Sjukhusstyrelsen i Region Uppsala

**Diarienummer:**
IMY-2023-2522

**Ert diarienummer:**
SHS2023-00030

**Datum:**
2025-04-24

# Beslut efter tillsyn enligt dataskyddsförordningen – Sjukhusstyrelsen i Region Uppsala

## Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten (IMY) konstaterar att Sjukhusstyrelsen i Region Uppsala från den 25 maj 2018 till den 29 november 2022 i egenskap av personuppgiftsansvarig har behandlat personuppgifter i strid med artikel 32.1 i dataskyddsförordningen genom att inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till riskerna med behandlingen av patienters personuppgifter i verksamhetens e-posttjänst.

IMY ger Sjukhusstyrelsen i Region Uppsala en reprimand med stöd av artikel 58.2 b i dataskyddsförordningen för den konstaterade överträdelsen.

## Redogörelse för tillsynsärendet

### Bakgrund

Sjukhusstyrelsen i Region Uppsala (hädanefter Sjukhusstyrelsen) bedriver och utför vård enligt hälso- och sjukvårdslagen (2017:30), HSL, vid Uppsala Akademiska sjukhus och Lasarettet i Enköping. Den 29 november 2022 mottog IMY en anmälan om en personuppgiftsincident som skett inom ramen för Sjukhusstyrelsens vårdverksamhet. Anmälan avsåg upptäckten att personuppgifter om patienter, innefattande personnummer och uppgifter om hälsa, under perioden 2014–2022, hade behandlats i e-posttjänsten Microsoft Outlook. Enligt anmälan har incidenten berott på bristande organisatoriska rutiner eller processer.

Med anledning av anmälan inledde IMY tillsyn mot Sjukhusstyrelsen i syfte att kontrollera om Sjukhusstyrelsen, i sin verksamhet som utförande vårdgivare enligt HSL, har vidtagit lämpliga åtgärder för att säkerställa skyddet av patienters personuppgifter vid behandling av deras personuppgifter i e-posttjänsten Microsoft Outlook. Som ett led i tillsynen genomfördes den 8 mars 2023 en inspektion på plats i Sjukhusstyrelsens lokaler.

IMY:s granskning omfattar frågan om Sjukhusstyrelsen uppfyller de krav på säkerhet som uppställs i artikel 32 i dataskyddsförordningen avseende behandling av personuppgifter i e-posttjänsten. Prövningen i ärendet har avgränsats till frågan om Sjukhusstyrelsen vidtagit tillräckliga organisatoriska och tekniska åtgärder för att

**Postadress:**
Box 8114
104 20 Stockholm

**Webbplats:**
www.imy.se

**E-post:**
imy@imy.se

**Telefon:**
08-657 61 00

förhindra och upptäcka otillåten personuppgiftsbehandling i e-posttjänsten. Granskningen omfattar inte om behandlingen är förenlig med regleringen i dataskyddsförordningen i övrigt.

Dataskyddsförordningen började tillämpas den 25 maj 2018. IMY:s tillsyn omfattar därför perioden från den 25 maj 2018 till den 29 november 2022 när anmälan om personuppgiftsincident kom in.

## Tidigare beslut

Den 26 januari 2022 utfärdade IMY en administrativ sanktionsavgift mot Sjukhusstyrelsen efter att ha funnit att Sjukhusstyrelsen behandlat personuppgifter i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen genom att ha skickat okrypterade känsliga personuppgifter till patienter och remittenter i tredjeland samt lagrat känsliga personuppgifter i e-posttjänsten (DI-2021-5595). Tillsynen inleddes mot bakgrund av en personuppgiftsincident som inkom till IMY under 2019. IMY bedömde att Sjukhusstyrelsen inte hade vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som var lämplig i förhållande till risken med behandlingen.

## Redogörelse från sjukhusstyrelsen

Inom ramen för tillsynen har Sjukhusstyrelsen bland annat uppgett följande.

**Personuppgiftsansvar**
Sjukhusstyrelsen bedriver och utför vård enligt HSL vid Uppsala Akademiska sjukhus och Lasarettet i Enköping. Sjukhusstyrelsen är personuppgiftsansvarig enligt 2 kap. 6 § patientdatalagen (2008:355), PDL. Den är således personuppgiftsansvarig då den behandlar personuppgifter om patienter enligt ändamålen i 2 kap. 4 § PDL, såsom att dokumentera uppgifter i patientjournal.

