Datatilsynet

UNIVERSITETET I AGDER
Postboks 422
4604 KRISTIANSAND S

Deres referanse	Vår referanse	Dato
	24/00793-9	04.09.2024

Vedtak om overtredelsesgebyr - Universitetet i Agder

Vi viser til vårt varsel om vedtak om overtredelsesgebyr 28. juni 2024. Universitetet i Agder (heretter UiA) sendte inn melding om brudd på personopplysningssikkerheten (avviksmelding) 14. februar 2024. Vi har ikke mottatt kommentarer fra UiA til vårt varsel.

1. Vedtak om overtredelsesgebyr

Datatilsynet har i dag fattet følgende vedtak:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26, jf. personvernforordningen artikkel 83, pålegges Universitetet i Agder å betale et overtredelsesgebyr på 150 000 NOK – hundreogfemtitusen norske kroner – til statskassen, for overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32 og artikkel 24.*

2. Beskrivelse av avviket

2.1 Generelt om avviket

Ifølge avviksmeldingen, har dokumenter med personopplysninger vært lagret i åpne Teams-mapper, hvor ansatte uten tjenstlig behov har hatt tilgang. Det var en ansatt som oppdaget avviket etter å ha søkt i åpne Teams-mapper. Avviket hadde pågått fra 2018, da UiA tok i bruk Microsoft Teams og Sharepoint.

14. februar 2024 ble det avdekket fire dokumenter i Microsoft Teams med manglende tilgangskontroll og som inneholdt personopplysninger om ansatte og studenter:

I Et dokument med oversikt over alle ansatte og eksterne personer tilknyttet universitetet tilbake til 2014. Dette gjelder 4 851 ansatte og 10 419 eksterne personer som er nevnt ved navn, med fødsels- og personnummer, ansattnummer, fratredelsesdato og organisasjonsenhet. Alle ansatte har hatt tilgang til dokumentet.

II Et dokument med oversikt over 568 studenter som har fått tilrettelagt eksamen. Dokumentet inneholder navn, fødsels- og personnummer, studentnummer, spesialtilpasningskode, fritekst om hva tiltaket gjelder og dato. Alle ansatte har hatt tilgang til dokumentet.

III I det offentlige teamet «Akademisk dugnad – Ukraina» har det ligget oversikt over 64 flyktninger fra Ukraina med fullt navn, adresse, studentnummer, fødselsdato, telefonnummer, tidligere utdanningsbakgrunn, studieretning, hvorvidt de har meldt seg til Lånekassen, planlagt studieforløp og bosettingsstatus. Det har vært mulig for både ansatte og studenter å få tilgang til mappen.

IV Liste over ansatte på biblioteket knyttet til et prosjekt fra 2015. Listen inneholdt opplysninger om navn, bostedsadresse og fødsels- og personnummer. Alle ansatte har hatt tilgang til dokumentet.

Den 16. februar 2024 avdekket UiA fem nye dokumenter i Microsoft Teams uten tilgangskontroll:

V En liste fra 2014 der en ekstern praksislærer blir omtalt som «sykemeldt høst 2014». Informasjonen har vært tilgjengelig for alle ansatte ved universitetet.

VI Et dokument med 177 av studentenes navn, fødselsnummer, UiA e-postadresse, privat e-postadresse og eksamensmelding. Listen har vært tilgjengelig for alle ansatte.

VII En liste med oversikt over 60 studenters navn, fødselsnummer, studentnummer og eksamensforsøk. Dokumentet har vært tilgjengelig for alle ansatte.

VIII Liste over 13 studenter med opplysninger om navn, fødselsnummer og adresse. Listen har vært tilgjengelig for alle ansatte.

IX Liste med oversikt over 40 studenters navn, eksamensemne og type særordning. Listen har vært tilgjengelig for alle ansatte.

Avviket omfatter både alminnelige personopplysninger og personopplysninger av særlig kategori. De alminnelige personopplysningene består blant annet av elevers og ansattes kontaktopplysninger, fødselsnummer, utdanningsinformasjon og bosettingsstatus for flyktninger, eksamensmelding og antall eksamensforsøk. I tillegg, vil informasjon om studenters tilrettelegging av eksamen, særordning knyttet til studieemne, samt opplysning om sykemelding knyttet til en ansatt, innebære behandling av helseopplysninger.

