienummer:
IMY-2022-9092

Ert diarienummer:

Datum:
2023-08-24

Beslut efter tillsyn enligt dataskyddsförordningen – Vklass AB

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Vklass AB i egenskap av personuppgiftsbiträde har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen[1]. Det har skett genom att personuppgifter från Vklass AB:s lärplattform Vklass har exponerats öppet på en webbplats på internet under senare delen av 2021 fram till september 2022. Vklass AB har inte vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen och har därigenom inte fortlöpande säkerställt konfidentialiteten för personuppgifterna och skyddat dem mot obehörigt röjande och obehörig åtkomst.

Integritetsskyddsmyndigheten ger Vklass AB en reprimand enligt artikel 58.2 b i dataskyddsförordningen för den konstaterade överträdelsen.

Integritetsskyddsmyndigheten förelägger Vklass AB enligt artikel 58.2 d i dataskyddsförordningen att i enlighet med artikel 32 vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa bolagets (i) förmåga att kunna identifiera avvikande händelser i lärplattformen Vklass samt (ii) förmåga till spårbarhet i lärplattformen i syfte att kunna upptäcka och fastställa orsaken bakom och omfattningen av en inträffad personuppgiftsincident.

Redogörelse för tillsynsärendet

Utgångspunkt för tillsynen

Under september 2022 mottog Integritetsskyddsmyndigheten (IMY) anmälningar om inträffade personuppgiftsincidenter från ett sextiotal personuppgiftsansvariga. De personuppgiftsansvariga bedriver såväl kommunal som privat skol- och utbildningsverksamhet och de använder lärplattformen Vklass (Plattformen) som tillhandahålls av Vklass AB (Vklass eller bolaget) i sina respektive verksamheter. De aktuella personuppgiftsansvariga är, eller har åtminstone varit, kunder till Vklass. Plattformen används i huvudsak för kommunikation mellan elever, deras vårdnadshavare och skolpersonal. Anmälningarna avsåg att personuppgifter kopplade till Plattformen publicerats otillåtet på en webbplats öppet tillgänglig på internet. I

[1] 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).

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

anmälningarna har de personuppgiftsansvariga angett att det skett obehörigt röjande av eller obehörig åtkomst till personuppgifter som behandlas i Plattformen.

Med anledning av de aktuella anmälningarna har IMY inlett tillsyn mot Vklass avseende de personuppgiftsbehandlingar som sker på Plattformen.

Handläggningen har skett genom skriftväxling.

Vad Vklass har uppgett

Vklass har i huvudsak uppgett följande.

Vklass tillhandahåller Plattformen som är en lärplattform för skol- och utbildningsverksamhet. Den används av elever, deras vårdnadshavare och skolpersonal. Vklass är personuppgiftsbiträde åt de kunder (personuppgiftsansvariga) som har lämnat in en anmälan om de inträffade personuppgiftsincidenterna till IMY. Under 2021 hade Vklass 77 kunder och per den 1 oktober 2022 hade Plattformen 427 207 aktiva konton.

Den 21 september 2022 mottog Vklass ett e-postmeddelande från en användare av tjänsten med information om att det på webbplatsen www.zenbase.se (Zenbase) fanns en söktjänst där man kunde söka efter personuppgifter om elever. Flera av uppgifterna verkade härstamma från Plattformen. Samma dag som detta uppdagades skickade Vklass juridiska ombud ett meddelande till aktören bakom Zenbase med en begäran om att upphöra med den otillåtna publiceringen. Aktören bakom Zenbase var en elev som gick på en av de skolor som använder Plattformen. Vidare skickade Vklass ett meddelande till samtliga av sina kunder för att informera om de upptäckta personuppgiftsincidenterna och uppmanade dem samtidigt att göra en anmälan till IMY. Under natten till den 22 september 2022 togs allt innehåll på Zenbase bort.