**Allmänt om e-posttjänsten**
Inom verksamheterna på Uppsala Akademiska sjukhus och Lasarettet i Enköping används e-posttjänsten Microsoft Outlook sedan 2014. Microsoft tillhandahåller driften av e-posttjänsten i sina datacenter samt ger stöd till Region Uppsalas förvaltningsobjekt Digital arbetsplats som i sin tur administrerar tjänsten inom regionen.

Den aktuella e-posttjänsten har omkring 8 300 användare inom Sjukhusstyrelsens verksamhet, varav majoriteten (ca 6 400) av dessa arbetar med vård.

**Personuppgiftsincidenten**
Vid handläggning av en begäran om registerutdrag den 24 november 2022 upptäcktes att personuppgifter om patienter hade skickats i ett e-postmeddelande mellan medarbetare inom ramen för Sjukhusstyrelsen vårdverksamhet. E-postmeddelandet som lagrats i e-posttjänsten innehöll excel-filer med uppgifter om patienter där det framgick namn, personnummer, antal sjukhusbesök och antal vårddagar.

Sjukhusstyrelsen startade efter denna upptäckt en utredning och fann då ytterligare okrypterade e-postmeddelanden som hade skickats under perioden 2010–2022 innehållandes personuppgifter om patienter. Under utredningen upptäcktes 15 stycken e-postmeddelanden med personuppgifter om patienter samt ett återkommande automatutskick för personnummersammanslagningar.

Det har varit fråga om e-postmeddelanden mellan personal på sjukhusen och det har inte framkommit några indikationer på e-postkonversation direkt mellan vårdpersonal och patienter.

**Tekniska och organisatoriska åtgärder**
Det finns styrande dokumenthanteringsplaner för Uppsala Akademiska sjukhus och Lasarettet i Enköping där det framgår vilka handlingar och informationsmängder som hanteras, i vilka system de ska lagras och hur länge informationen ska bevaras. Det finns även en arkivhandbok som generellt beskriver regler och rutiner för gallring, inklusive gallring av e-post, samt en bevarande- och gallringsplan för administrativa handlingar i vilken anges specifika regler om gallring av e-post.

När ett e-postmeddelande mottas är utgångspunkten att det ska omhändertas och registreras i det system där handlingarna hör hemma. Därefter ska handlingarna raderas från e-posttjänsten. Korrespondens av tillfällig och ringa betydelse kan raderas vid inaktualitet.

På regionövergripande nivå finns riktlinjer och beslut som anger att känsliga uppgifter inte ska hanteras via e-post. Uppsala Akademiska sjukhus och lasarettet i Enköping har var för sig regler för hantering av e-post där det framgår att känsliga uppgifter, såsom sekretessbelagda uppgifter och känsliga personuppgifter, inte får förekomma i e-post såvida filerna inte krypteras. Som standard är e-post krypterad med TLS under transport. Det kan dock inte garanteras att all e-post är krypterad med TLS under transport då denna inställning är beroende på mottagaren/avsändaren. Om e-post används för att skicka känsliga uppgifter ska de krypteras med de krypteringslösningar som Region Uppsala har godkänt för att skicka sådana uppgifter.

Det framgår även i ett regiondirektörsbeslut från år 2019 och i riktlinjen *Informationssäkerhet för medarbetare* att om e-post ska användas för känsliga uppgifter ska informationen krypteras. Andra informationsvägar där vikten av säker e-post poängteras är till exempel chefsbrev och obligatoriska utbildningar.

Trots åtgärderna som vidtagits kan det finnas enskilda individer som av okunskap eller av misstag mejlar känsliga personuppgifter okrypterat. Mognadsnivån gällande säker hantering av känsliga uppgifter upplevs av Sjukhusstyrelsen som hög. Eftersom vårdpersonal inte primärt arbetar i e-posttjänsten finns det dock en risk att rutiner för korrekt handhavande av känslig information blir mindre kända.

Enskilda medarbetares e-postinnehåll övervakas inte. Medarbetare arbetar utifrån ett förtroende som erhålls i samband med anställning att följa de interna regelverken kring lagring och gallring. Det är enbart den enskilde medarbetaren som kommer åt sin e-post och kan radera sina e-postmeddelanden som innehåller känsliga uppgifter.

