Datatilsynet

NORGES IDRETTSFORBUND OG OLYMPISKE OG PARALYMPISKE KOMITÉ
Postboks 5000

0840 OSLO

Unntatt offentlighet:
Offl. § 13 jf. Popplyl. § 24 (1) 2. pkt.

Deres referanse	Vår referanse	Dato
	20/01626-5	02.12.2020

Varsel om vedtak om overtredelsesgebyr - Melding om avvik - NORGES IDRETTSFORBUND OG OLYMPISKE OG PARALYMPISKE KOMITÉ

Vi viser til tidligere korrespondanse i saken, senest ved Norges Idrettsforbunds (heretter «NIF») oversendelse av rapport fra Orange Cyberdefense om avviket 30. juni 2020.

1. Varsel om overtredelsesgebyr

Dette er et forhåndsvarsel, jf. forvaltningsloven § 16, om at Datatilsynet vil fatte følgende vedtak:

1. *Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i pålegges Norges idrettsforbund og olympiske og paralympiske komité, org.nr. 947 975 072, å betale et overtredelsesgebyr til statskassen på 2 500 000 – to millioner fem hundre tusen – kroner for brudd på personvernforordningen artikkel 5 nr. 1 bokstav a, c og f, artikkel 6 og artikkel 32.*

2. Nærmere om sakens faktiske forhold

Nedenfor vil vi gjengi faktum i saken slik det samlet fremgår av avviksmeldingen, NIFs svar på krav om redegjørelse 28. februar 2020, Skype-møte med Datatilsynet 4. mai 2020, NIFs svar på krav om ny redegjørelse 25. mai 2020 og rapporten fra Orange Cyberdefense av 3. juni 2020.

<u>NIFs arbeid med overgang fra on-premise løsning til skyløsning</u>

Et IT-utvalg nedsatt av Idrettsstyret avla i 2016 en rapport som la føringer for at all utvikling og drift i størst mulig grad burde skje gjennom bruk av standardkomponenter og basert på

skytjenester. Det ble besluttet at NIF skulle bygge en ny digital plattform basert på Microsoft sine skytjenester.

Etter en anbudsrunde ble det inngått et samarbeid med Albatross IT Consultant AS, som hadde særlig kompetanse på Microsoft sine løsninger. Det ble etablert en plan for en gradvis overgang fra løsninger i NIFs eget datasenter til tjenester etablert ved bruk av Microsoft Azure. Det ble ikke gjennomført en vurdering av personvernkonsekvenser (DPIA) som beskrevet i personvernforordningen artikkel 35, da NIF ikke vurderte at en slik overgang til Azure i seg selv utløste plikt til å gjøre en DPIA.

Om avviket

Datatilsynet mottok 20. desember 2019 en avviksmelding fra NIF. I avviksmeldingen fremgikk det at NIF mottok en henvendelse fra Nasjonalt Cybersikkerhetssenter (NCSC-NO) den 18.12.19 angående et uttrekk fra idrettens medlemsdatabase som var tilgjengelig uten tilgangskontroll på en offentlig IP adresse. Gjennom å gå inn via en URL, var det mulig å søke på personer i databasen som inneholder 3,2 millioner oppføringer. Dette ble oppdaget som del av en rutinescan av irske IP adresser utført av irske National Cyber Security Centre (CSIRT-IE). CSIRT-IE varslet NCSC-NO om funnet, som igjen varslet NIF.

Avviket oppsto i forbindelse med overføringer av ressurser fra en on-premise løsning til Azure, og relaterte seg til uttesting av en tjeneste i Azure som heter Elasticsearch. Elasticsearch ble tatt i bruk i forbindelse med uttesting av en mulig løsning overfor tredjepartsleverandører av medlemssystemer til norsk idrett, for å muliggjøre verifikasjon av personer mot idrettens sentrale database. Elasticsearch inneholder et produkt som heter Kibana, som kjører på en port som ikke er åpen via NIF sitt nettverk og ut mot internett.

I forbindelse med etableringen av testløsningen, ble det vurdert at det var behov for å teste på reelle personopplysninger, og at en måtte ha et betydelig omfang for å få en reel test av løsningen. For at denne løsningen skulle virke, ble det vurdert som viktig å sikre integriteten til opplysninger, og få til en mest mulig realistisk kommunikasjonstest. Det ble også vurdert at det var tidskritisk å få testet løsningen. Basert på disse vurderingene, ble det konkludert med at den beste løsningen var å benytte reelle data, og NIF gjorde et uttrekk av en betydelig del av idrettens sentrale database.

NIF erkjenner at denne vurderingen ikke var riktig, og at det ble satt i gang en jobb med uttrekk av idrettens sentrale database til cache uten at det ble foretatt tilstrekkelige risikovurderinger eller vurderinger av om det var mulig å bruke avidentifiserte eller et mer begrenset utvalg av data i dette arbeidet. Det var på tidspunktet for hendelsen ikke etablert driftsrutiner eller tekniske sikkerhetsløsninger knyttet til det nye skybaserte miljøet, da det skybaserte miljøet på dette tidspunktet ikke var produksjonssatt.