Efter Vklass efterforskningar kunde bland annat följande konstateras. Det troliga scenariot är att en elev som hade behörighet till Plattformen, själv eller tillsammans med andra, utnyttjat en sårbarhet som tidigare fanns i ett av Plattformens API:er. Eleven har manipulerat API-anrop mot tjänstens adressböcker och sedan sparat ned personuppgifter från Plattformen till en egen databas. På detta sätt har eleven kunnat tillskansa sig mer information från Plattformen än vad dennes åtkomsträttigheter tillåtit. Eleven har sedan byggt Zenbase där de inhämtade uppgifterna har publicerats öppet på internet. Den aktuella sårbarheten är numera åtgärdad till följd av flera förändringar som genomfördes i Plattformen under 2021. Ett annat scenario till att personuppgiftsincidenterna kan ha uppstått är att flera användare från olika skolor har samarbetat genom att hämta uppgifter, som var och en av dem haft behörig tillgång till, då det finns en separation mellan personuppgiftsansvarigas personuppgifter i Plattformen. Uppgifterna har därefter publicerats på Zenbase.

Vklass polisanmälde händelsen och den misstänkte eleven den 22 september 2022. Eleven blev samtidigt avstängd från Plattformen.

Efter Vklass slagningar på Zenbase kunde det konstateras att följande kategorier av personuppgifter om elever och skolpersonal fanns tillgängliga på webbplatsen innan innehållet togs bort:

- för- och efternamn
- smeknamn
- bild

- klass
- e-postadress
- telefonnummer.

Det var endast möjligt att hämta uppgifter om e-postadress och telefonnummer från Plattformen om användaren själv valt att visa den informationen för andra användare som går på samma skola. Vad gäller smeknamn och bild fanns sådan information endast tillgänglig förutsatt att användaren valt att skriva in eller lägga upp detta i Plattformen. Den information som Vklass kunde hitta på Zenbase innefattade i de flesta fall inte uppgifter om telefonnummer, e-postadresser, bilder eller smeknamn. Plattformen är inte utformad för att hantera skyddade personuppgifter.

Uppgifter om smeknamn fanns endast exponerade på två ställen i Plattformen: dels på respektive användares profilsida, dels i Plattformens adressböcker. Vad gäller profilsidorna förs en logg som registrerar när en användare öppnar en sådan sida. Efter en genomsökning av loggarna kunde det konstateras att uppgifterna inte hade hämtats från profilsidorna. Den misstänkte eleven måste därför ha kommit åt dem via Plattformens adressböcker genom att ha utnyttjat den sårbarhet som tidigare fanns i ett av Plattformens API:er.

Det har inte gått att fastställa hur många kunder (personuppgiftsansvariga) som drabbats av ifrågavarande personuppgiftsincidenter. Vklass vet att åtminstone tre kunder har berörts, men troligtvis har fler än så drabbats. Det har heller inte gått att fastställa hur många registrerade som drabbats eller vilken information om dem som hämtats ut då de API-anrop som görs mot Plattformens adressböcker inte loggas.

Det saknas kännedom om de exakta tidpunkterna för när de obehöriga intrången i Plattformen skedde och också under hur lång tid som de pågick. De bedöms dock ha inträffat någon gång under 2021, även om det inte kan uteslutas att de inträffat tidigare än så. Den elev som misstänks ligga bakom intrången hade haft ett konto vid Plattformen sedan 2016. Domännamnet zenbase.se registrerades i juli 2021.

Vklass har ställt frågor till bland annat den misstänkte eleven för att få svar på hur denne gått till väga för att hämta personuppgifterna från Plattformen samt vilka uppgifter som publicerats på Zenbase. Eleven har dock inte återkommit med något svar.

Vad gäller Plattformens säkerhet har det sedan tidigare implementerats flera olika typer av skydd och rekommenderade metoder tillgängliga för den miljö som Vklass använder. Plattformen har bland annat skydd mot överbelastningsattacker och SQL-injektioner[2].