När en anställd slutar avslutas e-postkontot och all e-post tas bort, men det finns inte någon stadigvarande, teknisk funktionalitet för att automatiskt gallra e-postmeddelanden. Det pågår dock ett arbete för att se över förutsättningarna för gallring av e-post äldre än 2014.

**Åtgärder efter incidenten**
När incidenten upptäcktes anmäldes den till dataskyddsombudet och det kallades till möten för att snabbt utreda omfattningen av incidenten och för att bedöma vad det var för typ av information som hittats. En gruppering tillsattes med ansvar för att hantera incidenten samt identifiera och genomföra de omedelbara åtgärder som krävdes. I det

akuta läget efter att incidenten upptäckts och anmälts gallrades de identifierade e-postmeddelandena. De e-postmeddelanden som tidigare hade automatgenererats togs också bort. Information skickades ut till medarbetarna för att bland annat förtydliga hur känsliga personuppgifter hanteras på rätt sätt.

Sjukhusstyrelsen slutförde under våren 2022 – dvs. efter IMY:s tidigare beslut (DI-2021-5595) – en risk- och sårbarhetsanalys. Detta resulterade i en lista med åtgärder (aktivitetslistan) för att komma till rätta med en rad identifierade risker kopplade till bland annat e-posthantering. I samband med den nu aktuella incidenten gjordes omprioriteringar i det pågående arbetet med aktivitetslistan. Det pågår fortsatt arbete med de åtgärder som identifierats.

Exempel på åtgärder som genomförts är att utreda möjligheter för gallring av delmängder i e-posttjänsten och att införa funktioner i e-posttjänsten som kan upplysa och varna användare som försöker skicka e-post som innehåller personnummer. Möjligheten att skicka säkra meddelanden mellan användare har driftsatts och det pågår även arbete för att ansluta Region Uppsala till den av Myndigheten för digital förvaltning (DIGG) tillhandahållna nationella tjänsten Säker Digital Kommunikation[1]. Vad gäller de automatiska utskicken ska de upphöra i den form som fanns vid incidenten.

# Motivering av beslutet

## Gällande regler

**Den personuppgiftsansvariges ansvar**
Den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter är personuppgiftsansvarig. Om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. Det framgår av artikel 4.7 i dataskyddsförordningen.

Enligt 2 kap. 6 § första stycket PDL är en vårdgivare personuppgiftsansvarig för den behandling av personuppgifter som vårdgivaren utför. I en region och en kommun är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Den personuppgiftsansvarige har ett ansvar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandling av personuppgifter utförs i enlighet med dataskyddsförordningen. Detta framgår av de grundläggande principerna i artikel 5, men regleras även i artikel 24 i förordningen. Åtgärderna ska genomföras med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers fri- och rättigheter. Åtgärderna ska ses över och uppdateras vid behov.

[1] https://www.digg.se/saker-digital-kommunikation

**Kravet på säkerhet vid behandling av personuppgifter m.m.**
Uppgifter om hälsa utgör så kallade känsliga personuppgifter. Det är förbjudet att behandla sådana personuppgifter enligt artikel 9.1 i dataskyddsförordningen, såvida behandlingen inte omfattas av något av undantagen i artikel 9.2 i förordningen.

Av artikel 32.1 i dataskyddsförordningen framgår det att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med personuppgiftsbehandlingen. Det ska ske 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. Detta inbegriper, när det är lämpligt, förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna samt ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Vid bedömningen av lämplig säkerhetsnivå ska 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. Det framgår av artikel 32.2 i dataskyddsförordningen.

I skäl 75 i dataskyddsförordningen anges de faktorer som ska beaktas vid bedömningen av risken för fysiska personers rättigheter och friheter som kan uppkomma vid behandling av personuppgifter. Bland annat ska beaktas om behandlingen gäller personuppgifter om hälsa eller om sårbara fysiska personer, framförallt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

## IMY:s bedömning

**Personuppgiftsansvar**
Sjukhusstyrelsen har uppgett att den bedriver och utför vård vid Uppsala Akademiska sjukhus och Lasarettet i Enköping samt är personuppgiftsansvarig enligt 2 kap. 6 § PDL. Sjukhusstyrelsen är således personuppgiftsansvarig för den personuppgiftsbehandling som Sjukhusstyrelsen utför inom ramen för sin vårdverksamhet, vilket enligt IMY innefattar den personuppgiftbehandling som sker när personuppgifter om patienter inom Sjukhusstyrelsens verksamhet behandlas i e-posttjänsten. Sjukhusstyrelsen är därmed personuppgiftsansvarig för den i ärendet aktuella behandlingen av personuppgifter i e-posttjänsten.

