Datatilsynet

NTNU - Det medisinske fakultet

Norges Idrettsforbund

Olympiatoppen Midt-Norge

[redacted]

Deres referanse	Vår referanse	Dato
2016/11434/HESK	16/00824-4/TJU	20.07.2016

Varsel om overtredelsesgebyr - Misbruk av kamerasystem - NTNU - Olympiatoppen

1. Sakens bakgrunn

Datatilsynet har mottatt en avviksmelding og en etterfølgende redegjørelse fra NTNU, Det medisinske fakultet. Avviket gjelder uautorisert innsyn i og utlevering fra fire kameraer i et idrettslaboratorium. Vi legger til grunn at NTNU og Olympiatoppen Midt-Norge sammen er behandlingsansvarlige for kamerasystemet.

En beskrivelse av avviket følger i punkt 3. NTNU stiller spørsmål om hvordan varsling til de berørte skal skje og når skjermbildene og videoklippene skal slettes. Vi kommenterer dette i punkt 4 om avvikshåndtering. I punkt 5 gjør vi rede for reglene om informasjonssikkerhet som vi mener er brutt i dette tilfellet. I punkt 6 og 7 begrunner vi overtredelsesgebyret. I punkt 8 finnes frist for tilsvar til dette varselet.

2. Varsel om overtredelsesgebyr

Dette er et varsel om at Datatilsynet vil ilegge følgende overtredelsesgebyr:

> *Med hjemmel i personopplysningsloven § 46 første ledd vil NTNU og Norges idrettsforbund og olympiske og paralympiske komité ved Olympiatoppen Midt-Norge sammen pålegges å betale et overtredelsesgebyr til statskassen stort 100 000 kroner for å ha behandlet personopplysninger uten å utføre risikovurdering, jf. personopplysningsforskriften § 2-4, jf. personopplysningsloven § 13, ved å sette et kamerasystem i bruk uten forutgående risikovurdering, og for ikke å ha iverksette tilstrekkelige sikkerhetstiltak, jf. personopplysningsforskriften § 2-14, jf. personopplysningsloven § 13, ved å la kamerasystemet ligge åpent tilgjengelig på nettverket.*

3. Beskrivelse av avviket

Det er snakk om ett avvik fordelt på to hendelser.

Avviket gjelder uautorisert innsyn i og utlevering fra fire kameraer i et idrettslaboratorium leid av NTNU og en treningssal leid av Olympiatoppen Midt-Norge (heretter OLT). Kameraene er OLTs eiendom og koblet til NTNUs nett. Kameraene brukes som del av tilbudet i treningssal og idrettslaboratorium og brukes typisk for å filme utøveres teknikk for forsknings- og treningsformål. Kamerasystemet ble satt i drift i mars 2014.

Manglende sikkerhetstiltak førte til at en ukjent aktør mellom mars 2014 og 6. august 2015 skaffet seg tilgang til kameraene og styringssystemet. Aktøren har tatt opp flere videoer av brukere i treningsaktivitet, og videoene er tatt opp på en måte som kan defineres som seksualisert. Ansikter er gjenkjennbare. Det kan heller ikke utelukkes at utøvere har blitt filmet i bar overkropp eller at det har vært barn tilstede.

6. august 2015 ble NTNU gjort kjent med at tre bilder fra kameraene ble publisert på Facebook (hendelse 1). 3. mai 2016 ble det oppdaget flere bilder og videoer på fildelingstjenesten [redacted] (hendelse 2). Man antar at disse bildene og videoene ble tatt opp før 6 august 2015 slik at det ikke er snakk om et nytt avvik. NTNU kjenner til totalt ni videoklipp og åtte skjermbilder, men det kan finnes flere.

Etter hendelse 1 ble kamerasystemet skrudd av, og nettverkskoblingen ble endret ved at det ble opprettet et VLAN med privatadresser. Dette ble vurdert til å være tilstrekkelig sikkert, og kamerasystemet ble tatt i bruk igjen. Avviket ble ikke meldt inn til Datatilsynet i påvente av ytterligere sikkerhetstiltak. NTNU har beklaget dette.