Efter att incidenterna uppdagades har bland annat följande åtgärder vidtagits för att öka säkerhet ytterligare. Det har implementerats en ny funktion som kallas *rate limiting*. Genom denna funktion hindras en enskild användare från att kunna göra för många anrop i Plattformen under ett visst tidsintervall. Om användaren överskrider antalet tillåtna anrop, spärras denne under en viss tid från att kunna göra fler anrop. Detta försvårar exempelvis användningen av skadliga program (skript) som gör automatiserade anrop mot Plattformen i syfte att hämta ut stora mängder information.

[2] IMY:s kommentar: En metod för dataintrång som utnyttjar en sårbarhet i SQL. SQL är ett programmeringsspråk som används för att hämta och modifiera data i en relationsdatabas.

Därtill har det installerats en *bot protection*[3] som är särskilt anpassad för Vklass speciella trafikmönster.

Motivering av beslutet

Allmänt om ansvaret för behandling av personuppgifter
Enligt principen om ansvarsskyldighet i artikel 5.2 i dataskyddsförordningen ska den personuppgiftsansvarige ansvara för efterlevnaden av principerna som beskrivs i första stycket i artikeln, däribland säkerhetsprincipen (artikel 5.1 f i dataskyddsförordningen). Ansvarsskyldighetsprincipen har vidareutvecklats i artikel 24 där det framgår att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Dessa åtgärder ska ses över och uppdateras vid behov. Ansvarsskyldighetsprincipen återspeglas också i artikel 28 som fastställer den personuppgiftsansvariges skyldigheter när denne anlitar ett personuppgiftsbiträde.

Ett personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Personuppgiftsbiträdet är ansvarigt för att följa de bestämmelser i dataskyddsförordningen som riktar sig direkt till biträdet, däribland artiklarna 32 och 33.2. Dessutom kan ett personuppgiftsbiträde bli ansvarigt för överträdelser av dataskyddsförordningen som är en följd av att biträdet inte har efterlevt den personuppgiftsansvariges instruktioner.

Vklass som tillhandahåller och är ansvarig för Plattformen är personuppgiftsbiträde gentemot de utbildningsverksamheter (personuppgiftsansvariga) som använder den. I Plattformen hanteras bland annat personuppgifter om elever, deras vårdnadshavare och skolpersonal.

Personuppgiftsbiträdets skyldighet att underrätta personuppgiftsansvariga
Enligt artikel 33.2 i dataskyddsförordningen ska ett personuppgiftsbiträde utan onödigt dröjsmål underrätta den personuppgiftsansvarige efter att biträdet fått vetskap om att en personuppgiftsincident har ägt rum. Det är sedan den personuppgiftsansvarige som ska bedöma om personuppgiftsincidenten är sådan att den ska anmälas till behörig tillsynsmyndighet. För att den personuppgiftsansvarige ska kunna uppfylla sin anmälningsskyldighet krävs att personuppgiftsbiträdet snabbt underrättar den ansvarige.

Vklass har inte kunnat meddela de personuppgiftsansvariga om de har berörts av incidenten eller inte. Att Vklass inte har kunnat fastställa detta är en brist som i grunden handlar om brister i tekniska och organisatoriska åtgärder vilket redogörs för nedan. IMY konstaterar att Vklass har uppmanat samtliga personuppgiftsansvariga att anmäla en personuppgiftsincident till IMY samt underrättat dem utan onödigt dröjsmål. IMY finner därför inte skäl att kritisera Vklass enligt artikel 33.2 i dataskyddsförordningen.

Skyldigheten att vidta lämpliga tekniska och organisatoriska åtgärder
Både den personuppgiftsansvarige och personuppgiftsbiträdet ska enligt artikel 32.1 i dataskyddsförordningen vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå till skydd för de uppgifter som behandlas. Vid

3 IMY:s kommentar: Bot protection upptäcker och blockerar skadliga botar som obehörigt vill komma åt data på en webbplats eller i en applikation. En bot är ett datorprogram konstruerat för att automatiskt genomföra fördefinierade aktiviteter.

bedömningen av vilka tekniska och organisatoriska åtgärder som är lämpliga ska den personuppgiftsansvarige och personuppgiftsbiträdet beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.