2.2 Tilgangskontroll

Åpne Teams-mapper er noe hver enhet ved UiA bruker for å kunne dele dokumenter ved internt samarbeid på tvers av enhetene. Avviket har oppstått som følge av at sluttbrukerne ikke har vært klar over at dokumenter lagret i «delte dokumenter» eller «Public Teams» blir delt med alle ansatte i virksomheten. Totalt er det snakk om ni dokumenter uten tilgangskontroll. Alle de ni dokumentene har vært tilgjengelige for alle ansatte. Studenter har også hatt mulighet for tilgang til mappen som inneholder opplysninger om 64 ukrainske flyktninger.

2.3 Loggkontroll
Avviksmeldingen opplyser om at det var loggkontroll av tilgangen til dokumentene for seks måneder tilbake i tid. For det aktuelle avviket kan derfor ikke UiA bekrefte eller avkrefte om uvedkommende faktisk har hatt tilgang, gjort endringer eller lastet ned dokumenter for største delen av avviksperioden.

2.4 Interne rutiner for lagring og skjerming
UiA hadde ingen interne rutiner for eller opplæring i skjerming av dokumenter i Microsoft Teams (Sharepoint).

2.5 Iverksatte og planlagte tiltak
Avviket ble først meldt internt av en ansatt som oppdaget avviket gjennom søk i åpne grupper i Microsoft Teams. UiA gjennomgikk alle delte mapper og rettet opp i tilgangsstyringen umiddelbart. Alle offentlige team i Microsoft Teams ble gjort private, slik at ansatte som ønsker tilgang må godkjennes av teamets eier. Det er sendt ut informasjon til ansatte om trygg lagring i Microsoft Teams.

2.6 Informasjon til de registrerte
UiA kontaktet de berørte registrerte den 21. februar 2024.

I tillegg, har UiA lagt ut detaljert informasjon om avviket på sine nettsider. Det har også vært flere mediesaker som omhandler avviket.

3. Rettslig bakgrunn

Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personvern-forordningen artikkel 57.

3.1 Grunnprinsippene for behandling av personopplysninger
De grunnleggende prinsippene for behandling av personopplysninger fremgår av personvernforordningen artikkel 5. Vi viser særlig til artikkel 5 nr. 1 bokstav f, hvor det fremgår:

> «1. Personopplysninger skal (…)
> f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling (…), ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)».

Det er den behandlingsansvarliges ansvar at prinsippene overholdes, og den behandlingsansvarlige skal kunne påvise dette, jf. artikkel 5 nr. 2.

3.2 Kravene til personopplysningssikkerhet og styringssystemer
Personvernforordningen artikkel 32 regulerer kravene til sikkerhet ved behandlingen av personopplysninger. Under følger et utdrag av relevante deler av artikkel 32:

«1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet, (…)
b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene, (…)
d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av (…) ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».

Plikten til å gjennomføre egnede tekniske og organisatoriske tiltak fremgår tilsvarende av personvernforordningen artikkel 24, som regulerer den behandlingsansvarliges ansvar særskilt.

3.3 Informasjon til berørte personer

Dersom det er sannsynlig at sikkerhetsbruddet vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette de berørte personene om bruddet, jf. personvernforordningen artikkel 34 nr. 1.

Tilsynsmyndigheten kan pålegge den behandlingsansvarlige å informere berørte personer, jf. artikkel 34 nr. 4. De nærmere kravene til innholdet i en slik underretning fremgår av artikkel 34 nr. 2 og 3.

3.4 Særlig om ileggelse av overtredelsesgebyr

Av personvernforordningen artikkel 58 nr. 2 bokstav i og personopplysningsloven § 26 annet ledd, fremgår det at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83 ved brudd på bestemmelser i de respektive lovene.

I personvernforordningen artikkel 83 angis vilkårene for ileggelse av gebyr. Bestemmelsen inneholder blant annet en oversikt over hvilke momenter det skal tas hensyn til, både når det vurderes hvorvidt overtredelsesgebyr skal ilegges og i utmålingen av gebyret.
De relevante delene av artikkel 83 nr. 1 og nr. 2 gjengis under:

«1. Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.

2. (…) Når det treffes avgjørelse om hvorvidt det skal ilegges overtredelsesgebyr samt om overtredelsesgebyrets størrelse, skal det i hvert enkelt tilfelle tas behørig hensyn til følgende:

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,
b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt,
c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd,
d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32,
e) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren,
f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den,
g) kategoriene av personopplysninger som er berørt av overtredelsen,
h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen,
i) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes,
j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42 og
k) enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen».