Applikasjonen var ikke satt opp med noen autentiseringsmekanisme, og det ble gjort en feil som medførte at det ble etablert en offentlig IP-adresse. Elasticsearch og Kibana ble kort tid etter forkastet, og NIF gikk videre med en annen løsning. Det ble besluttet å utsette sletting av innholdet i testmiljøet til et senere tidspunkt. NIF hadde etablert [redacted]

[redacted] dette inkluderte ikke Elasticsearch og Kibana. NIF oppdaget dermed ikke at opplysningene lå åpent tilgjengelig.

NIF avdekket at tilgangen hadde vært åpen i 87 dager, og satte umiddelbart i gang tiltak for å stoppe tilgangen. De berørte er medlemmer, frivillige og andre personer med tilknytning til norsk idrett, totalt ca. 3,2 millioner personer. Av disse var 486 447 mindreårige, fordelt på alderen 3-17 år.

Tjenesten som ble brukt eksponerte i utgangspunktet ikke dataene for nedlasting, men ga mulighet for enkeltsøk. Kibana tilbyr også mulighet til «fuzzy search», noe som innebærer at massesøk er mulig. For å kunne gjennomføre massesøk, eksempelvis søke opp alle medlemmer på et poststed eller i en klubb, var det likevel behov for særlig kunnskap [redacted] Løsningen var heller ikke omfattet av åpne indekseringsløsninger, og en måtte således enten kjenne til IP-adressen eller gjøre mer målrettede søk for finne tjenesten.

Kategoriene av personopplysninger som var eksponert som følge av avviket var navn, fødselsdato, kjønn, adresse, e-post, telefonnummer og klubbtilhørighet. Personer med beskyttelsestiltakene strengt fortrolig adresse (kode 6) eller fortrolig adresse (kode 7), var ikke en del av uttrekket som var eksponert.

NIF har ingen indikasjoner på at andre enn de irske og norske sikkerhetsmyndigheter har foretatt søk. Elastic Search og Kibana hadde imidlertid ikke etablert aksesslogger ettersom dette var bare en trail-versjon, og på grunn av dette kan det ikke utelukkes at et datainnbrudd har funnet sted.

[redacted]

Basert på dette vurderer NIF det som lite sannsynlig at andre enn de irske og norske sikkerhetsmyndigheter har foretatt søk.

Etterforskningen til Orange Cyberdefense hadde som formål å avdekke om personopplysningene har blitt utnyttet kriminelt, og fant ingen indikasjoner på dette. Etterforskningen hadde imidlertid sine begrensninger, og kan blant annet bare finne personopplysninger for salg som averteres på markedet eller forum, men for eksempel ikke det som selges gjennom private meldinger mellom forummedlemmer. Etterforskningen skjedde også mellom 21. mai og 2. juni, og fanger ikke opp personopplysninger for salg som averteres på markedet eller forum før dette tidspunktet, og som ikke har etterlatt seg spor.

Rapporten fra Orange Cyberdefense presiserer at det finnes flere typer verktøy som overvåker databaselekkasjer, og som automatisk kan finne tilfeller av Elasticseach og Kibana som er eksponert på nettet. Dette betyr imidlertid ikke at alle tilfeller av eksponerte databaser blir

funnet og utnyttet. Videre kan en eksponert database bli funnet og utnyttet, uten at angriperen prøver å selge informasjonen.

Oppsummering og NIFs videre arbeid med skyløsninger

NIF erkjenner at dere på tidspunktet for hendelsen ikke hadde etablert gode nok sikkerhetsløsninger og rutiner knyttet til det nye skybaserte miljøet. Det var ikke etablert egne rutiner for testdata i det skybaserte miljøet på tidspunktet for hendelsen. Uttestingen av den tjenesten som eksponerte dataene var ikke planlagt brukt i det skybaserte miljøet, og var derfor heller ikke omfattet av de sikkerhetsvurderinger som var gjort på dette tidspunkt.

NIF har i tiden etter hendelsen jobbet mye med å revidere og forbedre eksisterende driftsrutiner, samt etablere nye rutiner der det er behov. NIF har innskjerpet krav til at det skal foretas risikovurderinger, og at disse skal dokumenteres i forkant av endringer.

Hendelsen har også avdekket behov for å forbedre NIFs rutiner for håndtering av testdata, der NIF i større grad enn tidligere skal benytte syntetiske testdata. NIF skriver at det har vært vanskelig å gjøre endringer i de gamle on-premise løsningene, særlig på grunn av at mye forretningslogikk har ligget i databasen. NIF har behov for å foreta grundige testinger på et stort volum av data på grunn av kompleksiteten på oppbygging av norsk idrett, og at dere har idrettslag i alle kommuner og tettsteder i Norge. NIF jobber nå med å etablere nye testmiljøer hvor all testing [redacted] syntetiske data, og med et mer begrenset antall opplysningskategorier.

3. Nærmere om personopplysningslovens krav

Grunnprinsippene for behandling av personopplysninger

De grunnleggende prinsippene for behandling av personopplysninger følger av personvernforordningen artikkel 5 nr. 1. Vi viser til artikkel 5 nr. 1 bokstav a, b, c og f:

> *«1. Personopplysninger skal (...)*
>
> *a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),*
>
> *b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenelig med disse formålene (...) («formålsbegrensning»),*
>
> *c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»), (...)*
>
> *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»)».

Den behandlingsansvarlige er ansvarlig og skal kunne påvise at prinsippene overholdes, jf. artikkel 5 nr. 2.

