

Lars Lind
Uppsala universitet

Diarienummer:
IMY-2026-8907

Datum:
2026-06-24

Förhandssamråd enligt dataskyddsförordningen

Sammanfattande råd

Integritetsskyddsmyndigheten (IMY) lämnar enligt artikel 36 i dataskyddsförordningen¹ följande råd med anledning av Uppsala universitets begäran om förhandssamråd. Råden ges utifrån den konsekvensbedömning och övrigt underlag som Uppsala universitet har gett in till IMY.

- Utveckla den systematiska beskrivningen av personuppgiftsbehandlingen i konsekvensbedömningen
- Ta fram lättbegriplig, skriftlig information om personuppgiftsbehandlingen till de registrerade
- Utvärdera och överväga andra lämpliga tekniska åtgärder som ett alternativ till den planerade token-baserade autentiseringen med länk via e-post
- Utveckla konsekvensbedömningen vad gäller de åtgärder som planeras för att hantera risker i insamlingsfasen
- Bedöma pseudonymiseringen i ljuset av alla åtgärder som vidtas
- Säkerställa att det regelbundet kontrolleras om behandlingen genomförs i enlighet med konsekvensbedömningen och att det sker en översyn om risker förändras

Bakgrund

Uppsala universitet har den 7 maj 2026 begärt förhandssamråd om en planerad behandling av personuppgifter inom ramen för en forskningsstudie (EpiHealth). Studien har till syfte att undersöka hur livsstilsfaktorer påverkar sjukdomar som astma, hjärt-kärlsjukdom och demens. Undersökningen planeras att genomföras som en webbenkät riktad till cirka 25 000 individer som sedan tidigare deltar i forskningsstudien. Den planerade personuppgiftsbehandlingen är omfattande och inbegriper hälsouppgifter.

Skyldigheten att begära förhandssamråd

En konsekvensbedömning ska enligt 35.1 i dataskyddsförordningen genomföras om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

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).

fysiska personers rättigheter och friheter. Konsekvensbedömningen ska göras av den personuppgiftsansvarige före behandlingen.

Om konsekvensbedömningen visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvariga vidtar åtgärder för att minska risken, ska den personuppgiftsansvariga samråda med tillsynsmyndigheten före behandlingen. Denna skyldighet att begära förhandssamråd regleras i artikel 36 i dataskyddsförordningen.

Om tillsynsmyndigheten anser att den planerade behandlingen skulle strida mot dataskyddsförordningen, särskilt om den personuppgiftsansvarige inte i tillräcklig mån har fastställt eller reducerat risken, ska myndigheten ge den personuppgiftsansvarige skriftliga råd. Tillsynsmyndigheten får då utnyttja alla de befogenheter som den har enligt artikel 58. Detta framgår av artikel 36.2 i dataskyddsförordningen.

Uppsala universitetets redogörelse

Behandlingen av personuppgifter

Uppsala universitet fungerar som personuppgiftsansvarig för personuppgiftsbehandlingen, i nära samarbete med Lunds universitet.

Uppsala universitet utför behandlingen för att utföra en uppgift av allmänt intresse enligt artikel 6.1 e i dataskyddsförordningen. Uppgiften att bedriva högkvalitativ forskning är fastställd i högskolelagen (1992:1434) och utgör en central del av lärosätets uppdrag. Deltagarna i studien har i samband med första undersökningen gett samtycke till att bli kontaktade för uppföljningar.

Webbenkäten ska riktas till cirka 25 000 individer som sedan tidigare deltar i forskningsstudien och som är medelålders eller äldre. Enkäten innehåller frågor om ett brett spektrum av medicinska och psykosociala förhållanden som sjukdomshistoria, mental hälsa, reproduktiv hälsa, levnadsvanor och fysiska besvär. Enkäten innehåller även andra integritetskänsliga personuppgifter som personnummer, socioekonomiska uppgifter, arbetsmiljö och boendeuppgifter.