Enligt artikel 32.1 omfattar lämpliga skyddsåtgärder bland annat
a) pseudonymisering och kryptering av personuppgifter,
b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemen och -tjänsterna,
c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och
d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Enligt artikel 32.2 i dataskyddsförordningen ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandlingen medför, i synnerhet för 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.

Vklass är tillhandahållare av Plattformen. Bolaget har i egenskap av personuppgiftsbiträde en skyldighet enligt dataskyddsförordningen att vidta lämpliga skyddsåtgärder för att säkerställa en lämplig säkerhetsnivå för de personuppgifter som Vklass behandlar i Plattformen för de personuppgiftsansvarigas räkning. Vad som är lämpliga skyddsåtgärder ska inte uppfattas som att det är frågan om en godtycklig bedömning utan en bedömning som är adekvat utifrån behandlingens art, omfattning, sammanhang och ändamål samt riskerna för den enskildes fri- och rättigheter.

I detta fall är det frågan om en lärplattform som ska ge elever, deras vårdnadshavare och skolpersonal en kommunikationskanal. Eleverna är i stor utsträckning barn och barns personuppgifter har ett särskilt skydd enligt dataskyddsförordningen (skäl 38). Det är många skol- och undervisningsverksamheter som använder Plattformen och den används dagligen av ett stort antal personer. Vklass har uppgett att fler än 70 olika personuppgiftsansvariga använde Plattformen under 2021 och att Plattformen hade över 400 000 aktiva konton per den 1 oktober 2022.

En av anledningarna till att kommunikationen sker på en särskild plattform och inte på allmänna öppna kanaler är att denna kommunikation behöver kunna ske på ett förtroendefullt sätt och inte vara tillgänglig för alla och envar. Det innebär att oavsett om det rör sig om elever, deras vårdnadshavare eller skolpersonal har de alla rätt att förvänta sig att deras personuppgifter behandlas på ett sätt som säkerställer att dessa uppgifter varken obehörigen röjs eller att någon obehörigen får åtkomst till dem. Att personuppgifter från Plattformen har publicerats på en webbplats, öppen för alla och envar att läsa på internet, har inneburit ett obehörigt röjande av uppgifter enligt dataskyddsförordningen.

Vklass har angett att det troliga scenariot till att de aktuella personuppgiftsincidenterna kunde ske var att en elev med viss behörighet till Plattformen hade utnyttjat en sårbarhet som tidigare fanns i ett av Plattformens API:er. På så vis kunde eleven få tillgång till uppgifterna i de adressböcker som fanns i Plattformen. Vklass har inte själv upptäckt att uppgifter hämtats ut från Plattformen och bolaget har heller inte kunnat ange när de obehöriga intrången skedde eller under hur lång tid de pågick. Vklass utgår från de uppgifter som bolaget hittat efter egna slagningar på Zenbase och

bedömer att dessa har hämtats ut från Plattformen under 2021, även om bolaget inte kan utesluta att det också skett i tiden dessförinnan. Den misstänkte eleven hade haft ett konto vid Plattformen sedan 2016. Vklass känner till att den sårbarhet som misstänks ha utnyttjats åtgärdades under 2021 till följd av olika förändringar som Vklass genomförde i Plattformen.

Vidare har Vklass angett att ett alternativt scenario till de aktuella incidenterna kan vara att flera användare från olika skolor har samarbetat genom att hämta uppgifter, som var och en av dem haft behörig tillgång till i Plattformen, och därefter samlat ihop uppgifterna och publicerat dem på Zenbase.