Rettslig grunnlag for behandling av personopplysninger

All behandling av personopplysninger må ha et rettslig grunnlag i artikkel 6 for å være lovlig. Vi visert her til de alternative rettslige grunnlagene i artikkel 6 nr. 1 bokstav b) og f), samt nr. 4 om viderebehandling:

«1. Behandlingen er bare lovlig dersom og i den grad minst ett av de følgende vilkår er oppfylt: (...)

b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i (...)

f) behandlinger er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn. (...)

4. Dersom behandlingen for et annet formål enn det som personopplysningene er blitt samlet inn for, ikke bygger på den registrertes samtykke eller på unionsretten eller medlemsstatenes nasjonale rett som utgjør et nødvendig og forholdsmessig tiltak i et demokratisk samfunn for å sikre oppnåelse av målene nevnt i artikkel 23 nr. 1, skal den behandlingsansvarlige for å avgjøre om behandlingen for et annet formål er forenlig med formålet som personopplysningene opprinnelig ble samlet inn for, blant annet ta hensyn til følgende:

a) enhver forbindelse mellom formålene som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen,

b) i hvilken sammenheng personopplysningene er blitt samlet inn, særlig med hensyn til forholdet mellom de registrerte og den behandlingsansvarlige,

c) personopplysningenes art, især om særlige kategorier av personopplysninger behandles, i henhold til artikkel 9, eller om personopplysninger om straffedommer og lovovertredelser behandles, i henhold til artikkel 10,

d) de mulige konsekvensene av den tiltenkte viderebehandlingen for de registrerte,

e) om det foreligger nødvendige garantier, som kan omfatte kryptering eller pseudonymisering»

Sikkerhet ved behandling

Kravene til personopplysningssikkerhet er nærmere regulert i artikkel 32. Her følger det:

> *«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, (...)*
>
> *a) pseudonymisering og kryptering av personopplysninger,*
>
> *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».*

4. Datatilsynets vurdering

4.1.Rettslig grunnlag for behandling og prinsippene om lovlighet og dataminimering – artikkel 6 og artikkel 5 nr. 1 bokstav a og c

Formålet med behandlingen av personopplysninger

Det følger av personvernerklæringen til NIF at dere behandler personopplysninger om medlemmer som er nødvendig for medlemskap og aktivitet i idretten, og at registrering av medlemsopplysninger er en forutsetning for medlemskap i norsk idrett. Datatilsynet legger dermed til grunn at nødvendig medlemsadministrasjon er formålet ved NIFs behandlingen av personopplysninger om medlemmer i norsk idrett, og at NIF har rettslig grunnlag i artikkel 6 nr. 1 bokstav b for denne behandlingen.

Det følger av personvernforordningen artikkel 5 nr. 1 bokstav b at personopplysninger bare skal behandles for spesifikke, uttrykkelig angitte og berettigede formål, og formålet må fastsettes før behandlingen av personopplysninger settes i gang.

Det er ikke spesifikt og uttrykkelig angitt i informasjonen fra NIF til de registrerte at personopplysninger vil brukes til test av nye mulige løsninger for medlemsadministrasjon for å undersøke om disse er hensiktsmessige å ta i bruk.

Datatilsynet vurderer først om behandling av personopplysningene for formålet om test av nye mulige skyløsninger for medlemsadministrasjon er dekket av det opprinnelige formålet som personopplysningene til NIFs medlemmer ble behandlet for – behandling for det angitte formålet om nødvendig medlemsadministrasjon for deltakelse i norsk idrett.

Bruken av personopplysningene til medlemmer av norsk idrett for testing av nye mulige løsninger for medlemsadministrasjon, er ikke isolert sett nødvendig for å fasilitere at det enkelte medlemmet kan delta i idretten. Testing av nye skyløsninger skiller seg dermed i natur fra formål om nødvendig medlemsadministrasjon for å muliggjøre deltakelse i norsk idrett. Dette gjelder selv om løsningene som skal testes også knytter seg til medlemsadministrasjon. I lys av kravet om at formål må være spesifikt og uttrykkelig angitt, vurderer Datatilsynet behandling av personopplysningene for formålet om test av nye mulige skyløsninger for medlemsadministrasjon ikke er dekket av det opprinnelige formålet om nødvendig medlemsadministrasjon for deltakelse i norsk idrett.

Behandling av personopplysningene til medlemmer av norsk idrett for formålet om test av nye mulige skyløsninger for medlemsadministrasjon er dermed et nytt formål.

Vurdering av om det forelå rettslig grunnlag for behandlingen av personopplysninger

For behandling av personopplysninger for et annet formål enn det som personopplysningene ble samlet inn for, er det to kumulative krav i personvernforordningen.

For det første kreves det, som ved all behandling av personopplysninger, at behandlingen har et rettslig grunnlag i artikkel 6 nr. 1 for å være lovlig.

I tillegg kreves det at det nye formålet med behandlingen av personopplysninger er forenelig med formålet personopplysningene ble samlet inn for, jf. artikkel 6 nr. 4. Det er et unntak fra dette vilkåret dersom den nye behandlingen bygger på den registrertes samtykke eller har hjemmel i lov, men det er klart at dette unntaket ikke kommer til anvendelse i denne saken.

Datatilsynet vurderer først om NIF hadde rettslig grunnlag etter artikkel 6 nr. 1 for å behandle en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett for formålet om uttesting av nye mulige skyløsninger for medlemsadministrasjon.