Artikkel 83 angir også rammene for overtredelsesgebyrets størrelsesorden. Vi viser i denne forbindelse til artikkel 83 nr. 4. De relevante delene av bestemmelsene lyder:

«4. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 10 000 000 euro […]:

a) den behandlingsansvarliges og databehandlerens forpliktelser i henhold til artikkel 8, 11, 25-39 […]».

I personopplysningsloven § 26 første ledd fremgår det at personvernforordningen artikkel 83 nr. 4 gjelder tilsvarende for overtredelser av forordningen artikkel 24. Dette vil si at brudd på personvernforordningen artikkel 24 etter norsk rett kan sanksjoneres med overtredelsesgebyr på opptil et beløp som tilsvarer 10 millioner euro.

4. Datatilsynets vurdering

I redegjørelsen for vår vurdering, vil vi følge samme kronologi som under punkt 2 *beskrivelse av avviket* over.

4.1 Tilgangskontroll
Avviket representerer et brudd på plikten til å bevare personopplysningers konfidensialitet som følge av at ansatte på UiA har hatt tilgang til personopplysninger uten tjenstlig behov. Det har i tillegg vært en mappe med personopplysninger om 64 ukrainske flyktninger som har vært lagret tilgjengelig for alle studenter. Ifølge UiAs nettsider, er det omtrent 1 200 ansatte og 12 000 studenter tilknyttet universitetet.

Personopplysningene har ligget lett tilgjengelig inne i Microsoft Teams, og ansatte har kunnet få tilgang gjennom søk i åpne Teams-mapper.

Vi legger til grunn at UiA har brutt sin plikt til å sørge for tilgangsstyring som en del av sin internkontroll og plikt til å ivareta tilstrekkelig personopplysningssikkerhet, jf. personvernforordningen artikkel 32 og artikkel 24.

4.2 Loggkontroll
UiA har ikke hatt tilstrekkelig funksjon for loggføring av aktivitet i Microsoft Teams. Loggkontrollen som har vært etablert har vist aktivitet seks måneder tilbake i tid, men logg over oppslag utover dette finnes ikke.

Datatilsynet vurderer at UiA har brutt sin plikt til å ha funksjon for loggføring i store deler av avviksperioden på seks år. På denne måten har det ikke vært mulig å avdekke uautorisert tilgang til personopplysningene, jf. personvernforordningen artikkel 32 og artikkel 24.

4.3 Interne rutiner for lagring og skjerming
Avviket illustrerer at UiA har hatt utilstrekkelige interne rutiner og opplæring av de ansatte i forbindelse med skjerming av personopplysninger i Microsoft Teams.

Vi understreker at det er ledelsens ansvar å iverksette tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder interne rutiner for sikker lagring og tilstrekkelig opplæring av ansatte.

UiA har ikke iverksatt egnede tiltak for å ivareta personopplysningssikkerheten i Microsoft Teams. Dette er et brudd på personvernforordningen artikkel 32 og artikkel 24.

4.4 Iverksatte og planlagte tiltak
UiA iverksatte strakstiltak etter at avviket ble oppdaget og meldte avviket raskt inn til Datatilsynet. Vi ser positivt på at alle tilganger til delte mapper nå er stengt og informasjon om skjerming av personopplysninger ved bruk av Microsoft Teams er kommunisert til alle ansatte.

Datatilsynet har ellers ingen merknader til de iverksatte tiltakene.

4.5 Informasjon til de registrerte

UiA har informert de berørte registrerte etter personvernforordningen artikkel 34.

4.6 Oppsummering

Ledelsen ved UiA har en lovpålagt plikt til å sørge for at ansatte ikke har tilgang til personopplysninger de ikke har tjenstlig behov for. I tillegg, skal det etableres systemer for logging og etterfølgende kontroll som blant annet gjør det mulig å avdekke avvik.

Det er et ledelsesansvar at tekniske og organisatoriske løsninger er på plass slik at universitetet er i stand til å håndtere sensitive personopplysninger på en tilstrekkelig sikker måte.

Datatilsynet vurderer at det har vært grunnleggende mangler ved internkontrollen og personopplysningssikkerheten knyttet til ansattes bruk av Microsoft Teams.

4.7 Vurdering av skyldkravet for ileggelse av overtredelsesgebyr

For at Datatilsynet skal kunne ilegge UiA et overtredelsesgebyr, kreves det at den eller de som har opptrådt på vegne av universitetet har utvist en form for skyld, jf. personvernforordningen artikkel 83, jf. sak C-807/21 (*Deutsche Wohnen*). I denne saken er vår vurdering at den aktuelle skyldformen er simpel uaktsomhet.