Deltagarna ska få en inbjudan via post eller e-post med information om studien och en länk till webbenkäten. Autentisering sker via en unik, personlig länk (token) som skickas till deltagarens e-postadress. Planen är inte att använda tvåfaktorsautentisering (2FA), e-legitimation (BankID, Freja eID+) eller annan stark autentisering. När deltagaren fyller i enkäten sparas svaren krypterat i REDCap-databasen vid Uppsala Clinical Research Center. Detta möjliggör att deltagaren kan återvända och fortsätta fylla i enkäten via samma länk vid ett senare tillfälle. Datan skickas sedan via krypterade kanaler (TLS) från deltagarens webbläsare till universitetets servrar. Uppgifterna lagras i REDCap-miljön (KRT 3:3:1-klassificerade servrar) där logiska kontroller utförs. Efter avslutad insamling ersätts personnumret med ett löpnummer. Kodnyckeln arkiveras säkert i en separerad miljö. Forskare får tillgång till det pseudonymiserade datasetet.

Konsekvensbedömning och kvarvarande risker

Uppsala universitets konsekvensbedömning omfattar den digitala processen för datainsamling som planeras ske via enkätverktyget REDCap, lagringen av dessa data på dedikerade servrar vid Uppsala universitet och den efterföljande hanteringen av data för forskningsändamål.

Enligt Uppsala universitets interna riktlinjer för informationssäkerhet klassificeras insamlingen av informationen till den högsta säkerhetsklassen (KRT 3:3:1-klassificerad information). Enligt riktlinjerna ska informationen åtkomstskyddas med stark autentisering på BankID-nivå (så kallad tvåfaktorsautentisering eller 2FA). Den planerade lösningen med token-baserade e-postlänkar uppfyller inte dessa krav.

Universitetets val att inte använda 2FA motiveras av följande överväganden:

- Risk för exkludering av en vetenskapligt viktig undergrupp av äldre deltagare som saknar tillgång till eller förmåga att använda BankID.
- Risk för lägre svarsfrekvens som försämrar studiens vetenskapliga värde.
- REDCap-miljön saknar etablerad och validerad integration med BankID/Freja eID+ för externa deltagare.

Följande tekniska och organisatoriska åtgärder planeras för att minska riskerna:

- Unik, personlig länk (token): varje deltagare tilldelas en unik URL. Länken är bunden till deltagarens personnummer i REDCap.
- Tidsbegränsade sessioner: automatisk utloggning vid inaktivitet för att minska risken med kvarglömda öppna sessioner.
- KRT 3:3:1-klassificerade lagringssystem: data lagras efter insamlingsfasen i en REDCap-miljö med krypterade diskar.
- Kryptering av datatrafik: TLS 1.3 och certifikatskontroller.
- Pseudonymisering: efter insamlingsfasen ersätts personnummer med löpnummer i forskningsmiljön. Kodnyckeln förvaras separat.
- Rollbaserad behörighetsstyrning och loggning: REDCap konfigureras för loggning av varje åtkomst till känsliga fält. Behörigheter ses över kvartalsvis.
- Pappersenkät som alternativ: deltagare som saknar eller inte vill använda digital åtkomst erbjuds pappersenkät.

Trots dessa riskreducerande åtgärder finns två kvarvarande risker:

- Obehörig åtkomst via e-postlänk: en person med tillgång till deltagarens e-postkorg kan följa länken och ta del av den sparade enkätsessionen med mycket känsliga hälsouppgifter.
- Identitetssäkring: token-baserad åtkomst verifierar inte vem som faktiskt svarar. Enkäten kan i princip fyllas i av en annan person utan att det går att upptäcka i efterhand. Det leder också till problem om en deltagare behöver återkontakts p.g.a. fynd i studien.

Ramarna för IMY:s yttrande

Det är upp till Uppsala universitet att säkerställa att samtliga höga risker har identifierats och hanteras i enlighet med dataskyddsförordningen. IMY:s yttrande har utformats utifrån de av Uppsala universitet identifierade risker, de frågor som har ställts och det underlag som har getts in.

Uppsala universitets fråga om hur avvägningen ska göras mot kravet på inkludering och representativitet i epidemiologisk forskning om IMY bedömer att stark autentisering behövs, besvaras inte i detta yttrande. Det stämmer visserligen att en pappersenkät kan utgöra ett alternativ som kan vägas in i proportionalitetsbedömningen men det ingår inte i IMY:s uppdrag eller expertis att t.ex. göra en bedömning av representativitet i epidemiologisk forskning.