Datatilsynet har spurt NIF om hvilket rettslig grunnlag etter artikkel 6 dere hadde for å behandle medlemmenes personopplysninger i forbindelse med uttesting av den nye skyløsningen i begge våre krav om redegjørelser av henholdsvis 10. februar 2020 og 24. mars 2020. NIF har ikke vist til noe rettslig grunnlag for denne behandlingen av personopplysninger i noen av deres svar, og Datatilsynet legger dermed til grunn at det aldri ble vurdert om det forelå rettslig grunnlag for de aktuelle behandlingene av

personopplysninger. Datatilsynet vil likevel foreta en selvstendig vurdering av behandlingsgrunnlag.

Datatilsynet vurderer først om NIF har rettslig grunnlag etter artikkel 6 nr. 1 bokstav b for den aktuelle behandlingen av personopplysninger, ettersom dette er det rettslige grunnlaget som tilsynelatende forutsettes i personvernerklæringen til NIF. Datatilsynet påpeker for ordens skyld at personvernforordningen artikkel 13 nr. 1 bokstav c krever at det informeres om det rettslige grunnlaget for behandlingen.

Det følger av artikkel 6 nr. 1 bokstav b at behandlingen må være «nødvendig» for å oppfylle en avtale som den registrerte er part i. Det må dermed vurderes om det var nødvendig for å oppfylle avtalen mellom medlemmene og NIF å behandle en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett for uttesting av nye mulige skyløsninger for medlemsadministrasjon.

Behandlingsansvarlig må gjøre konkrete vurderinger av hvilke personopplysninger det er nødvendig å behandle knyttet til hvert enkelt formål. Med støtte fra EU-domstolens avgjørelser har Personvernrådet (EDPB) i sine retningslinjer for artikkel 6 nr. 1 bokstav b knyttet til nettjenester, pekt på at det i vurderingen av nødvendighet må vurderes hvorvidt formålet kan oppnås på mindre personverninngripende måter.[1] Dette samsvarer med det som følger av fortalepunkt 39 i personvernforordningen. Hvis det foreligger realistiske, mindre personverninngripende alternativer, er ikke behandlingen «nødvendig».

Videre uttaler Personvernrådet at den behandlingsansvarlige bare kan benytte «nødvendig for å oppfylle en avtale som den registrerte er part i» dersom den aktuelle behandlingen av personopplysninger er objektivt og genuint nødvendig for oppfyllelsen av den konkrete avtalen. Artikkel 6 nr. 1 bokstav b dekker dermed ikke behandling som er nyttig for den behandlingsansvarlige, men som ikke er objektivt nødvendig for å oppfylle avtalen.[2] I slike tilfeller må den behandlingsansvarlige vurdere andre behandlingsgrunnlag. Datatilsynet legger til grunn at disse tolkningene også gjør seg gjeldende for nødvendighetsvurderingen etter artikkel 6 nr. 1 bokstav b på generelt grunnlag – og ikke bare for nettjenester.

I forbindelse med uttestingen av skyløsningen besluttet NIF å bruke en rekke kategorier av personopplysninger om 3,2 millioner personer fra deres sentrale database. NIF erkjenner at det ikke ble gjort tilstrekkelige vurderinger av om det var mulig å bruke avidentifiserte eller et mer begrenset utvalg av data i dette arbeidet, og at denne beslutningen som ble gjort ikke var riktig. NIF har siden jobbet med å forbedre deres rutiner for håndtering av testdata, og jobber nå med å etablere nye testmiljøer [redacted] syntetiske data, og med et mer begrenset antall opplysningskategorier.

Behandlingen av personopplysningene til medlemmer av norsk idrett for testing av nye mulige skyløsninger for medlemsadministrasjon, er ikke isolert sett nødvendig for å fasilitere at det enkelte medlemmet kan delta i idretten. Dermed er heller ikke den aktuelle

[1] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, avsnitt 25
[2] Guidelines 2/2019 avsnitt 25-28

behandlingen av personopplysninger objektivt og genuint nødvendig for å oppfylle medlemsavtalen med medlemmene av norsk idrett. For ordens skyld finner Datatilsynet det uansett er klart at formålet om test av nye mulige løsninger for medlemsadministrasjon kunne oppnås på mindre personverninngripende måter, herunder ved å behandle syntetiske data – eller i det minste gjennom behandling av langt færre personopplysninger.

Datatilsynet vurderer dermed at det ikke var nødvendig for å oppfylle avtalen mellom medlemmene og NIF å behandle en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett for uttesting av nye skyløsninger for medlemsadministrasjon. Ettersom nødvendighetsvilkåret ikke er oppfylt, hadde ikke NIF rettslig grunnlag etter artikkel 6 nr. 1 bokstav b for denne aktuelle behandlingen av personopplysninger.

NIF har ikke selv anført at artikkel 6 nr. 1 bokstav f var et aktuelt rettslig grunnlag i saken, og det er heller ikke gitt informasjon om dette rettslige grunnlaget til de registrerte etter artikkel 13 nr. 1 bokstav c, eller hvilke berettigede interesser som eventuelt forfølges etter artikkel 13 nr. 1 bokstav d. Datatilsynet foretar likevel en selvstendig vurdering av rettslig grunnlag etter dette alternativet.

Datatilsynet vurderer dermed om behandlingen av en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett for uttesting av nye mulige skyløsninger for medlemsadministrasjon var nødvendig for et formål knyttet til NIFs berettigede interesse, og om denne interessen gikk foran de registrertes interesser og grunnleggende rettigheter og friheter, jf. personvernforordningen artikkel 6 nr. 1 bokstav f.