Bestemmelsen om uaktsomhet er lovhjemlet i straffeloven § 22, som uttrykker at:

> «Den som handler i strid med kravet til forsvarlig opptreden på et område, og som ut fra sine personlige forutsetninger kan bebreides, er uaktsom».

I henhold til kravet om aktsomhet, må virksomheter sette seg inn i hvilken lovgivning som gjelder på området og innrette virksomheten i samsvar med de rammer som følger av det aktuelle regelverket.

I den aktuelle avvikssaken, har UiA erkjent manglende tilgangskontroll i delte mapper i Microsoft Teams. Det har heller ikke vært etablert tilstrekkelig loggføring for størstedelen av avviksperioden på seks år. Vi legger til grunn at kravene til internkontroll og informasjonssikkerhet er et ledelsesansvar, jf. personvernforordningen artikkel 5 nr. 2.

Som følge av de nevnte manglene, er Datatilsynet av den oppfatning av at lovbruddet må betegnes som uaktsomt.

Skyldkravet for å ilegge overtredelsesgebyr er dermed oppfylt.

4.8 Vurdering av om overtredelsesgebyr skal ilegges

Datatilsynet har kommet til at UiA har brutt personvernforordningen artikkel 32 og artikkel 24. Det foreligger derfor et lovbrudd som kan gi grunnlag for ileggelse av overtredelsesgebyr.

Nedenfor gjennomgår vi de momentene som vi anser relevante for vurderingen av om overtredelsesgebyr skal ilegges jf. personvernforordningen artikkel 83 nr. 4.

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd

Avviket representerer et alvorlig brudd på personopplysningssikkerheten ved at personopplysninger om ansatte og studenter har vært tilgjengelig for ansatte uten tjenstlig behov i en periode på seks år. Avviket innebærer at omtrent 1 200 ansatte har hatt tilgang til ni dokumenter med personopplysninger av ulik grad av sensitivitet. I tillegg er det omtrent 12 000 studenter som har hatt tilgang til et dokument med opplysninger om 64 ukrainske flyktninger.

Det er totalt sett et stort antall personopplysninger som omfattes av avviket, herunder kontaktopplysninger, fødselsnummer til 16 000 ansatte og studenter, informasjon om tilrettelegging av eksamen for 568 studenter, utdanningsinformasjon og bosettingsstatus for 64 ukrainske flyktninger, opplysning om sykemelding knyttet til én ansatt, særordning i studieemne for 40 studenter og antall eksamensforsøk for 60 studenter.

Fødsels- og personnummer er ikke i seg selv taushetsbelagte opplysninger eller opplysninger med krav om ekstra beskyttelse under personvernforordningen artikkel 9. Likevel er det klare grenser for når fødselsnummer lovlig kan tas i bruk etter personopplysningsloven § 12[1].

Integritetsbruddet har ført til at de registrerte har mistet kontroll over sine egne personopplysninger, herunder hvorvidt personopplysninger har blitt spredd videre til uvedkommende. Personopplysningene har vært lett tilgjengelig i Microsoft Teams, og ansatte har gjennom søk i delte mapper/grupper hatt enkel mulighet for tilgang. Det har til enhver tid kun vært loggkontroll seks måneder tilbake i tid.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Vi viser til vår vurdering under punkt 4.7 og vår konklusjon om at lovbruddet må anses som uaktsomt av ledelsen ved UiA.

Saken viser at UiA ikke har hatt tilstrekkelige rutiner for og opplæring i bruk av Microsoft Teams, og UiA må iverksette tiltak for å sikre seg mot slike brudd på personopplysningssikkerheten.

c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd

UiA har raskt lukket avviket og meldt bruddet til Datatilsynet. De berørte registrerte mottok informasjon om avviket allerede en uke etter avviket ble oppdaget, enten gjennom direkte kontakt eller gjennom informasjon på nettside og i mediene. UiA har også iverksatt tiltak for å bedre personopplysningssikkerheten. Dette taler i formildende retning.