IMY:s yttrande

1. Utveckla konsekvensbedömningen (råd 1)

Enligt artikel 35.7 a i dataskyddsförordningen ska konsekvensbedömningen avseende dataskydd innehålla en systematisk beskrivning av den planerade behandlingen av personuppgifter och behandlingens syften. Den ska tydligt, och så heltäckande som möjligt, beskriva behandlingens art, omfattning, sammanhang, ändamål, nödvändiga resurser, funktionell beskrivning av behandlingen och roller och ansvarsfördelning.²

IMY ser positivt på att Uppsala universitet har utvecklat behovet av konsekvensbedömningen och generellt på ett tydligt sätt har beskrivit den planerade behandlingen.

IMY råder Uppsala universitet att fördjupa bedömningen och klargöra behandlingens omfattning på ett så heltäckande sätt som möjligt genom att till exempel nämna det stora antalet registrerade och den totala mängden av personuppgifter som kommer att behandlas under avsnittet som handlar om den systematiska beskrivningen av personuppgiftsbehandlingen. I denna del kan även tydliggöras vilka forskare som kommer att ha åtkomst till uppgifterna och om det endast rör sig om forskare som är kopplade till Uppsala universitet eller även sådana som finns hos Lunds universitet. Uppsala universitet bör också klargöra om universitetet ensamt eller tillsammans med någon annan aktör bestämmer ändamålen och tillvägagångssätten för behandlingen av personuppgifterna samt om personuppgifter kommer att överföras till externa mottagare.

2. Skriftlig information till de registrerade (råd 2)

De registrerade har rätt att få information om när och hur deras personuppgifter behandlas. Information om behandlingen av personuppgifter, inklusive hur längre personuppgifterna kommer att lagras, ska lämnas av den personuppgiftsansvariga både när uppgifterna samlas in och när den registrerade begär det. De registrerade har också rätt att få information om sina rättigheter. Informationen ska vara koncise och begriplig och den ska presenteras i lätt tillgänglig form med användning av klart och tydligt språk. Dessa skyldigheter framgår av artikel 12–15 i dataskyddsförordningen.

Den Europeiska dataskyddstyrelsen, EDPB, ger i sina riktlinjer om personuppgiftsbehandling för forskningsändamål exempel på hur information bäst lämnas till de registrerade. När personuppgiftsbehandling för forskningsändamål sker över lång tid rekommenderas bland annat att de registrerade ska få välja kontaktväg (e-post, brev eller telefon). Det rekommenderas också att tillhandahålla en webbsida eller applikation för information om personuppgiftsbehandlingen samt en kontaktpunkt för de registrerade att kunna ställa frågor och kunna utöva sina rättigheter.³

IMY råder Uppsala universitet att ta fram lättbegriplig, skriftlig information om den planerade personuppgiftsbehandlingen och att säkerställa att deltagarna kan ta del av informationen på ett enkelt sätt. Informationen bör tas fram med särskilt beaktande av

² Se även IMY:s Vägledning vid konsekvensbedömning. En praktisk guide, februari 2025: [Konsekvensbedömning enligt GDPR | IMY](#) (i synnerhet avsnitt 3.2 och 3.7).

³ Europeiska dataskyddstyrelsens (EDPB:s) riktlinjer (1/2026) om behandling av personuppgifter för forskningsändamål, antagna den 15 april 2026, p. 78–79 och 81. Notera att riktlinjerna för närvarande är under publik konsultation.

hälsouppgifternas känsliga karaktär. Informationen bör även innehålla uppgifter om de registrerades rättigheter och instruktioner för hur rättigheterna kan utövas.