Vklass känner till att åtminstone tre personuppgiftsansvariga har varit föremål för de aktuella personuppgiftsincidenterna, men misstänker att fler än så kan ha drabbats. Vklass har dock inte kunnat fastställa den fulla omfattningen av incidenterna. Bolaget har uppgett att det varken kan ange vilka personuppgiftsansvariga som påverkats eller vilka personer som har fått sina personuppgifter röjda på Zenbase. Anledningen till detta är att de API-anrop, vilka misstänks ha manipulerats och som görs mot adressböckerna i Plattformen, inte loggas.

Som ovan angetts har Vklass inte själv upptäckt att uppgifterna hämtats ut från Plattformen. Bolaget har inte kunnat redogöra för omfattningen av de aktuella personuppgiftsincidenterna och har heller inte kunnat fastställa den bakomliggande orsaken till dem, dvs. om det har rört sig om en användare som obehörigen hämtat ut information från Plattformen genom manipulerade API-anrop eller om det i stället har varit frågan om flera användare som samarbetat genom att inhämta information som var och en av dem haft behörighet till i Plattformen. Att Vklass inte har kunnat fastställa omfattningen av, eller den bakomliggande orsaken till, personuppgiftsincidenterna tyder på att det har funnits brister i bolagets loggnings- och monitoreringssystem.

Förmåga att ha kontroll över vad som sker, och vad som har skett, i en verksamhets olika IT-system är grundläggande för att upprätthålla säkerheten för de personuppgifter som behandlas där. Detta är av särskild vikt i förhållande till organisationer som tillhandahåller och administrerar IT-system åt andra verksamheter på motsvarande sätt som Vklass gör gentemot sina kunder, dvs. de personuppgiftsansvariga. Det kan konstateras att Vklass saknar en systemövervakning avseende de API-anrop som görs mot Plattformens adressböcker. En adekvat övervakning av denna del av Plattformen hade gett Vklass möjlighet att kunna upptäcka avvikande händelser och identifiera vilka uppgifter som hämtats från Plattformen, vem eller vilka användare som hämtat uppgifterna samt om en användare berett sig tillgång till uppgifter som denne inte haft behörighet att ta del av. Att Vklass inte har kunnat göra detta i relation till de uppgifter som hämtats från Plattformens adressböcker visar på brister i säkerheten samt att Vklass inte haft förmåga att fortlöpande säkerställa konfidentialiteten för personuppgifterna som behandlas i Plattformen och att skydda dem mot obehörigt röjande eller obehörig åtkomst.

Sammanfattningsvis finner IMY att Vklass inte har vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som var lämplig i förhållande till risken med behandlingarna. Anledningen till detta är att Vklass inte haft ett adekvat loggnings- och monitoreringssystem på plats avseende de API-anrop som Plattformens användare gör mot tjänstens adressböcker. Vklass har därmed behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen.

Vklass har i tiden efter att de aktuella personuppgiftsincidenterna uppdagades vidtagit åtgärder för att förbättra säkerheten i Plattformen, bland annat genom att ha implementerat en så kallad *rate limiting* och en specialanpassad *bot protection*. IMY anser att det är positivt att Vklass har stärkt säkerheten i detta avseende och därmed ökat sin skyddsförmåga, men IMY bedömer samtidigt att det fortfarande finns brister vad gäller bolagets interna loggnings- och monitoreringssystem. Att föra erforderliga loggar är en viktig skyddsåtgärd för att kunna kartlägga och fastställa orsaken bakom, och omfattningen av, en inträffad personuppgiftsincident.

Val av ingripande

Av artikel 58.2 i och artikel 83.2 i dataskyddsförordningen framgår att IMY har befogenhet att påföra en administrativ sanktionsavgift. Beroende på omständigheterna i det enskilda fallet ska en administrativ sanktionsavgift påföras utöver eller i stället för de andra åtgärder som avses i artikel 58.2, som t.ex. ett föreläggande eller ett förbud. Vidare framgår av artikel 83.2 vilka faktorer som ska beaktas vid beslut om en administrativ sanktionsavgift ska påföras och vid bestämmande av avgiftens storlek. Om det är frågan om en mindre överträdelse får IMY enligt vad som anges i skäl 148 i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

IMY har konstaterat att Vklass har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen. En överträdelse av den bestämmelsen kan föranleda en sanktionsavgift.