[1] Bestemmelsen legger til grunn at fødselsnummer kun kan brukes når det er saklig behov for sikker identifisering av en person og når fødselsnummeret er nødvendig for å oppnå slik identifisering.

d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32

UiA har ikke overholdt sine plikter til å etablere egnet informasjonssikkerhet og internkontroll ved bruk av Microsoft Teams. Datatilsynet mener at avviket representerer grunnleggende mangler ved tilgangskontroll og interne rutiner/opplæring knyttet til UiAs bruk av Microsoft Teams. Funksjon for loggkontroll har heller ikke vært tilstrekkelig, da denne kun har hatt dokumentasjon seks måneder tilbake i tid.

f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den

Datatilsynet mottok raskt melding om brudd på personopplysningssikkerheten og har blitt løpende orientert i avvikssaken med utfyllende informasjon.

g) kategoriene av personopplysninger som er berørt av overtredelsen

Det faktum at avviket omfatter særlige kategorier av personopplysninger gjør situasjonen mer alvorlig. Vi har blitt opplyst om at avviket omfatter et dokument med informasjon om en sykemeldt ansatt. I et annet dokument fantes det opplysninger om tilrettelagt eksamen for 568 studenter, herunder opplysninger om spesialtilpasning med fritekst. Denne informasjonen vil ofte avsløre helseopplysninger. I et annet dokument var det oversikt over om særordning i studieemner for 40 studenter, som også kvalifiserer som helseopplysninger.

I tillegg, omfatter avviket omtrent 16 000 fødsels- og personnummer, som ikke faller innenfor vernet under personvernforordningen artikkel 9, men som er særlig beskyttet i loven og innebærer en viss risiko for misbruk.

Det er videre uheldig at opplysninger om bosettingsstatus, tidligere utdanning og nåværende utdanningsløp for 64 ukrainske flyktninger har ligget tilgjengelig i en åpen mappe for både ansatte og studenter. Til sammen utgjør dette 13 200 personer som i teorien kan ha hatt tilgang til opplysningene.

Alt i alt gjelder avviket et stort omfang av personopplysninger, til dels av svært sensitiv karakter.

h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen

UiA meldte selv fra om avviket til Datatilsynet, i tråd med plikten i personvernforordningen artikkel 33.

Datatilsynets oppsummering og vurdering

UiA er pålagt å sørge for at ansatte ikke har tilgang til personopplysninger de ikke har tjenstlig behov for. Dette innebærer å ha gode rutiner og opplæring av ansatte i skjerming av personopplysninger i systemene universitetet benytter. I tillegg, foreligger det en plikt til å etablere systemer for logging og etterfølgende kontroll som gjør det mulig å avdekke avvik.

Datatilsynet ser positivt på at det ble iverksatt tiltak for å stanse eksisterende praksis umiddelbart etter at avviket ble oppdaget.

Avviket representerer et brudd på konfidensialiteten til personopplysningene til flere av studentene ved UiA. Opplysningene har vært lagret relativt lett tilgjengelig samt består av en stor mengde personopplysninger av sensitiv art. En spredning av fødselsnummer innebærer også en viss risiko for misbruk. Personopplysningene som har manglet tilgangskontroll er gjerne opplysninger man ønsker å holde for seg selv, som for eksempel antall forsøk en student har hatt på eksamen.

Basert på en samlet vurdering, mener vi at avviket er av en så alvorlig karakter at det er nødvendig å ilegge UiA et overtredelsesgebyr.

4.9 Gebyrets størrelse

I vurderingen av gebyrets størrelse, har vi sett hen til at UiA raskt sørget for skjerming av personopplysningene som var tilgjengelige og informerte de registrerte. UiA har raskt meldt fra om avviket og samarbeidet med Datatilsynet under sakens gang.

I denne avvikssaken har en stor mengde personopplysninger vært tilgjengelig for 1 200 ansatte uten tjenstlig behov i en periode på seks år. Det er tale om personopplysninger knyttet til omtrent 14 000 personer. Avviket har avdekket manglende opplæring og uklare rutiner ved skjerming av personopplysninger i Microsoft Teams.

Det er store mengder fødsels- og personnummer som omfattes av avviket. Et anslag viser at det er snakk om omtrent 16 000 slike nummer.

Datatilsynet har kommet til at et overtredelsesgebyr på 150 000 NOK er rimelig i denne saken.

5. Klageadgang

Vedtaket om overtredelsesgebyr kan påklages **innen tre uker** etter at dere har mottatt dette brevet, jf. forvaltningsloven §§ 28 og 29.

En eventuell klage sendes til Datatilsynet. Dersom vi opprettholder vår avgjørelse, vil vi sende saken til Personvernnemnda for klagebehandling, jf. personopplysningsloven § 22.

Dersom dere har spørsmål, kan dere kontakte oss på e-post postkasse@datatilsynet.no.

Med vennlig hilsen

Camilla Nervik
seksjonssjef

Kristin Skolt
juridisk rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: UNIVERSITETET I AGDER, Johanne Lavold
UNIVERSITETET I AGDER, Trond Hauso