3. Regelbunden kontroll och översyn (råd 3)

Av artikel 35.11 i dataskyddsförordningen följer en skyldighet att vid behov kontrollera om behandlingen genomförs i enlighet med konsekvensbedömningen och se över om risker förändras. Att löpande se över sina konsekvensbedömningar och behandlingar är viktigt för att bibehålla nivån på uppgiftsskyddet över tid. Kravet på regelbunden översyn av konsekvensbedömningen gäller utöver den översyn som måste göras om riskbilden förändras.⁴

IMY vill understryka vikten av att uppföljning och översyn av risker sker kontinuerligt så länge behandlingen pågår. Uppsala universitet har uppgett att deltagarnas uppgifter planeras att lagras i REDCap-miljön. Forskare kommer att få tillgång till det pseudonymiserade datasetet. Behörigheter till REDCap ses över kvartalsvis men det har till exempel inte framkommit om Uppsala universitet planerar för till exempel en årlig uppföljning av konsekvensbedömningen.

Utöver kontrollen av behörigheter till REDCap råder IMY därför Uppsala universitet att ta fram en plan om hur Uppsala universitet kommer att kontrollera att behandlingen genomförs i enlighet med konsekvensbedömningen och om risker förändras. Det framgår inte av konsekvensbedömningen hur länge personuppgifterna kommer att lagras. Det bör anges när och hur ofta konsekvensbedömningen ska följas upp samt vilka roller eller funktioner i organisationen som ansvarar för uppföljningen. Det bör även beskrivas hur det ska säkerställas att eventuella förändringar av risken fångas upp inom organisationen.

4. Andra lämpliga tekniska åtgärder (råd 4)

Uppsala universitet har frågat IMY om det planerade tillvägagångssättet att skicka en unik länk via e-post till webbenkätens deltagare utgör en lämplig teknisk åtgärd enligt artikel 32 i dataskyddsförordningen.

Uppgifter om hälsa utgör s.k. känsliga personuppgifter. Det är förbjudet att behandla sådana särskilda kategorier av personuppgifter enligt artikel 9.1 i dataskyddsförordningen, såvida behandlingen inte omfattas av något av undantagen i artikel 9.2. Dessa uppgifter anses extra skyddsvärda eftersom behandling kan innebära betydande risker för enskildas grundläggande rättigheter och friheter.⁵

Enligt artikel 24.1 i dataskyddsförordningen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen, där åtgärderna ska ses över och uppdateras vid behov. Vidare framgår av artikel 32.1 i dataskyddsförordningen att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå till skydd för personuppgifterna. Vid bedömningen av vilka åtgärder som är lämpliga ska den personuppgiftsansvarige beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för

⁴ Jfr Artikel 29-gruppens Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen "sannolikt leder till en hög risk" i den mening som avses i förordning 2016/679, 17/SV, antagna den 4 april 2017 och reviderade den 4 oktober 2017 s. 14.

⁵ Se skäl 51 i dataskyddsförordningen.

fysiska personers rättigheter och friheter. I artikeln nämns exempel på lämpliga skyddsåtgärder:

- Pseudonymisering och kryptering av personuppgifter.
- Förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna.
- Förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident.
- 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 enligt artikel 32.2 i dataskyddsförordningen särskild hänsyn tas till de risker som behandlingen medför, i synnerhet för oavsiktlig eller olaglig förstörelse, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Det är den personuppgiftsansvarige som enligt artikel 32 i dataskyddsförordningen är ansvarig för säkerheten vid personuppgiftsbehandling. Av det skälet är det också den personuppgiftsansvarige som behöver bedöma de risker som är förknippade med den planerade behandlingen av personuppgifter och vidta lämpliga tekniska och organisatoriska åtgärder för att hantera de risker som identifieras. Vad som utgör lämpliga åtgärder ska inte uppfattas som en fråga om godtycklig bedömning utan bedömningen ska vara adekvat utifrån behandlingens art, omfattning, sammanhang och ändamål samt riskerna för den enskildes fri- och rättigheter.