**Tekniska och organisatoriska åtgärder**

*Behandlingen har inneburit en hög risk och krävt en hög skyddsnivå*

Sjukhusstyrelsen bedriver vårdverksamhet vilket innebär att känsliga och särskilt skyddsvärda personuppgifter behandlas inom verksamheten i stor omfattning. IMY kan även konstatera att majoriteten av Sjukhusstyrelsens användare av e-posttjänsten utgörs av ca 6 400 personer som arbetar med vård. Detta innebär en påtaglig risk för att personuppgifter, inklusive känsliga och särskilt skyddsvärda sådana, kan komma att hanteras i e-posttjänsten. Att så är fallet får stöd av att Sjukhusstyrelsen uppgett att

det finns en risk för att en användare av misstag kan skicka känsliga personuppgifter i e-posttjänsten.

Det övergripande syftet med en e-posttjänst är att kunna ta emot, sprida och kommunicera information. IMY har i tidigare tillsyn mot Sjukhusstyrelsen (DI-2021-5595) bedömt att e-postsystem generellt sett är en olämplig lagringsplats för känsliga personuppgifter. Ett e-postsystem är exponerat mot internet vilket innebär att uppgifterna i systemet riskerar att bli åtkomliga för obehöriga. Att det främst är de enskilda användarna som har kännedom om vilka uppgifter användarna hanterar i e-posttjänsten kan vidare medföra svårigheter för den personuppgiftsansvarige att säkerställa att uppgifter inte hanteras i tjänsten på ett otillåtet sätt. Behandling av personuppgifter i en e-posttjänst innebär således i sig särskilda risker.

Mot denna bakgrund anser IMY att det måste ställas höga krav på de tekniska och organisatoriska åtgärder som Sjukhusstyrelsen behöver vidta för att säkerställa en lämplig säkerhetsnivå avseende behandling av personuppgifter i e-posttjänsten.

*Sjukhusstyrelsen har inte vidtagit tillräckliga säkerhetsåtgärder*

Som framgår av artikel 32.2 i dataskyddsförordningen ska vid bedömningen av lämplig säkerhetsnivå särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlats. Den personuppgiftsansvarige ska alltså vidta åtgärder för att i möjligaste mån undvika personuppgiftsincidenter.[2]

Åtgärderna kan bland annat inbegripa förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna samt ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Det är mot denna bakgrund av vikt att den personuppgiftsansvarige vidtar åtgärder för att kunna förhindra och upptäcka otillåten behandling av personuppgifter.

Av utredningen i ärendet framgår att det under den i ärendet aktuella tidsperioden funnits centrala dokument och regler som tillämpas inom Sjukhusstyrelsens verksamhet och som bland annat tar sikte på hantering av handlingar och informationsmängder samt hantering av personuppgifter i e-post. I dessa framgår bland annat att integritetskänsliga uppgifter såsom personnummer, sekretessbelagda uppgifter och känsliga personuppgifter inte får förekomma i e-post såvida filerna inte krypteras med den krypteringslösning som godkänts. Anställda får även genomgå obligatoriska utbildningar, bland annat avseende informationssäkerhet och hantering av personuppgifter i e-posttjänsten.

Sjukhusstyrelsen hade alltså vidtagit ett antal åtgärder för att förhindra otillåten behandling av personuppgifter i e-posttjänsten. Mot bakgrund av att det vid den i ärendet aktuella personuppgiftsincidenten framkom att känsliga och särskilt skyddsvärda personuppgifter behandlats i e-posttjänsten framgår det dock att medarbetare inte följt de riktlinjer som funnits avseende behandling av sådana personuppgifter i e-posttjänsten. Det kan även konstateras att det funnits uppsatta

[2] EU-domstolen dom den 14 december 2023, Natsionalna agentsia za prihodite, mål C-340/21, ECLI:EU:C:2023:986, punkt 30.

tjänster för automatiska utskick som kontinuerligt skickade personuppgifter om patienter via e-post i strid med riktlinjerna.