Etter hendelse 2 ble kameraene på nytt skrudd av. Hendelsen ble politianmeldt, men politiet har henlagt saken. Avviksmelding ble gitt til Datatilsynet muntlig 3. mai 2016 og skriftlig 18. mai 2016. Videre ble kamerasystemet risikovurdert. Kamerasystemet er nå tilbake i drift. NTNU planlegger å flytte PC/server fysisk til IT på Det medisinske fakultet, iverksette fysisk sikring av PC/server som driver kamerasystemet, montere fysiske brytere på kamerasystemet (det vil ikke lenger være mulig å bruke kameraene uten aktivt å skru dem på) og å utbedre skilting av lokalene.

Antall avbildede personer er syv ved hendelse 1 (hvorav to er identifiserte) og 17 ved hendelse 2 (hvorav åtte er identifiserte). De identifiserte har blitt varslet muntlig og/eller i brevs form. NTNU har videre opplysninger fra bookingsystemet som sammen med medlemslister kan gi en oversikt over personer som har planlagt bruk av lokalene i perioden avviket fant sted. NTNU har imidlertid ingen oversikt over hvorvidt personene faktisk har vært i lokalene. Videre er det sannsynlig at personer som ikke hadde planlagt bruk har benyttet seg av lokalene. I dag har ca. 70 personer tilgang til lokalene, og det er ikke uvanlig at personer med tilgang har med seg besøkende.

Om årsaken til avviket skriver NTNU: «Årsaken til avviket er menneskelig svikt. Kamerasystemet er montert uten en grundig nok sikkerhetsvurdering. NTNU kan ikke gjøre rede for at systemet er dokumentert risikovurdert i tråd med egne rutiner. Dette vil bli gjort før systemet settes tilbake til ordinær drift.»

4. Avvikshåndtering

NTNU har beklaget at avviket ikke ble meldt inn tidligere. Vi har valgt å ikke legge vekt på at avviksmelding ble inngitt sent i vurderingen av overtredelsesgebyr. Det betyr at når vi har vurdert om overtredelsesgebyr skal gis og hva størrelsen på det skal være, har ikke dette vært et moment i vurderingen.

NTNU har iverksatt og er i ferd med å iverksette sikkerhetstiltak for å lukke avviket og for å unngå at denne typen hendelser skal inntreffe i fremtiden. Vi forutsetter at sikkerhetstiltakene slik de er skissert i NTNUs redegjørelse av 30. juni 2016, gjennomføres. På denne bakgrunn ser ikke vi grunn til å pålegge NTNU og OLT ytterligere sikkerhetstiltak.

Når det gjelder varsling, er det fremdeles uklart hvem som er berørt av avviket. Avviket består både av at det har funnet sted uautorisert innsyn i opptak fra kameraene og av at skjermbilder og videoklipp har blitt tilgjengeliggjort på Internett (utlevert). For det første er det uklart hvem som har vært tilstede i lokalene. For det andre er det uklart hvem som er avbildet på bildene og videoene som ble tilgjengeliggjort. For det tredje er det uklart hvor mange bilder og videoer som har blitt tilgjengeliggjort. Det er trolig ikke mulig å få full klarhet i disse spørsmålene.

NTNU har bedt Datatilsynet om en vurdering av hvordan varsling skal skje. NTNU skriver at man ikke ønsker å varsle offentlig om hva som har skjedd fordi det kan føre til at bildene og videoene blir spredd på nytt. Offentlig varsling kan derfor forverre personvernkonsekvensene.

I mellomtiden har saken blitt omtalt i media. Av den grunn er det ikke lenger noen grunn til å unngå offentlig varsling. Det er imidlertid ikke sikkert at et offentlig varsel når alle de berørte. Vår vurdering er at de personene som hadde planlagt aktiviteter i lokalene og de personene som hadde tilgang til lokalene, bør varsles direkte på egnet måte. Disse kan igjen oppfordres til å varsle andre de kjenner til som har brukt lokalene, for eksempel gjester de har hatt med seg.