Datatilsynet legger til grunn at formålet om uttesting av nye skyløsninger for medlemsadministrasjon for å vurdere om disse er hensiktsmessige å ta i bruk, er et formål knyttet til NIFs berettigede interesse.

Det må deretter vurderes om behandlingen av en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett var «nødvendig» for formålet om uttesting av nye mulige skyløsninger for medlemsadministrasjon.

Som vi har redegjort for knyttet til nødvendighetsvilkåret etter 6 nr. 1 bokstav b, vil det også for nødvendighetsvilkåret i artikkel 6 nr. 1 bokstav f måtte vurderes hvorvidt formålet kan oppnås på mindre personverninngripende måter. Hvis det foreligger realistiske, mindre personverninngripende alternativer, er ikke behandlingen nødvendig.

Som nevnt ovenfor i vurderingen av nødvendighetsvilkåret etter 6 nr. 1 bokstav b, finner Datatilsynet det klart at formålet om testing av nye mulige løsninger for medlemsadministrasjon kunne oppnås på mindre personverninngripende måter enn å behandle en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett. Formålet kunne oppnås ved å behandle syntetiske data – eller i det minste gjennom behandling av langt færre personopplysninger.

Datatilsynet finner det ikke nødvendig for saken å gå konkret inn på vurderingen av om det eventuelt var nødvendig for formålet å behandle en langt mindre andel av de aktuelle

personopplysningene for formålet om uttesting av nye mulige skyløsninger for medlemsadministrasjon.

Ettersom nødvendighetsvilkåret ikke er oppfylt, hadde NIF heller ikke rettslig grunnlag i artikkel 6 nr. 1 bokstav f for behandlingen av en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett for uttesting av nye mulige skyløsninger for medlemsadministrasjon.

Dermed hadde den aktuelle behandlingen av personopplysninger ikke rettslig grunnlag i artikkel 6 nr. 1, og behandlingen var ulovlig.

Ettersom kravet om rettslig grunnlag ikke er oppfylt, finner ikke Datatilsynet det nødvendig å gå inn på vurderingen hvorvidt dette nye formålet var forenelig med formålet personopplysningene til medlemmene av norsk idrett ble samlet inn for, jf. personvernforordningen artikkel 6 nr. 4.

Vurdering av prinsippet om lovlighet

Prinsippet om at en behandling må være lovlig etter artikkel 5 nr. 1 bokstav a, innebærer at den må ha et rettslig grunnlag i personvernforordningen. En behandling av personopplysninger uten rettslig grunnlag vil uten videre være ulovlig, og dermed være i strid med det grunnleggende kravet i prinsippet i artikkel 5 nr. 1 bokstav a. Som vist over finner vi at det ikke forelå et rettslig grunnlag for behandlingen av en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett for uttesting av nye mulige skyløsninger for medlemsadministrasjon, og behandlingen er dermed i strid med prinsippet om lovlighet, artikkel 5 nr. 1 bokstav a.

Vurdering av prinsippet om dataminimering

Prinsippet om dataminimering i artikkel 5 nr. 1 bokstav c innebærer at personopplysninger skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for. Etter prinsippet om dataminimering er det ikke tilstrekkelig at det er praktisk eller ønskelig å behandle personopplysninger; behandlingen må være nødvendig for at formålet kan nås. Behandlingsansvarlig må gjøre konkrete vurderinger av hvilke personopplysninger det er nødvendig å behandle knyttet til hvert enkelt formål.

Som det følger av vurderingen av rettslig grunnlag og nødvendighetsvilkåret etter artikkel 6 nr. 1 ovenfor, finner Datatilsynet at behandlingen av en rekke kategorier av personopplysninger om 3,2 millioner personer fra idrettens sentrale database, ikke begrenset seg til det som er nødvendig for formålet om uttesting av nye mulige skyløsninger for medlemsadministrasjon. Formålet med den aktuelle behandlingen av personopplysninger kunne oppnås ved bruk syntetiske data, eller i det minste ved behandling av langt færre personopplysninger. Behandlingen var dermed også i strid prinsippet om dataminimering i artikkel 5 nr. 1 bokstav c.

4.2. Sikkerhet ved behandling personopplysninger – artikkel 5 nr. 1 bokstav f og artikkel 32

Som det følger av punkt 3, krever personvernforordningen artikkel 5 bokstav f at personlige opplysninger 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. Artikkel 32 krever at den behandlingsansvarlige gjennomfører egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Som det følger av ordlyden i begge bestemmelsene, er det ikke slik at ethvert brudd på personopplysningssikkerheten utgjør et brudd på personvernforordningen artikkel 5 nr. 1 bokstav f eller artikkel 32. Spørsmålet er om den behandlingsansvarlige har overholdt plikten til å iverksette *egnede* tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er *egnet* med hensyn til risikoene forbundet med behandlingen.

Hvilke tiltak og sikkerhetsnivå som er egnet må ha bakgrunn i den vurderingen som er foretatt av risikoene forbundet med behandlingen, i tillegg til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, jf. artikkel 32 nr. 1 og nr. 2.