De åtgärder som vidtagits för att förhindra otillåten personuppgiftsbehandling i e-posttjänsten har enligt IMY främst omfattats av organisatoriska säkerhetsåtgärder med exempelvis regler, riktlinjer och utbildning för hur personal som arbetar inom verksamheten ska hantera känsliga uppgifter. Sjukhusstyrelsen har visserligen efter den inträffade incidenten bland annat vidtagit ett antal tekniska åtgärder för att förhindra otillåten behandling, till exempel avseende funktioner för att upplysa och varna användare som försöker skicka e-post som innehåller personnummer. Några sådana funktioner fanns dock inte på plats vid tidpunkten för incidenten.

Flera av de e-postmeddelanden som omfattades av incidenten hade lagrats i e-posttjänsten under lång tid, vilket talar för att Sjukhusstyrelsen inte haft ett effektivt förfarande för att kunna följa upp och utvärdera effektiviteten av de åtgärder som vidtagits. Även den omständigheten att upptäckten av en stor mängd känsliga och särskilt skyddsvärda personuppgifter som behandlats under en längre tid i e-posttjänsten skedde vid handläggning av en begäran om registerutdrag talar för en avsaknad av proaktiva åtgärder för att upptäcka otillåten behandling. IMY konstaterar vidare att det vid tidpunkten för personuppgiftsincidenten varit upp till enskilda medarbetare att upptäcka och radera e-postmeddelanden som innehåller känsliga eller särskilt skyddsvärda personuppgifter.

Sammantaget bedömer IMY att Sjukhusstyrelsen inte vidtagit tillräckliga åtgärder för att förhindra och upptäcka otillåten personuppgiftsbehandling i e-posttjänsten. Sjukhusstyrelsen har därmed från den 25 maj 2018 till den 29 november 2022 i egenskap av personuppgiftsansvarig behandlat personuppgifter i strid med artikel 32.1 genom att inte ha vidtagit lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till riskerna med behandlingen av patienters personuppgifter i e-posttjänsten.

## 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 till exempel förelägganden och 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. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans. Om det är fråga 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.

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

Sjukhusstyrelsen har under den i ärendet aktuella perioden inte vidtagit tillräckliga tekniska och organisatoriska åtgärder för att förhindra och upptäcka otillåten personuppgiftsbehandling i e-posttjänsten. De otillräckliga åtgärderna har lett till att en stor mängd känsliga och särskilt skyddsvärda personuppgifter behandlats i

e-posttjänsten i strid med Sjukhusstyrelsens riktlinjer. Sjukhusstyrelsen har i ett tidigare tillsynsbeslut från IMY ålagts att betala en administrativ sanktionsavgift för bland annat överträdelse av artikel 32.1 vid hantering av personuppgifter i e-posttjänsten (DI-2021-5595). Sjukhusstyrelsen slutförde efter IMY:s tidigare beslut en risk- och sårbarhetsanalys som resulterade i en aktivitetslista för att komma till rätta med identifierade risker kopplade till bland annat e-postanvändning. I samband med den i detta ärende aktuella personuppgiftsincidenten gjordes omprioriteringar i det pågående arbetet med aktivitetslistan. Av aktivitetslistan framgår både genomförda och planerade tekniska och organisatoriska åtgärder som bland annat syftar till att öka förmågan att förhindra och upptäcka otillåten behandling av personuppgifter. Sjukhusstyrelsen har även beslutat om upphörande av de automatiska utskicken med personnummersammanslagningar i den form som var aktuell vid incidenten.

Vid en sammantagen bedömning av omständigheterna i ärendet bedömer IMY att det inte är proportionerligt att besluta om sanktionsavgift för den överträdelse som konstaterats inom ramen för denna tillsyn. Sjukhusstyrelsen ska därför, istället för sanktionsavgift, ges en reprimand enligt 58.1 b i dataskyddsförordningen.

---

Detta beslut har fattats av enhetschefen Christelle Bourquin efter föredragning av it- och informationssäkerhetsspecialisten Johnny Gordon Tornesjö. Vid den slutliga handläggningen av ärendet har även avdelningsjuristen Andreas Persson medverkat.

Christelle Bourquin

**Kopia till**
Dataskyddsombudet

# 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 inom tre veckor från den dag ni fick del av beslutet. Om ni är en part som företräder det allmänna ska överklagandet dock ha kommit in inom tre veckor från den dag då beslutet meddelades. 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.