NTNU har tatt vare på skjermbildene og videoklippene slik at de berørte kan få se dem. NTNU lurer på om bildene og videoene kan slettes etter dette. Slik sletting er i tråd med personopplysningsloven. Formålet med å ta vare på materialet er å gi de berørte en mulighet til innsyn. Etter at dette har skjedd er det ikke lenger nødvendig for formålet å ta vare på materialet, og da skal det slettes, jf. § 28. NTNU kan for eksempel ta vare på materialet 30 dager etter at varsel til de berørte har funnet sted.

5. Informasjonssikkerhet

Etter personopplysningsloven § 2-4 har virksomheter som behandler personopplysninger plikt til å utføre en risikovurdering av behandlinger før de iverksettes. Risikovurderingen skal identifisere sannsynligheten for og konsekvensene av sikkerhetsbrudd. Samtidig skal virksomheten fastlegge kriterier for akseptabel risiko forbundet med behandlingen. Risikovurderingen skal dokumenteres.

I dette tilfellet er det på det rene at risikovurdering ikke ble utført i tråd med § 2-4 før kamerasystemet ble satt i drift. Dette skyldes menneskelig svikt. NTNU har opplyst at virksomheten ellers har rutiner for risikovurdering.

Etter personopplysningsloven § 2-14 har virksomheter som behandler personopplysninger plikt til å iverksette sikkerhetstiltak. Tiltakene skal både hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å avdekke hendelser som kan forårsake sikkerhetsbrudd. Alle forsøk på uautorisert bruk av informasjonssystemet må registreres. Det er ikke tilstrekkelig med rutiner som den enkelte medarbeider forutsettes å følge – de behandlingsansvarlige må også iverksette tiltak som fungerer uavhengig av medarbeidernes handlinger, for eksempel i form av nettverks- eller applikasjonskontroll i sikkerhetsbarrierer. Sikkerhetstiltak skal dokumenteres.

I dette tilfellet hadde ikke NTNU og OLT tilstrekkelige sikkerhetstiltak for å hindre sikkerhetsbrudd. Dette førte til uautorisert bruk i form av uautorisert innsyn og utlevering.

6. Begrunnelse for overtredelsesgebyr

Datatilsynet mener det er nødvendig å reagere på overtredelsene, og varsler overtredelsesgebyr.

Etter personopplysningsloven § 46 kan Datatilsynet ilegge overtredelsesgebyr. Vi siterer fra bestemmelsen:

Datatilsynet kan pålegge den som har overtrådt denne loven eller forskrifter i medhold av den, å betale et pengebeløp til statskassen (overtredelsesgebyr) på inntil 10 ganger grunnbeløpet i folketrygden. Fysiske personer kan bare ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser. Et foretak kan ikke ilegges overtredelsesgebyr dersom overtredelsen skyldes forhold utenfor foretakets kontroll.

Ved vurderingen av om overtredelsesgebyr skal ilegges, og ved utmålingen, skal det særlig legges vekt på

a) hvor alvorlig overtredelsen har krenket de interesser loven verner,
b) graden av skyld,
c) om overtrederen ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne ha forebygget overtredelsen,
d) om overtredelsen er begått for å fremme overtrederens interesser,
e) om overtrederen har hatt eller kunne ha oppnådd fordel ved overtredelsen,
f) om det foreligger gjentakelse,
g) om andre reaksjoner som følge av overtredelsen blir ilagt overtrederen eller noen andre som har handlet på vegne av denne, blant annet om noen enkeltperson blir ilagt straff og
h) overtrederens økonomiske evne.

Bestemmelsen sier at ileggelse av overtredelsesgebyr skal bero på en skjønnsmessig helhetsvurdering, men legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal tillegges særlig vekt.

Adgangen til å ilegge overtredelsesgebyr er gitt som et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Overtredelsesgebyr ikke å anse som en straff, men en administrativ sanksjon. Det må imidlertid antas at overtredelsesgebyr er å anse som straff etter EMK (den europeiske menneskerettighetskonvensjonen) art 6, og i samsvar med Høyesteretts praksis, jf. Rt. 2012 side 1556, legger Datatilsynet til grunn at det kreves klar sannsynlighetsovervekt for lovovertredelse for å kunne ilegge gebyr. Saksforholdet og spørsmålet om å ilegge overtredelsesgebyr er vurdert med utgangspunkt i dette beviskravet.

Datatilsynet finner det klart at NTNU og OLT har behandlet personopplysninger uten å utføre risikovurdering, jf. personopplysningsforskriften § 2-4, jf. personopplysningsloven § 13, og ikke har iverksatt tilstrekkelige sikkerhetstiltak, jf. personopplysningsforskriften § 2-14, jf. personopplysningsloven § 13.

I vurderingen av om overtredelsesgebyr skal ilegges, legger Datatilsynet særlig vekt på at overtredelsene betydelig har krenket grunnleggende interesser som loven verner, jf. § 46 annet ledd bokstav a. Loven verner om grunnleggende personverninteresser som den personlige integritet og privatlivets fred, jf. lovens § 1.

Datatilsynet trekker her frem at det var snakk om et kamera som var rettet mot og hadde som formål å fange opp utøveres kropp. Dette er et stort inngrep i den personlige integriteten. Manglende sikring på et slikt kamera vil derfor ha et stort konsekvenspotensiale og risiko for personvernkrenkelser, noe som stiller høyere krav til informasjonssikkerheten. Kamerasystemet var i bruk over lang tid uten at sikkerhetstiltak eller risikovurdering ble iverksatt. Disse momentene taler med styrke for at overtredelsesgebyr bør ilegges.

Når det gjelder graden av skyld, jf. personopplysningsloven § 46 annet ledd bokstav b, forklarer lovens forarbeider[1] at det med graden av skyld siktes til hvor klanderverdig handlingen er, for eksempel om den bærer preg av et uhell eller om den har et mer systematisk eller planmessig preg. I dette tilfellet er det snakk om «menneskelig svikt» ved at gjeldende rutiner for risikovurdering ikke ble fulgt. Dette er i seg selv klart klanderverdig, men skyldgraden er ikke like stor som hvis det var snakk om systematisk svikt.

Vi legger også vekt på at overtredelsen kunne vært forebygget ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak, jf. § 46 annet ledd bokstav c. Virksomhetene kunne unngått overtredelsen med sikkerhetsrevisjoner eller en form for avsjekk for om rutinene var fulgt før systemet ble tatt i bruk. Siden det her var snakk om «menneskelig svikt», kan det heller ikke utelukkes at bedre opplæring og kontroll ville avverget overtredelsen.

Overtrederens økonomiske evne er det i liten grad lagt vekt på, jf. § 46 annet ledd bokstav h.

Datatilsynet kan ikke se at de øvrige momentene som loven fremhever, gjør seg gjeldende i nevneverdig grad.

[1] Ot.prp. nr. 71 (23007–2008)

Datatilsynet er etter dette kommet til at overtredelsesgebyr bør ilegges.

7. Vurdering av gebyrets størrelse

Når det gjelder gebyrets størrelse, skal de samme momenter som ved vurdering av om gebyr skal ilegges, tillegges særlig vekt. Gebyret bør settes så høyt at det får den nødvendige virkning også utover den konkrete saken. Samtidig må gebyrets størrelse stå i et rimelig forhold til overtredelsen.

Etter en totalvurdering av saken og graden av alvorlighet i overtredelsen, har vi kommet til at et overtredelsesgebyr på 100 000 kroner anses riktig.

8. Tilsvar

Dersom dere har merknader til dette varselet, ber vi om at de sendes Datatilsynet snarest og innen **mandag 26. september 2016.**

Vennlig hilsen

Bjørn Erik Thon
direktør

Tobias Judin
rådgiver