Datatilsynet vurderer dermed om NIF gjennomførte egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som var egnet med hensyn til risikoen knyttet til å behandle en rekke kategorier av personopplysninger til 3,2 millioner medlemmer av norsk idrett for uttesting av nye skyløsninger for medlemsadministrasjon, jf. artikkel 32 nr. 1.

I denne saken er det i stor grad tale om behandling av kontaktopplysninger, i tillegg til opplysninger om fødselsdato og klubbtilhørighet. I utgangspunktet er ikke dette de kategoriene av personopplysninger det er størst risikoer knyttet til. Omfanget av behandling er imidlertid enormt stort, ettersom det er tale om personopplysningene til cirka 3,2 millioner personer – omtrent 60 % av Norges befolkning.[3]

Barns personopplysninger har også et særlig vern etter personvernforordningen, jf. personvernforordningens fortalepunkt 38. Ved uttestingen av skyløsningen ble det behandlet personopplysninger om 486 447 mindreårige, fordelt på alderen 3-17 år.

Antall registrerte og omfanget av personopplysninger som ble behandlet, i tillegg til omfanget av personopplysninger om mindreårige registrerte, taler for at personopplysningene hadde et stort beskyttelsesbehov, og at risikoene knyttet til eventuell ikke-autorisert utlevering av eller tilgang til personopplysningene var betydelige.

Det erkjennes i redegjørelsene til NIF at det ikke ble foretatt tilstrekkelige eller konkrete risikovurderinger i forkant av at NIF gjorde uttrekk av personopplysninger til 3,2 millioner personer fra idrettens sentrale database til det skybaserte testmiljøet. Den aktuelle uttestingen var ikke omfattet av de risikovurderinger som var gjort i forbindelse med arbeid med skyløsninger på dette tidspunktet. I en dokument som NIF har oversendt fra 2018, er det på

[3] https://www.ssb.no/befolkning/statistikker/folkemengde/aar-per-1-januar

overordnet nivå beskrevet en rekke risikoer hvor risikonivået betegnes som «høyt» ved overgangen til skyløsningen, men verken risikovurderingene eller tiltakene som skisseres i dette dokumentet var fulgt opp på tidspunktet for hendelsen.

Ettersom NIF ikke hadde tilstrekkelig eller konkret risikovurdert de aktuelle behandlingene, hadde dere heller ikke forutsetningen for å avdekke hvilke konkrete risikoer behandlingen innebar. Dermed hadde dere heller ikke forutsetningen for å vurdere hvilket sikkerhetsnivå som var egnet med hensyn til risikoen, eller hvilke tekniske og organisatoriske tiltak som var egnet for å oppnå dette sikkerhetsnivået.

Artikkel 32 nr. 1 trekker frem eksempler på kategorier av tiltak som potensielt er egnet avhengig av behandlingen, og Datatilsynet vurderer at tre av disse kategoriene av tiltak kunne vært egnet i den foreliggende saken:

> *a) pseudonymisering og kryptering av personopplysninger,*
>
> *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.*

Når det gjelder mer konkrete retningslinjer på tekniske og organisatoriske tiltak som kan gjennomføres for slike prosesser, viser Datatilsynet til Nasjonal Sikkerhetsmyndighets (NSM) «Grunnprinsipper for IKT-sikkerhet 2.0»[4], og spesielt punkt 2.1 «Ivareta sikkerhet i anskaffelses- og utviklingsprosesser»[5] og punktet om «Bruk av tjenesteutsetting og skytjenester» i introduksjonen[6]. NSMs grunnprinsipper er forankret mot det globale rammeverket ISO 27002 (Informasjonssikkerhet).[7]

På tidspunktet for hendelsen hadde imidlertid ikke NIF etablert driftsrutiner eller tekniske sikkerhetsløsninger knyttet til det nye skybaserte miljøet, da det på dette tidspunktet ikke var produksjonssatt. Det var heller ikke var etablert egne rutiner for testdata i det skybaserte miljøet. NIF har en generell norm for behandling av personopplysninger og informasjonssikkerhet i idretten, men punktene i denne om risikovurdering og tiltak for å sikre konfidensialitet og integritet ble ikke fulgt opp for den aktuelle behandlingen av personopplysninger. Punktene om tiltak i det overordnede dokumentet NIF har oversendt fra 2018 var heller ikke fulgt opp.

---

[4] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-opprettholde/ivareta-sikkerhet-i-anskaffelses-og-utviklingsprosesser/

[5] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/beskytte-og-opprettholde/ivareta-sikkerhet-i-anskaffelses-og-utviklingsprosesser/

[6] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/bruk-av-tjenesteutsetting-og-skytjenester/

[7] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/stotteprodukter/

I lys av dette vurderer Datatilsynet at det har vært grunnleggende mangler ved oppfølgingen av det interne styringssystemet og informasjonssikkerheten ved den aktuelle behandlingen av personopplysninger knyttet til uttesting av skyløsninger for medlemsadministrasjon. NIF gjennomførte ikke egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen forbundet med den aktuelle behandlingen av personopplysninger, og det foreligger brudd på pliktene i personvernforordningen artikkel 32.

Som vurderingen av artikkel 32 ovenfor viser, har NIF heller ikke behandlet personopplysninger på en måte som sikret tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling ved bruk av egnede tekniske eller organisatoriske tiltak. Behandlingen var dermed også i strid prinsippet om konfidensialitet jf. artikkel 5 nr. 1 bokstav f.