I detta fall är det fråga om en webbenkät där deltagarna ska lämna ett stort antal hälsouppgifter. Behandlingen är enligt Uppsala universitets egna riktlinjer av synnerligen känslig karaktär. Att det rör sig om behandling av känsliga personuppgifter innebär att det ställs högre krav på de tekniska och organisatoriska åtgärder som den personuppgiftsansvarige ska vidta. Mot denna bakgrund är det av central betydelse att kunna säkerställa deltagarnas identitet (och att svaren kan knytas till rätt person på ett rättssäkert sätt). Den enda praktiskt genomförbara lösningen som uppfyller dessa krav är användning av e-legitimation, som till exempel BankID eller Freja eID. Detta eftersom dessa tjänster ger hög identitetsgaranti och möjliggör säker återinloggning och spårbar autentisering. Därför bör e-legitimation vara primär autentiseringsmetod när det ska behandlas känsliga personuppgifter för forskningsändamål.

Det finns andra metoder som Uppsala universitet kan utvärdera utifrån ett säkerhetsperspektiv. Några metoder som har mycket hög nivå på säkerhet och spårbarhet är:

- Digital brevlåda — Elektronisk leverans av inloggningskod eller länk till användarens säkra brevlåda. Ger starkare leveransbindning än vanlig e-post eftersom åtkomst normalt kräver verifierad inloggning hos brevlådeleverantören och leveransen lämnar spårbar kvittens.
- FIDO2 / passkeys (WebAuthn) — Nyckelbaserad autentisering som använder offentlig/privat afi och är i praktiken phishing-resistent. Fördelen är hög säkerhet och god användarupplevelse i moderna webbläsare och mobila enheter.
- Hårdvarunyckel (FIDO2) — Fysisk säkerhetsnyckel som lagrar privata nycklar lokalt och kräver fysisk närvaro vid inloggning. Mycket hög säkerhet och motståndskraft mot nätfiske.

- TOTP-authenticator — Tidsbaserade engångskoder genererade lokalt på användarens enhet genom en app. Ger bättre säkerhet än SMS eftersom koden inte transporteras över mobilnätet.

Dessa metoder, som också redovisas i den sammanfattande tabellen i bilagan till detta yttrande, kräver olika mycket av sändare och mottagare i forskningsstudien.

Deltagarna lämnar ut känsliga och andra integritetskänsliga personuppgifter om sig själv inom ramen för forskningsstudien. Deltagarna är medelålders och äldre. Äldre personer tillhör en grupp av sårbara personer. Det kan därför argumenteras att deltagarna bör ges möjligheten att använda en säkerhetsmetod som de känner sig bekväma med.

IMY råder mot ovan bakgrund Uppsala universitet att utvärdera och överväga lämpliga tekniska åtgärder som ett alternativ till den planerade token-baserade autentiseringen med länk via e-post. På så sätt kan Uppsala universitet bedöma om de tekniska och organisatoriska åtgärder som hittills har vidtagits är sådana att det har gjorts vad som ankommer universitetet för att minimera risker för de registrerades fri- och rättigheter.

5. Hantera risker i insamlingsfasen (*råd 5*)

Uppsala universitet undrar om token-baserad åtkomst via e-post, utan ytterligare verifiering av att rätt individ besvarar enkäten, kan uppfylla krav på riktighet enligt artikel 5.1 d och krav på säkerhet enligt art. 32 i dataskyddsförordningen vid behandling av uppgifter som ska länkas mot nationella register via personnummer.

Utöver de bestämmelserna som nämns under 4.1 finns ytterligare rättsliga utgångspunkter. Ansvarsskyldigheten i artikel 5.2 i dataskyddsförordningen innebär att den personuppgiftsansvarige ska ansvara för och kunna visa att principerna i artikel 5.1 efterlevs. En av dessa principer är principen om riktighet enligt artikel art. 5.1 d i dataskyddsförordningen som innebär att personuppgifter ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Enligt artikel 35.7 led d ska konsekvensbedömningen avseende dataskydd innehålla information om de åtgärder som planeras för att hantera riskerna. Det kan vara fråga om skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att dataskyddsförordningen följs.

Enligt Uppsala universitets konsekvensbedömning finns kvarvarande höga risker med den planerade behandlingen som inte kan elimineras utan att antingen använda stark autentisering eller acceptera ett säkerhetsglapp vid insamlingen av personuppgifterna.