Vid bedömning av överträdelsens allvar kan IMY konstatera att Vklass är en professionell tjänsteleverantör som tillhandahåller och administrerar Plattformen åt utbildningsverksamheter. Det är många verksamheter som använder Plattformen och det finns många registrerade på den som helhet. Många av dessa är barn och därför extra skyddsvärda. Vklass har därmed ett stort ansvar att tillhandahålla en säker tjänst.

Vklass har för de aktuella personuppgifterna saknat systemövervakning avseende de API-anrop som görs mot Plattformens adressböcker. En övervakning som skulle ha gett Vklass möjlighet att upptäcka avvikande händelser och identifiera vilka uppgifter som hämtats från Plattformen. Avsaknaden av en sådan systemövervakning och loggning har lett till att Vklass inte själv har upptäckt incidenterna och att det inte heller kan ange vilka personuppgiftsansvariga eller registrerade som har drabbats eller när detta skett.

Samtidigt kan IMY konstatera att det finns såväl behörighetsstyrning som övervakning och loggning på delar av tjänsten. De olika personuppgiftsansvarigas personuppgifter är separerade och ett uttag omfattande flera personuppgiftsansvariga ska därför inte vara möjligt. De personuppgifter som hämtats från adressböckerna har inte rört känsliga personuppgifter, personnummer eller skyddade personuppgifter. Det har inte heller varit frågan om omdömen eller fritexter, utan de uppgifter som röjts har rört sig om kontaktuppgifter såsom namn och e-postadresser.

IMY kan också konstatera att Vklass agerade direkt när de fick kännedom om incidenterna genom att kontakta samtliga personuppgiftsansvariga som kunde ha drabbats. Vklass kontaktade även Zenbase direkt och uppmanade aktören bakom

webbsidan att upphöra med publiceringen, vilket också skedde. Vklass har därefter vidtagit åtgärder för att förbättra säkerheten genom att implementera *rate limiting* och en specialanpassad *bot protection.*

Sammantaget innebär detta, enligt IMY:s bedömning, att det inte vore proportionerligt att påföra Vklass en sanktionsavgift för den konstaterade överträdelsen. Bolaget ska därför, med stöd av artikel 58.2 b i dataskyddsförordningen, i stället ges en reprimand.

Som konstaterats ovan anser IMY att Vklass fortfarande saknar ett adekvat system för att på ett lämpligt sätt kunna övervaka de personuppgiftsbehandlingar som sker i vissa delar av Plattformen, dvs. Plattformens adressböcker. Av denna anledning anser IMY att det finns skäl att förelägga Vklass enligt artikel 58.2 d i dataskyddsförordningen att vidta tekniska och organisatoriska åtgärder i enlighet med artikel 32 för att säkerställa bolagets förmåga att kunna identifierade avvikande händelser samt förmåga till spårbarhet i Plattformen i syfte att kunna upptäcka och fastställa orsaken bakom och omfattningen av en inträffad personuppgiftsincident. Om API-anrop tillåts till Plattformens adressböcker bör en lämplig åtgärd innefatta bland annat händelseloggning som registrerar användarnas anrop.

Detta beslut har fattats av enhetschefen Katarina Tullstedt efter föredragning av it- och informationssäkerhetsspecialisten Katarina Bengtsson och juristen Per Nydén.

Katarina Tullstedt, 2023-08-24 (Det här är en elektronisk signatur)

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till IMY. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till IMY senast tre veckor från den dag ni fick del av beslutet. Om överklagandet har kommit in i rätt tid sänder IMY det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till IMY om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.