5. Overtredelsesgebyr

5.1. Vurdering av om overtredelsesgebyr skal ilegges

Overtredelsesgebyr er et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsregelverket. Vi mener det er nødvendig å reagere på overtredelsene, og varsler med dette ileggelse av overtredelsesgebyr (jf. personvernforordningen artikkel 83).

I samsvar med Høyesteretts praksis (jf. Rt. 2012 side 1556) legger vi til grunn at overtredelsesgebyr er å anse som straff etter den europeiske menneskerettighetskonvensjonen art 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr.

Ved vurderingen av om det skal ilegges gebyr og ved utmålingen skal Datatilsynet ta hensyn til momentene i personvernforordningen artikkel 83 nr. 2 bokstav a) til k). Datatilsynet kan ilegge overtredelsesgebyr etter en skjønnsmessig helhetsvurdering, men de opplistede momentene legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal tillegges særlig vekt.

Vi vil her vurdere de relevante momentene fortløpende.

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

Overtredelsen innebærer brudd på flere av de grunnleggende prinsippene om behandling av personopplysninger, det grunnleggende kravet om at all behandling av personopplysninger må ha et rettslig grunnlag for å være lovlig, i tillegg til klare brudd på kravene til sikkerhet ved behandlingen. Den aktuelle overtredelsen innebærer behandling av en rekke kategorier av personopplysninger om 3,2 millioner personer uten rettslig grunnlag, langt utover den behandling som var nødvendig for formålet, uten tilstrekkelige risikovurderinger og på en måte som ikke ivaretok sikkerheten ved behandlingen. Dette må karakteriseres som et klart avvik fra de pliktene som følger av personvernforordningen, og disse forholdene vurderer Datatilsynet som svært skjerpende omstendigheter.

Av de 3,2 millioner personene som ble eksponert, var 486 447 mindreårige fordelt på alderen 3-17 år. Barn er en sårbar gruppe, og vi viser her til personvernforordningens fortalepunkt 38 hvor det pekes på at barns personopplysninger har et særlig krav på vern. At overtredelsen omfatter personopplysninger om mindreårige i en så stor skala, vurderer også Datatilsynet som en svært skjerpende omstendighet.

Personopplysningene var eksponert i 87 dager, noe Datatilsynet vurderer som en betydelig periode. Det faktum at NIF heller ikke hadde iverksatt tiltak som gjorde at dere kunne oppdage at databasen var eksponert, og at det er uklart hvorvidt eller når dere eventuelt ville oppdaget dette selv, er også et skjerpende moment.

Selv om det ikke kan utelukkes at personopplysningene har kommet på avveie, vurderer Datatilsynet at det ikke er klar sannsynlighetsovervekt for dette. Det er dermed ikke klar sannsynlighetsovervekt for materiell eller ikke-materiell skade lidt, utover de registrertes følelse av å miste kontroll over personopplysningene sine. At det ikke kan påvises noen slik konkret skade lidt er en formildende omstendighet i saken. Datatilsynet påpeker imidlertid at dette eventuelt skyldes tilfeldigheter. Ettersom det ikke kan utelukkes at personopplysningene har kommet på avveie, er et eventuelt skadeomfang likevel ukjent.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Den aktuelle behandlingen av personopplysninger ble gjennomført uten at det var gjennomført vurdering av rettslig grunnlag for behandlingen, tilstrekkelige risikovurderinger eller iverksatt konkrete egnede tekniske eller organisatoriske tiltak. Dette må karakteriseres som klart uaktsomt.

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

NIF sørget for at tilgangen til personopplysningene ble lukket da dere ble gjort kjent med den. NIF brukte deretter Orange Cyberdefense til å gjennomføre en etterforskning av om personopplysningene har blitt utnyttet kriminelt, noe Datatilsynet vurderer som en formildende omstendighet i saken.

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

NIF har en generell norm for behandling av personopplysninger og informasjonssikkerhet i idretten, men punktene i denne om risikovurdering og tiltak for å sikre konfidensialitet og integritet ble ikke fulgt opp i denne saken. Det faktum at den aktuelle behandlingen av personopplysninger ble gjennomført uten at det ble gjort en vurdering av rettslig grunnlag for behandlingen, tilstrekkelige risikovurderinger eller iverksatt noen konkrete egnede tekniske eller organisatoriske tiltak, gir uttrykk for mangler ved det interne styringssystemet.

e) eventuelle tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren

Datatilsynet har ikke vektlagt noen tidligere overtredelser i denne saken.

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

NIF har svart på spørsmålene fra Datatilsynet slik de er påkrevd. Dette trekker derfor hverken i skjerpende eller formildende retning.

g) kategoriene av personopplysninger som er berørt av overtredelsen

De berørte personopplysningene i denne saken er i stor grad kontaktopplysninger, i tillegg til opplysninger om fødselsdato og klubbtilhørighet, som det som utgangspunkt ikke er de største risikoene knyttet til. Dette trekker i utgangspunktet i formildende regning, men som nevnt ovenfor har Datatilsynet også lagt vekt at mindreåriges personopplysninger er berørt av overtredelsen, noe som er et skjerpende moment.