IMY utgår inledningsvis ifrån att Uppsala universitet planerar att använda sig av på förhand verifierade mejl eller telefonnummer när universitetet skickar ut inbjudan att delta i webbenkäten. Detta för att minska risken för att en annan person än den tilltänkta deltagaren tar emot inbjudan.

Ovan under avsnitt 4.2 nämnda alternativa metoder till e-legitimation är utformade utifrån säkerheten för användarna. Dessa metoder gör dock inget för att verifiera identiteten av användaren. I dagsläget är det enbart BankID och Freja ID som kan utföra verifieringen av deltagarnas identitet och därmed uppfylla kravet på riktighet, och att svaren kan knytas till rätt person. Det av Uppsala universitet planerade

tillvägagångsätt med token-baserad åtkomst via e-post möjliggör alltså inte någon verifiering av vem som är mottagare av enkäten och vem som avslutar enkäten. Med en alternativ metod som t.ex. hårdvarunyckel finns möjlighet att verifiera vem som har börjat och avslutat enkäten. Inte heller den metoden garanterar dock att det är rätt person som fyller i enkäten.

IMY konstaterar att de riskreducerande åtgärderna som har beskrivits i konsekvensbedömningen inte är kopplade till insamlingsfasen utan främst är kopplade till behandlingen av personuppgifter efter insamlingsfasen. Uppsala universitet bör därför utveckla konsekvensbedömningen med information om vilka åtgärder som planeras att vidtas för att hantera riskerna i insamlingsfasen. Det som behöver göras är en sammantagen riskbedömning. Denna ska utgå ifrån en riskanalys. Först ska risker identifieras. Sedan ska en bedömning göras av sannolikheten för och allvarlighetsgraden om riskerna inträffas. Efter det ska en handlingsplan med riskreducerande åtgärder upprättas.⁶

Det innebär bland annat att Uppsala universitet bör bedöma hur stor sannolikheten är att en annan person än den tilltänkta deltagaren fyller i enkäten, de konsekvenser det kan få för den tilltänkta deltagaren i forskningsstudien om enkäten fylls i av en annan person samt väga detta mot riskreducerande åtgärder. Att använda sig av en metod som möjliggör verifiering av deltagarens identitet utgör i det sammanhanget en riskreducerande åtgärd.

IMY rekommenderar Uppsala universitet att använda Excelbladet Riskhantering vid konsekvensbedömning som finns på IMY:s webbsida. Ytterligare vägledning finns på IMY:s webbsida.

6. Bedöma pseudonymiseringen (råd 6)

Uppsala universitet har ställt frågan om data som har den högsta säkerhetsklassificeringen men som pseudonymiseras kan klassas om till en lägre säkerhetsklassificering eller om ovanliga kombinationer av känsliga uppgifter kan göra att personer ändå kan identifieras.

Pseudonymisering är behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.⁷

Enligt EDPB bör personuppgifter som behandlas för vetenskaplig forskning i första hand anonymiseras, om syftet med behandlingen kan uppfyllas med hjälp av anonymiserade uppgifter.⁸ Pseudonymiserade uppgifter, som kan hänföras till en individ genom användning av ytterligare information, förblir information relaterad till en identifierbar fysisk person och är därför fortfarande personuppgifter.

⁶ IMY:s Vägledning vid konsekvensbedömning som finns på myndighetens webbsida utgör en praktisk guide, med rättsligt tolkningsstöd i en bilaga och flera mallar: [Konsekvensbedömning enligt GDPR | IMY](#). Se i synnerhet mallen som rör riskhantering vid konsekvensbedömning.

⁷ Artikel 4,5 i dataskyddsförordningen.

⁸ Europeiska dataskyddsstyrelsens (EDPB:s) riktlinjer (01/2025) för pseudonymisering, antagna den 16 januari 2025, p. 156. Notera att riktlinjerna har varit på publik konsultation och att riktlinjerna kommer att uppdateras.

Pseudonymisering kan användas som en av flera åtgärder som bidrar till en säkerhetsnivå som är anpassad till risken i samband med databehandlingen, i enlighet med artikel 32.1 i dataskyddsförordningen. Pseudonymisering kan mildra konsekvenserna av obehörig åtkomst till uppgifter. Personuppgiftsansvariga och personuppgiftsbiträden måste fortfarande tillhandahålla en säkerhetsnivå som är anpassad till de kvarvarande riskerna som är förknippade med behandlingen av de pseudonymiserade uppgifterna.⁹

Enligt EDPB är pseudonymisering ett värdefullt verktyg, men är det ofta mest effektivt när det kompletteras med ytterligare åtgärder. De personuppgiftsansvariga måste bedöma lämpligheten hos alla sina åtgärder sammantaget för att fastställa om de är tillräckliga för att uppfylla de relevanta dataskyddskraven.¹⁰

Beroende på vilka metoder som används kan pseudonymisering – genom att tilldela personer med likartade identifierade egenskaper vitt skilda pseudonymer – minska risken att personuppgifter felaktigt tillskrivs en registrerad.¹¹ Hur effektivt pseudonymiseringen genomförs avgör i vilken utsträckning riskerna för de registrerade minskas och vilka fördelar den personuppgiftsansvarige kan dra av detta, bland annat när det gäller att uppfylla dataskyddsskyldigheterna enligt artiklarna 24 och 32 i dataskyddsförordningen.¹²

Pseudonymisering kan alltså minska risker för de registrerades fri- och rättigheter. Frågan om pseudonymisering är bra nog för en viss klassificering påverkas i detta fall bland annat av vilka rådata som finns, hur stark kodnyckeln är och vad som är kvar i det pseudonymiserade datasettet som indirekt gör att man kan identifiera en deltagare trots god nyckelhantering.

IMY råder därför Uppsala universitet att bedöma pseudonymisering i ljuset av de åtgärder som vidtas och fastställa om dessa är tillräckliga för att uppfylla dataskyddskrav. Det ankommer på Uppsala universitet att bedöma hur personuppgifter som pseudonymiseras med den planerade metoden med kodnyckeln ska klassificeras.

6. Avslutande synpunkt

IMY vill framhålla att detta yttrande inte utgör en prövning av hela personuppgiftsbehandlingen i sak. Inom ramen för förhandssamråd lämnas inget förhandsgodkännande till en planerad personuppgiftsbehandling.

Med detta svar avslutas ärendet.

⁹ Europeiska dataskyddsstyrelsens (EDPB:s) riktlinjer (01/2025) för pseudonymisering, antagna den 16 januari 2025, p. 59.

¹⁰ Europeiska dataskyddsstyrelsens (EDPB:s) riktlinjer (01/2025) för pseudonymisering, antagna den 16 januari 2025, p. 44.

¹¹ Jfr Europeiska dataskyddsstyrelsens (EDPB:s) riktlinjer (01/2025) för pseudonymisering, antagna den 16 januari 2025, p. 29.

¹² Jfr Europeiska dataskyddsstyrelsens (EDPB:s) riktlinjer (01/2025) för pseudonymisering, antagna den 16 januari 2025, p. 30 och se avsnitt 3.1.

Detta yttrande har beslutats av enhetschefen Albin Brunskog efter föredragning av juristen Ninke Liebert. Enhetschefen Christelle Bourquin och IT- och informationssäkerhetsspecialisten Andreas Majunie har medverkat under handläggningen.

Albin Brunskog

Bilaga

Sammanfattande tabell av några metoder

BILAGA: Sammanfattande tabell

Metod	Identitetsgaranti	Risk för felaktig mottagare	Möjlighet till återupptagning	Säkerhet
BankID / Freja eID	Ja	Nej	Ja; säker återautentisering	Mycket hög
Engångskod via digital brevlåda	Nej	Nej	Ja; kod kan användas för återupptagande	Mycket hög
Hårdvarunyckel	Nej	Ja	Ja; kräver fysisk nyckel vid återinloggning	Mycket hög
TOTP authenticator	Nej	Ja	Ja; kodbaserat återupptagande möjligt	Mycket hög
SMS OTP	Nej	Ja	Ja; men sårbart för kapning	Låg
E-post engångskod	Nej	Ja	Ja; men risk för sessionskapning	Medel
Papperskod via post	Nej	Ja	Ja; kod kan användas för återupptagande	Hög