Datatilsynet vurderer at det kan utledes helseopplysninger gjennom klubbtilhørighet i klubber som heter «handicapidrettslag» eller lignende, og dermed særlige kategorier av personopplysninger omfattet av artikkel 9 nr. 1. Ettersom det ikke fremgår hvilken rolle i klubben personen har, og det også er funksjonsfriske som er medlemmer eller støtteapparat i handicapidrettslag, vil det imidlertid ikke kunne trekkes klare konklusjoner om funksjonsevne i mange tilfeller. Datatilsynet har derfor lagt begrenset vekt på dette momentet.

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

NIF meldte selv fra om avviket til Datatilsynet.

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

Det er ikke tidligere truffet tiltak overfor NIF med hensyn til samme saksgjenstand.

j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42

Datatilsynet finner ikke dette momentet relevant i saken.

k) og 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

Det er viktig for samfunnet at alle har mulighet til å utøve idrett ut fra sine ønsker og behov, og deltakelse i idrett kan blant annet bidra til glede, sosialisering, bedre fysisk og psykisk helse, integrering og samhørighet og samhold med andre mennesker – både for barn og voksne. Som det følger av personvernerklæringen til NIF, er registrering av medlemsopplysninger en forutsetning for medlemskap i norsk idrett. Som portvokter for et viktig samfunnsgode, har NIF et særlig ansvar for å forvalte disse medlemsopplysningene på en lovlig og forsvarlig måte – noe som ikke er gjort i denne saken. Datatilsynet vurderer dette som en skjerpende omstendighet.

Datatilsynet legger til grunn at NIF ikke har oppnådd noen økonomiske fordeler som følge av overtredelsen, utover eventuelle besparelser ved å ikke gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Det kan også sees hen til virksomhetens økonomiske situasjon. NIF mottar storparten av sine inntekter gjennom tilskudd fra det offentlige og andre instanser. Ifølge deres regnskap fra 2019 hadde NIF driftsinntekter på 1 948 935 000 kroner og et driftsresultat på 7 607 000 kroner. Datatilsynet finner at NIF har økonomi til å bære et overtredelsesgebyr.

Datatilsynet har ikke kjennskap til andre skjerpende eller formildende faktorer ved saken som vil påvirke utfallet av vurderingen.

Basert på vurderingene ovenfor kommer Datatilsynet til at overtredelsesgebyr bør ilegges.

5.2. Vurdering av gebyrets størrelse

Overtredelsesgebyret skal i henhold til artikkel 83 nr. 1 være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Dette innebærer at tilsynsmyndigheten skal gjøre en konkret, skjønnsmessig vurdering i hvert enkelt tilfelle.

Ved utmåling av gebyrets størrelse skal det legges vekt på de samme vurderingsmomentene som er gjennomgått i vedtakets punkt 5.1. Datatilsynet viser derfor til vurderingene gjort ovenfor, og at disse samlet taler for et gebyr av en viss størrelse.

I skjerpende retning legger vi særlig vekt på NIFs klare avvik fra de sentrale pliktene som personvernforordningens artikkel 5 nr. 1 bokstav a, c og f, artikkel 6 og artikkel 32 oppstiller. Vi vektlegger også særlig omfanget av personopplysninger som er berørt av overtredelsen, og spesielt omfanget av personopplysninger om mindreårige registrerte.

I formidlende retning legger vi vekt på at bruddet i stor grad omhandler kategorier av personopplysninger det ikke er tilknyttet de største risikoene til, samt at det ikke er kjent eller klar sannsynlighetsovervekt for at bruddet har ført til materiell eller ikke-materiell skade for de registrerte som er berørt.

Også virksomhetens økonomiske evne vil være av betydning, selv om det ikke er aktuelt å utnytte det spennet i overtredelsesgebyrets størrelse som følger av artikkel 83. nr. 5. Personvernforordningen artikkel 83 nr. 5. fastsetter et høyere maksbeløp for gebyr når saken

omhandler overtredelser av de grunnleggende prinsippene for behandling av personopplysninger i henhold til personvernforordningen artikkel 5 og 6.

NIF mottar som nevnt storparten av sine inntekter gjennom tilskudd fra det offentlige og andre instanser. Ifølge deres regnskap fra 2019 hadde NIF driftsinntekter på 1 948 935 000 kroner og et driftsresultat på 7 607 000 kroner. NIFs betydelige økonomiske tall taler for at vedtaket må være av en viss størrelse for at de preventive hensynene bak overtredelsesgebyr som reaksjonsform skal ivaretas.

Etter en helhetsvurdering av momentene i saken som vi har gjennomgått ovenfor og alvorligheten i overtredelsen, har vi kommet frem til at et overtredelsesgebyr på kr 2 500 000 anses riktig.

Dersom NIF, på grunn av den samfunnsmessige situasjonen med covid-19, opplever forhold som er relevant for det varslede vedtaket om overtredelsesgebyr, ber vi om at dere gir oss en tilbakemelding med relevant dokumentasjon.

Orientering om videre fremdrift
Dette er et forhåndsvarsel (jf. forvaltningsloven § 16). Dersom dere har merknader til dette varselet, må dere sende oss en tilbakemelding om dette så snart som mulig og senest innen **4. januar 2021.**

Innsyn og offentlighet
Dere har rett til innsyn i sakens dokumenter (jf. forvaltningsloven § 18). Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige (jf. offentlighetsloven § 3.)

Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentet fra offentlig innsyn ber vi dere om å begrunne dette.

Hvis dere har spørsmål, kan dere ta kontakt med Anders Obrestad på telefon 22 39 69 71.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Anders Sæve Obrestad
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer