Veileder

Den nye personvernforordningen (GDPR)

Oversikt over reglene om informasjonssikkerhet

UNINETT

Innhold

Innledning 4
Regelverkets formål 4
Betydning 4
Informasjonssikkerhet 5
Målgrupper 5
Gyldighet 5
Oppbygning 5
Del 1: Viktige begreper 7
Behandling av personopplysninger 7
Personopplysninger 7
Sensitive personopplysninger 8
Behandlingsansvarlig 8
Databehandler 9
De registrerte 9
Del 2: De sentrale kravene til informasjonssikkerhet 10
Informasjonssikkerhet som grunnprinsipp 10
Hovedreglene om informasjonssikkerhet 11
Varsling av sikkerhetshendelser 13
Del 3: Krav med betydning for informasjonssikkerheten 18
Internkontroll 18
Protokoll over behandlingsaktiviteter 19
Innebygd personvern og personvern som standardinnstilling 20
Vurdering av personvernkonsekvenser og forhåndsdrøftelser 20
Personvernrådgiver (ombud) 22
Databehandlere og databehandleravtaler 23
Atferdsnormer og sertifisering 24
Del 4: Datatilsynet, sanksjoner og erstatning 25
Datatilsynet 25
Overtredelsesgebyr 25

Tvangsmulkt 25
Erstatning 25
Straff 26
Klage på vedtak 26

Innledning

EUs nye personvernforordning (GDPR)[1] ble vedtatt i april 2016. Forordningen blir norsk lov, trolig fra 25. mai 2018. Dette skjer ved at forordningen inkorporeres i norsk lovgivning, det vil si at det vedtas en ny personopplysningslov[2] som gjør forordningens regler til norsk lov. Forordningen og den nye personopplysningsloven erstatter dagens personopplysningslov med forskrift.

Forslaget til ny personopplysningslov inneholder enkelte særnorske regler på områder hvor EUs personvernforordning tillater at landene lager slike regler. Et eksempel på dette er at sensitive personopplysninger tillates brukt for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål dersom behandlingen (prosjektet) er tilrådd av institusjonens personvernrådgiver (ombud).[3]

Regelverkets formål

Hovedformålet med forordningen og den nye personopplysningsloven, er å ivareta personvernet til den enkelte ved elektronisk behandling av personopplysninger.[4] Når det gjelder forordningen, er det også et viktig formål å oppnå større grad av likhet i hvordan regler om behandling av personopplysninger skal forstås og praktiseres på tvers av EU/EØS-land.

Betydning

I universitets- og høgskolesektoren vil forordningen ha betydning for hvordan institusjoner behandler og sikrer personopplysninger i forskning, undervisning, administrasjon og formidling. Det er derfor viktig at universiteter og høgskoler begynner å forberede seg på overgangen til det nye regelverket allerede nå.

---

[1] En uoffisiell norsk oversettelse av EUs personvernforordning, er tilgjengelig på https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/.

[2] Forslag til ny personopplysningslov er tilgjengelig på https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/.

[3] Forslag til personopplysningslov § 6 første ledd bokstav d.

[4] Reglene i forordningen gjelder også for behandling av personopplysninger som inngår eller er ment å inngå i manuelle (papirbaserte) personregistre.

UNINETT

Informasjonssikkerhet

I denne veilederen gis en kort innføring i hvilke krav som forordningen stiller til informasjonssikkerheten ved behandling av personopplysninger i forskning, undervisning, administrasjon og formidling. Med informasjonssikkerhet menes evnen til å forebygge, avdekke og håndtere hendelser som kan føre til brudd på personopplysningenes konfidensialitet,[5] integritet[6] eller tilgjengelighet.[7]

Forordningen inneholder en rekke regler og krav som ikke berører informasjonssikkerhet. Enkelte av disse nevnes nedenfor, men drøftes ikke nærmere. For utfyllende informasjon anbefales Datatilsynets temasider om personvernforordningen, se www.datatilsynet.no.

Forslaget til ny personopplysningslov inneholder få særnorske regler som berører informasjonssikkerhet. Men lovforslagets § 15 pålegger personvernrådgivere (ombud) taushetsplikt for enkelte opplysninger som de får tilgang eller kjennskap til i forbindelse med utførelsen av sine oppgaver. Det er i tillegg laget utkast til egne regler om hvordan arbeidsgivers innsyn i ansattes e-post, personlige lagringsområder, elektroniske utstyr og aktivitetslogger skal foregå. I utkastet foreslås det at innsynsreglene ikke skal gjelde ved kontroll av aktivitetslogger for å oppklare sikkerhetsbrudd i datanettverk.

Målgrupper

Denne veilederen retter seg spesielt mot vitenskapelig og administrativt ansatte som har ansvar for sikkerheten til personopplysninger som behandles i institusjonenes IT-løsninger (systemer, tjenester, digitalt utstyr og elektronisk infrastruktur).

Gyldighet

Denne veilederen baserer seg på foreløpig informasjon (pr. 10.08.2017) om hvordan det nye regelverket skal forståes og praktiseres. Veilederen vil bli oppdatert ved behov.

Oppbygning

I første del av veilederen gjøres det rede for sentrale begreper i forordningen. I andre del gjennomgås de viktigste reglene om informasjonssikkerhet. Tredje del omhandler regler som har

[5] Hindre uvedkommende i å få tilgang til personopplysninger.

[6] Hindre uautorisert endring og sletting av personopplysninger, eller at opplysningene skades eller ødelegges.

[7] Sørge for at autoriserte personer får tilgang til personopplysninger når de har behov for det.

betydning for arbeidet med informasjonssikkerhet. I del fire følger en oversikt over Datatilsynets oppgaver og myndighet, sanksjoner ved brudd på regelverket og klageordninger.

Del 1: Viktige begreper

I denne delen av veilederen gjøres det kort rede for grunnleggende begreper i personvernforordningen. Kjennskap til disse begrepene gjør det enklere å forstå forordningens regler om informasjonssikkerhet.

Behandling av personopplysninger

I forordningen defineres behandling av personopplysninger som alle former for bruk av personopplysninger, for eksempel registrering, lagring, sammenstilling, overføring, publisering eller sletting.

Personopplysninger

I forordningen defineres personopplysninger som alle opplysninger eller vurderinger som kan knyttes til en bestemt person (ansatt, student, gjesteforsker, gjest eller respondent/informant i forskningsprosjekter). Slike vurderinger eller opplysninger regnes som personopplysninger uavhengig av om de foreligger som tekst, bilder, lyd- eller videoopptak.

Eksempler på personopplysninger kan være:

- navn, adresse, alder, telefonnummer, e-postadresse, bankkontonummer og fødselsnummer,
- innholdet i eksamensbesvarelser, bachlor- eller masteroppgaver og kandidatenes karakterer
- innhold i saksdokumenter, utredninger eller vurderinger som omhandler ansatte eller studenter
- video- og lydopptak som gjøres ved bruk av overvåkningskamera og hvor enkeltpersoner kan gjenkjennes
- logging av aktivitet i datasystemer hvor loggene kan knyttes til bestemte ansatte eller studenter

Behandling av personopplysninger skal etter dagens regelverk i mange tilfeller meldes til Datatilsynet før behandlingen tar til. Når forordningen trer i kraft, faller meldepliktordningen bort.

Sensitive personopplysninger

I forordningen defineres sensitive personopplysninger som alle typer opplysninger eller vurderinger som kan knyttes til en bestemt person og som omhandler:

- opplysninger om helse og helserelaterte forhold
- genetiske opplysninger
- biometriske opplysninger som anvendes til entydig identifisering av personer
- opplysninger om etnisk eller rasemessig bakgrunn
- opplysninger om politiske eller religiøse oppfatninger og livssyn
- opplysninger om seksuell forhold og -legning
- opplysninger om fagforeningsmedlemskap

Eksempler på sensitive personopplysninger kan være:

- opplysninger om studenters sykdom eller diagnoser
- opplysninger om sykdom registrert i forbindelse med ansattes sykefravær
- opplysninger om ansattes alkohol- eller rusmisbruk og fagforeningsaktivitet
- opplysninger om holdninger til ulike typer religiøse eller politiske spørsmål som respondenter i spørreundersøkelser oppgir

Datatilsynet skal etter dagens regelverk i mange tilfeller forhånds-godkjenne (gi konsesjon til) behandling av sensitive personopplysninger. Når forordningen trer i kraft, faller ordningen med forhånds-godkjenning (konsesjonsplikt) bort.[8]

Behandlingsansvarlig

I forordningen defineres behandlingsansvarlig som vedkommende virksomhet eller enkeltperson som bestemmer hva personopplysningene skal brukes til (formål) og hvilke elektroniske hjelpemidler (IT-systemer, -tjenester, -utstyr eller -infrastruktur) som skal anvendes til å behandle opplysningene.

[8] Justisdepartementet foreslår likevel at Datatilsynet kan gi konsesjon for behandling av personopplysninger i særlige og uforutsette situasjoner og hvor behandlingen er nødvendig av hensyn til viktige samfunnsinteresser, jf. «Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett», side 72-73 (se også § 7 i forslaget til ny personopplysningslov). Det fremstår som uklart hvilken betydning (om noen) som denne ordningen kan tenkes å få i UH-sektoren.

Behandlingsansvarlig er ansvarlig for at personopplysninger håndteres i tråd med reglene i forordningen og i den nye personopplysningsloven. Dersom dette ikke er tilfelle, kan den behandlingsansvarlige bli gjenstand for ulike typer sanksjoner, for eksempel overtredelsesgebyr eller tvangsmulkt (se del fire i denne veilederen).

Universiteter og høgskoler vil være behandlingsansvarlig for bruk av personopplysninger som skjer i forbindelse med egen forsknings- og undervisningsvirksomhet, administrasjon og kunnskapsformidling.

Databehandler

I forordningen defineres databehandler som en virksomhet eller enkeltperson som behandler personopplysninger på vegne av den behandlingsansvarlige.

Universiteter og høgskoler anvender databehandlere når de setter ut driften av IT-systemer eller IT-tjenester som håndterer personopplysninger til eksterne aktører. Databehandlere kan være kommersielle aktører, for eksempel leverandører av nettbaserte tjenester eller skytjenester. Det kan også være universiteter eller høgskoler som drifter administrative IT-systemer eller forskningsdatabaser på vegne av andre institusjoner i sektoren.

Databehandleren har et selvstendig ansvar for at personopplysninger som tilhører den behandlingsansvarlige håndteres i tråd med reglene i forordningen og i den nye personopplysningsloven. Dersom dette ikke er tilfelle, kan databehandleren bli gjenstand for ulike typer sanksjoner, for eksempel overtredelsesgebyr eller tvangsmulkt (se del fire i denne veilederen).

De registrerte

De personer (studenter, ansatte, osv.) som personopplysningene relaterer seg til.

Del 2: De sentrale kravene til informasjonssikkerhet

I denne delen av veilederen følger en kort gjennomgang av de viktigste reglene om informasjonssikkerhet i den nye personvernforordningen.

Informasjonssikkerhet som grunnprinsipp

I forordningens artikkel 5 nr. 1 bokstav f, defineres ivaretakelse av personopplysningenes konfidensialitet og integritet som et grunnprinsipp ved behandling av personopplysninger. At konfidensialitet og integritet defineres som grunnleggende ved behandling av personopplysninger, er nytt sammenliknet med dagens regelverk. Dette innebærer en statusheving for arbeidet med informasjonssikkerhet.

Kravet er at personopplysninger skal være tilfredsstillende sikret med hensyn til opplysningenes konfidensialitet og integritet. Det stilles videre krav om at universiteter eller høgskoler (behandlingsansvarlige) iverksetter tekniske eller organisatoriske tiltak som sørger for tilfredsstillende beskyttelse av konfidensialiteten og integriteten. Til slutt kreves det at universiteter eller høgskoler må kunne dokumentere sikringstiltakene.

Personopplysningenes tilgjengelighet synes ikke å være definert som et grunnprinsipp ved behandling av personopplysninger. Tilgjengeligheten til personopplysninger skal imidlertid også være tilfredsstillende sikret. Kravene til tilgjengelighet følger av reglene i forordningens artikkel 32 (se nedenfor).

Betydning

Det blir særlig viktig for universiteter og høgskoler å forebygge, avdekke og håndtere sikkerhetshendelser som kan føre til at uvedkommende får tilgang til opplysningene (konfidensialitetsbrudd) eller at opplysningene slettes eller endres på uautoriserte måter (integritetsbrudd).

Tiltak

Universiteter og høgskoler må gjennomføre grundige risikovurderinger av IT-løsninger (systemer, tjenester, digitalt utstyr eller elektronisk infrastruktur) som behandler personopplysninger. Det må legges særlig vekt på identifisering og vurdering av uønskede hendelser som kan føre til brudd på personopplysningenes konfidensialitet eller integritet. Risikovurderingene må oppdateres dersom det skjer endringer i IT-løsninger eller andre forhold, for eksempel omorganiseringer, som kan påvirke sikkerheten til personopplysningene.

Dernest må universiteter og høgskoler være påpasselige med å iverksette tekniske eller organisatoriske sikringstiltak dersom risikovurderingene viser at det er nødvendig (risikohåndtering). Dette gjelder spesielt (men ikke bare) med hensyn til IT-løsninger hvor det behandles sensitive personopplysninger eller større mengder alminnelige (ikke-sensitive) opplysninger. Slike IT-løsninger kan for eksempel omfatte Felles Studentsystem, lønns- og personalsystem, saks- og arkivsystem, e-postsystem, læringsplattform (LMS), forskningsdatabaser, bærbare dataenheter, skybaserte lagringstjenester eller lokal infrastruktur. Sekretariatet for informasjonssikkerhet i UH-sektoren kan bistå som rådgiver i risikovurderinger.

Risikovurderinger og etablering av tekniske eller organisatoriske sikringstiltak må dokumenteres og dokumentasjonen må tas vare på (arkiveres).

Øvrige grunnprinsipper

Universiteter og høgskoler må være oppmerksom på at forordningens grunnprinsipper ikke bare omhandler informasjonssikkerhet (konfidensialitet og integritet). Det stilles i tillegg en rekke andre grunnleggende krav til behandling av personopplysninger.

Øvrige grunnprinsipper omfatter krav om at

- behandlingen må ha et lovlig grunnlag,
- opplysningene brukes til spesifikke og uttrykkelig angitte formål,
- opplysningene ikke gjenbrukes til nye og uforenelige formål uten samtykke eller lovhjemmel,
- det ikke samles inn flere opplysninger enn nødvendig,
- opplysningene er korrekte og oppdaterte,
- opplysningene slettes eller anonymiseres når det ikke lenger er behov for dem.

For utfyllende informasjon om øvrige grunnprinsipper, se Datatilsynets temasider om personvernforordningen (www.datatilsynet.no).

Hovedreglene om informasjonssikkerhet

Hovedreglene om informasjonssikkerhet finnes i forordningens artikkel 32. Reglene gjelder uavhengig av om universiteter og høgskoler er behandlingsansvarlige eller databehandlere.

Kravet som stilles er at informasjonssikkerheten skal være tilfredsstillende med hensyn til personopplysningenes konfidensialitet, integritet, tilgjengelighet og robusthet. Tilfredsstillende informasjonssikkerhet skal oppnås ved at egnede tekniske og organisatoriske sikringstiltak iverksettes på bakgrunn av risikovurderinger.[9] I risikovurderingene skal det blant annet legges vekt på hvilke typer personopplysninger som behandles, hva opplysningene skal brukes til, hvor omfattende behandlingen vil være og i hvilken grad behandlingen representerer en trussel mot personvernet til de registrerte.

Det kreves videre at konfidensialiteten, integriteten, tilgjengeligheten og robustheten til IT-løsninger (systemer, tjenester, osv.) som behandler personopplysninger, skal være tilfredsstillende så lenge løsningene anvendes til behandling av slike opplysninger (kontinuerlig forbedring). Dernest skal det etableres tiltak som sørger for at tilgjengeligheten til personopplysninger gjenopprettes etter alvorlige tekniske eller fysiske sikkerhetshendelser (kontinuitet og beredskap). Til slutt skal det etableres rutiner for regelmessig testing, vurdering og evaluering av om etablerte tekniske eller organisatoriske sikringstiltak har hatt den ønskede effekten på informasjonssikkerheten (sikkerhetsrevisjoner).

Alle ansatte eller studenter som har tilgang til personopplysninger som universiteter og høgskoler er ansvarlige for, skal få instrukser, for eksempel i form av skriftlige rutiner og opplæring, som tydeliggjør hvordan opplysningene skal behandles.

Betydning

I sine merknader til hovedreglene om informasjonssikkerhet, legger Justisdepartementet til grunn at forordningens regler langt på vei tilsvarer reglene om informasjonssikkerhet som i dag finnes i personopplysningsloven § 13 og personopplysningsforskriften kapittel to.[10] Dette betyr at eksisterende veiledninger fra Sekretariatet for informasjonssikkerhet i UH-sektoren og tiltak som universiteter og høgskoler har iverksatt på bakgrunn av disse veiledningene, fortsatt vil være

[9] Pseudonymisering og kryptering nevnes spesifikt som tiltak som bør vurderes for å beskytte personopplysninger mot brudd på informasjonssikkerheten.

[10] Se «Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett», side 56. Tilgjengelig på https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/.

gyldige og kan videreføres når det nye regelverket trer i kraft. Det vil imidlertid være behov for enkelte tilpasninger og oppdateringer (se nedenfor).

Tiltak

Universiteter og høgskoler må etablere et ledelsessystem for informasjonssikkerhet basert på anerkjente standarder for styring av informasjonssikkerhet, for eksempel ISO/IEC 27001: 2013. De må videre sørge for at ledelsessystemet blir en integrert del av den øvrige virksomhetsstyringen. Sekretariatet for informasjonssikkerhet i UH-sektoren har utarbeidet en veileder (med dokumentmaler) som kan benyttes i arbeidet med etablering av et slikt ledelsessystem.

Universiteter og høgskoler som enda ikke har etablert et ledelsessystem for informasjonssikkerhet, må iverksette dette arbeidet snarest. Sekretariatet for informasjonssikkerhet i UH-sektoren kan bistå som rådgiver i etableringsarbeidet.

Universiteter og høgskoler som har etablert et ledelsessystem for informasjonssikkerhet, må sørge for å sette ledelsessystemet i drift. Som nevnt ovenfor, er det spesielt viktig at det gjennomføres risikovurderinger og at det etableres tekniske eller organisatoriske sikringstiltak (risikohåndtering) der hvor vurderingene viser at det er nødvendig. Sekretariatet for informasjonssikkerhet i UH-sektoren kan bistå som rådgiver i risikovurderinger.

Ledelsessystemet for informasjonssikkerhet og de aktiviteter som utføres innenfor rammen av ledelsessystemet, for eksempel risikovurderinger, etablering av sikringstiltak, håndtering av sikkerhetshendelser eller sikkerhetsrevisjoner, må dokumenteres og dokumentasjonen må tas vare på (arkiveres).

Varsling av sikkerhetshendelser

Reglene om varsling av sikkerhetshendelser finnes i forordningens artikkel 33 og 34. Her kreves det at universiteter og høgskoler (behandlingsansvarlige) varsler Datatilsynet eller de registrerte (student, ansatt, osv.) om hendelser som har ført til brudd på informasjonssikkerheten til personopplysningene.

Varsling til Datatilsynet

Det kreves at Datatilsynet varsles om sikkerhetshendelser som innebærer risiko for krenkelser av personvernet til de registrerte. Datatilsynet skal varsles innen 72 timer etter at

sikkerhetshendelsen er blitt kjent. Institusjonen kan be Datatilsynet om at varslingsfristen forlenges dersom det er nødvendig.

Varslet til Datatilsynet skal inneholde følgende informasjon:

- hva slags sikkerhetshendelse det er snakk om og hvor omfattende hendelsen er (omtrent hvor mange personer som er berørt og omtrent hvor mange personopplysninger det dreier seg om)
- navn og kontaktinformasjon til institusjonens personvernrådgiver (eller andre kontaktpersoner som Datatilsynet kan henvende seg til)
- de sannsynlige konsekvensene av sikkerhetshendelsen
- hvilke tiltak som er iverksatt for å håndtere sikkerhetshendelsen og for å redusere hendelsens negative virkninger

I tillegg kreves det at universitetet eller høgskolen dokumenterer sikkerhetshendelsen, effektene av hendelsen og hva som er gjort for å utbedre situasjonen.

For universiteter eller høgskoler som drifter IT-løsninger på vegne av andre institusjoner og hvor personopplysninger behandles (databehandlere), kreves det at «kundene» (behandlingsansvarlige) varsles om sikkerhetshendelser uten ubegrunnet opphold. «Kundene» er ansvarlige for at varslet videreformidles til Datatilsynet.

Varsling til de registrerte

Det kreves at hver enkelt registrert (student, ansatt, osv.) varsles om sikkerhetshendelser som innebærer høy risiko for krenkelse av hans eller hennes personvern. Varslingen skal skje uten ubegrunnet opphold, det vil si så fort universitetet eller høgskolen er blitt kjent med sikkerhetshendelsen.

Varsling til de registrerte skal utformes i et klart og tydelig språk, og skal inneholde følgende informasjon:

- hva slags sikkerhetshendelse det er snakk om
- navn og kontaktinformasjon til institusjonens personvernrådgiver (eller andre kontaktpersoner som de registrerte kan henvende seg til)
- de sannsynlige konsekvensene av sikkerhetshendelsen

- hvilke tiltak som er iverksatt for å håndtere sikkerhetshendelsen og for å redusere hendelsens negative virkninger

Det kreves ikke varsling dersom universitetet eller høgskolen iverksetter (eller allerede har etablert) tekniske eller organisatoriske tiltak som gjør det svært lite sannsynlig at sikkerhetshendelsen fører til krenkelser av de registrertes personvern. Det kreves heller ikke varsling dersom det ikke er mulig uten å røpe visse typer opplysninger, for eksempel opplysninger underlagt taushetsplikt.[11]

Dersom det er uforholdsmessig vanskelig og kostnadskrevende å varsle hver enkelt registrert, kan de isteden varsles gjennom en offentlig bekjentgjørelse.

For universiteter eller høgskoler som drifter IT-løsninger på vegne av andre institusjoner og hvor personopplysninger behandles (databehandlere), kreves det som nevnt at «kundene» (behandlingsansvarlige) varsles om sikkerhetshendelser uten ubegrunnet opphold. «Kundene» er ansvarlige for å videreformidle varslet til hver enkelt registrert (dersom det er påkrevd).

Datatilsynet kan pålegge universiteter eller høgskoler å varsle hver enkelt registrert om sikkerhetshendelser som institusjonene ikke har varslet om på eget initiativ.

Betydning

Forordningens regler om varsling innebærer at flere aktører må varsles og at det må varsles om flere typer sikkerhetshendelser enn hva tilfelle er i dag. I dag skal Datatilsynet varsles ved hendelser som medfører brudd på konfidensialiteten til personopplysninger. Med det nye regelverket skal også de registrerte varsles om hendelser som innebærer høy risiko for krenkelser av personvernet.

I tillegg gjelder ikke varslingsplikten bare for hendelser hvor uvedkommende får tilgang til personopplysninger (konfidensialitetsbrudd), men også for andre typer sikkerhetshendelser, for eksempel ved uautorisert endring eller sletting av personopplysninger (integritetsbrudd).

[11] Det samme gjelder for opplysninger som kan unntas offentlighet og som er av betydning for Norges utenrikspolitiske interesser, nasjonale forsvars- og sikkerhetsinteresser, eller opplysninger som må hemmeligholdes av hensyn til å forebygge, etterforske eller avdekke straffbare handlinger, jf. forslag til personopplysningslov § 13 fjerde ledd.

Tiltak

Universiteter og høgskoler må etablere løsninger og avsette ressurser til forebygging, avdekking og håndtering av sikkerhetshendelser. Dette inkluderer forsøk på hacking og dataangrep. Statlige universiteter og høgskoler har påbegynt dette arbeidet gjennom etablering av ledelsessystemer for informasjonssikkerhet og opprettelse av egne responsteam (IRT – Incident Response Team). Responsteamene skal inngå i institusjonenes ledelsessystemer. I samarbeid med UNINETT CERT,[12] har de lokale teamene blant annet i oppgave å dele informasjon om og å håndtere felles sikkerhetsutfordringer. Øvrige høgskoler i sektoren bør etablere tilsvarende ledelsessystemer og responsteam. UNINETT CERT vil være behjelpelig med etablering av slike responsteam.

Responsteamene i sektoren må ha egne rutiner for varsling av alle typer sikkerhetshendelser som de har i oppgave å forebygge, avdekke og håndtere, og som omfattes av forordningens krav til varsling. Rutinene må omfatte varsling både til Datatilsynet og til de registrerte.

Universiteter og høgskoler som har et ledelsessystem for informasjonssikkerhet, skal ha etablert rutiner for intern varsling av avvik og sikkerhetshendelser som alle ansatte og studenter kan benytte. Det skal også finnes rutiner for ekstern varsling, det vil si melding til Datatilsynet ved hendelser som medfører brudd på konfidensialiteten til personopplysninger. I lys av forordningens nye varslingskrav, må eksisterende rutiner for varsling til Datatilsynet oppdateres slik at de omfatter andre typer sikkerhetshendelser enn bare konfidensialitetsbrudd. I tillegg må rutinene tilpasses kravet om varsling til de registrerte.

Universiteter og høgskoler som enda ikke har et ledelsessystem for informasjonssikkerhet, må etablere dette. De må videre sørge for at ledelsessystemet omfatter rutiner for varsling av sikkerhetshendelser som avdekkes av institusjonenes responsteam. Tilsvarende rutiner må etableres for sikkerhetshendelser som avdekkes av andre ansatte eller studenter. Rutinene må gjelde for alle typer sikkerhetshendelser som omfattes av forordningens varslingskrav. I tillegg må rutinene omfatte varsling både til Datatilsynet og til de registrerte. Sekretariatet for informasjonssikkerhet i UH-sektoren kan bistå som rådgiver i arbeidet med etablering av ledelsessystemer og varslingsrutiner.

[12] Computer Emergency Response Team.

Det antas at varsling av sikkerhetshendelser til Datatilsynet etter hvert kan skje via Datatilsynets hjemmesider på internett. Varsling til de registrerte må institusjonene selv forestå. Slik varsling kan for eksempel skje via e-post.

Del 3: Krav med betydning for informasjonssikkerheten

I denne delen av veilederen gis en skjematisk gjennomgang av øvrige krav i forordningen som (direkte eller indirekte) har betydning for arbeidet med informasjonssikkerhet i UH-sektoren.

Internkontroll

I forordningens artikkel 24, kreves det at universiteter og høgskoler (behandlingsansvarlige) etablerer internkontroll. Internkontroll innebærer at universiteter og høgskoler pålegges å iverksette tiltak som sørger for og dokumenterer at reglene i forordningen (og i den nye norske personopplysningsloven) etterleves i det daglige arbeidet. Det stilles videre krav om at det etableres interne retningslinjer og rutiner for behandling av personopplysninger.

Informasjonssikkerhet

Institusjonens ledelsessystem for informasjonssikkerhet er en viktig del av internkontrollen. Ledelsessystemet skal sørge for og dokumenterer at reglene om informasjonssikkerhet etterleves. Dette inkluderer interne retningslinjer og rutiner for sikker håndtering av personopplysninger i forbindelse med bruk av institusjonenes IT-løsninger.

Universiteter og høgskoler må også sørge for tilfredsstillende informasjonssikkerhet i forbindelse med bruk av de registrertes rettigheter. [13] Dette kan for eksempel omfatte autentisering av studenter som krever innsyn i egne personopplysninger eller rutiner for sikker håndtering av krav om retting eller sletting av personopplysninger.

Andre plikter

Institusjonene må i tillegg iverksettes tiltak som sørger for og dokumenterer at øvrige krav og plikter i forordningen etterleves. Dette gjelder blant annet grunnprinsippene for behandling av personopplysninger (forordningens artikkel 5), ivaretakelse av de registrertes rettigheter (forordningens kapittel tre[14]) og rutiner ved overføring av personopplysninger til land utenfor EU/EØS-området (forordningens kapittel fem).

[13] De registrertes rettigheter omfatter retten til å få informasjon om behandling av personopplysninger, retten til innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger, retten til å kreve begrenset behandling av egne personopplysninger, retten til å motsette seg behandling av egne personopplysninger, retten til overføring av egne personopplysninger til nye mottakere (dataportabilitet) og retten til ikke å være gjenstand for avgjørelser utelukkende fattet av automatiske beslutningssystemer.

[14] De registrertes rettigheter omfatter retten til å få informasjon om behandling av personopplysninger, retten til innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger, retten til å

For nærmere informasjon om disse og andre krav og plikter som inngår i internkontrollen, se Datatilsynets temasider om det nye regelverket (www.datatilsynet.no).

Protokoll over behandlingsaktiviteter

I forordningens artikkel 30, kreves det at universiteter og høgskoler som er ansvarlige for behandlinger av personopplysninger (behandlingsansvarlige) skal føre en oversikt (protokoll) over behandlingene. Tilsvarende krav gjelder for universiteter og høgskoler som drifter IT-løsninger på vegne av andre institusjoner og hvor personopplysninger behandles (databehandlere). Oversikten (protokollen) vil være en del av institusjonenes internkontroll.

Informasjonssikkerhet

Oversikten (protokollen) skal omfatte generelle beskrivelser av hvilke tekniske eller organisatoriske tiltak som er iverksatt for å beskytte personopplysningene mot brudd på informasjonssikkerheten. Denne delen av oversikten (protokollen) vil kunne hentes fra institusjonenes sikkerhetsdokumentasjon. Denne dokumentasjonen vil blant annet omfatte hvilke risikovurderinger som er gjennomført og hvilke sikringstiltak som er etablert på grunnlag av risikovurderingene.

Andre plikter

I tillegg skal oversikten (protokollen) omfatte informasjon om

- hva personopplysningene brukes til (formål),
- hvilke typer personopplysninger som behandles i ulike IT-løsninger,
- hvem opplysningene gjelder,
- hvilke eksterne aktører som eventuelt gis tilgang til opplysningene,
- opplysningene overføres til land utenfor EU/EØS-området og hvilket overføringsgrunnlag som i så fall anvendes,
- (hvis mulig) hvor lenge opplysningene vil bli oppbevart,
- hvem ved institusjonen som kan kontaktes for å svare på spørsmål om personvern og informasjonssikkerhet.

kreve at begrenset behandling av egne personopplysninger, retten til å motsette seg behandling av egne personopplysninger, retten til overføring av egne personopplysninger (dataportabilitet) og retten til ikke å være gjenstand for avgjørelser utelukkende fattet av automatiske beslutningssystemer.

Oversikten (protokollen) skal være tilgjengelig for Datatilsynet.

Innebygd personvern og personvern som standardinnstilling

I forordningens artikkel 25, kreves det at universiteter og høgskoler (behandlingsansvarlige) iverksetter egnede tiltak som sørger for at personvern blir en integrert del av IT-løsninger som anvendes til behandling av personopplysninger. Kravet innebærer at personvernet skal tas hensyn til gjennom hele livsløpet til IT-løsningene, det vil si fra utvikling eller anskaffelse via testing og produksjon/bruk til avvikling.

Informasjonssikkerhet

Kravet til innebygd personvern og personvern som standardinnstilling omfatter tiltak for å beskytte personopplysningene mot brudd på informasjonssikkerheten. Et sikringstiltak som nevnes spesifikt i forordningen, er pseudonymisering av personopplysninger. Ut over dette, kan en rekke andre innebygde sikringstiltak være aktuelle, for eksempel kryptering, tilgangsstyring, sikkerhetskopiering eller aktivitetslogging.

Andre plikter

Kravet om innebygd personvern og personvern som standardinnstilling omfatter ikke bare informasjonssikkerhet. Det omfatter også krav om innebygd funksjonalitet som ivaretar andre personvernhensyn. Dette kan for eksempel være løsninger som gir de registrerte innsyn i egne personopplysninger (min side-funksjonalitet) eller automatisk sletting av personopplysninger når institusjonene ikke lenger har bruk for eller lov til å oppbevare dem.

Vurdering av personvernkonsekvenser og forhåndsdrøftelser

I forordningens artikkel 35, kreves det at universiteter og høgskoler (behandlingsansvarlige) skal vurdere personvernkonsekvensene før bruk av visse typer IT-løsninger hvor personopplysninger behandles. Plikten gjelder uavhengig av om de aktuelle behandlingene eller IT-løsningene driftes internt eller av eksterne aktører (databehandlere).

Det er i dag uklart når universiteter og høgskoler eventuelt vil ha plikt til å gjennomføre vurderinger av personvernkonsekvenser. I forordningen kreves det blant annet at slike vurderinger gjennomføres før det iverksettes behandling av store mengder sensitive personopplysninger. Det kan derfor tenkes at plikten vil gjelde for store forskningsprosjekter som behandler sensitive personopplysninger, for eksempel opplysninger om enkeltpersoners helse.

Datatilsynet pålegges å publisere en liste over hvilke behandlinger eller IT-løsninger som omfattes av plikten til å gjennomføre personvernkonsekvensvurderinger. Det antas at listen etter hvert vil bli gjort tilgjengelig via Datatilsynets hjemmesider på internett. Universiteter og høgskoler må selv sjekke Datatilsynets liste for å finne ut om de har plikt til å gjennomføre vurderinger av personvernkonsekvenser.

Informasjonssikkerhet

Det kreves at det iverksettes egnede tekniske eller organisatoriske tiltak dersom personvernkonsekvensvurderingen viser at behandlingen av personopplysninger eller bruken av den aktuelle IT-løsningen innebærer en uakseptabel høy risiko for krenkelser av de registrertes personvern. Konsekvensvurderingen må derfor omfatte informasjonssikkerhet. Videre må det iverksettes egnede tiltak for å forebygge, avdekke eller håndtere brudd på informasjonssikkerheten dersom konsekvensvurderingen viser at det er nødvendig.

I forordningens artikkel 36, kreves det at universiteter og høgskoler (behandlingsansvarlige) tar kontakt med Datatilsynet for forhåndsdrøftelser dersom personvernkonsekvensvurderingen viser at behandlingen eller bruken av den aktuelle IT-løsningen innebærer en uakseptabel høy risiko for krenkelser av de registrertes personvern. Dette kan for eksempel være som følge av mangelfull informasjonssikkerhet. Universitetet eller høgskolen skal blant annet informere Datatilsynet om hvilke tiltak som planlegges iverksatt for å redusere risikoen til et akseptabelt nivå.

Etter at universitetet eller høyskolen har tatt kontakt med Datatilsynet, har Datatilsynet plikt til å gi skriftlig veiledning om hvordan risikoen kan håndteres. Veiledningen fra Datatilsynet kan blant annet inneholde vurderinger av om planlagte sikringstiltak er tilstrekkelige, eller om det er behov for ytterligere eller andre typer tiltak. Datatilsynet kan også bestemme at behandlingen eller den aktuelle IT-løsningen innebærer en så høy sikkerhetsrisiko at den ikke kan tas i bruk.

Datatilsynets skriftlige veiledning skal gis innen åtte uker etter at universitetet eller høgskolen har kontaktet Datatilsynet. Fristen kan forlenges med nye seks uker dersom Datatilsynet har behov for det.

Andre plikter

Plikten til å gjennomføre personvernkonsekvensvurderinger inkluderer vurderinger av andre forhold enn bare informasjonssikkerhet. Hvilke andre forhold som også må vurderes, fremgår av Datatilsynets veileder «Vurdering av personvernkonsekvenser etter nytt regelverk». Veiledningen er tilgjengelig på https://www.datatilsynet.no/regelverk-og-skjema/veiledere/vurdering-av-personvernkonsekvenser2/

Sekretariatet for informasjonssikkerhet i UH-sektoren vil tilby rådgiving til universiteter og høgskoler som må gjennomføre vurderinger av personvernkonsekvenser.

Personvernrådgiver (ombud)

I forordningens artikkel 37-39, kreves det at enkelte virksomheter utpeker en personvernrådgiver. Plikten til å utnevne personvernrådgivere gjelder uavhengig av om virksomhetene er behandlingsansvarlige eller databehandlere.

Plikten til å utpeke personvernrådgivere gjelder blant annet for forvaltningsorganer. Den vil derfor omfatte universiteter og høgskoler.

Informasjonssikkerhet

Det kreves at personvernrådgiverne har spesialkompetanse om det nye regelverket og om personvern. Dette innebærer at rådgiverne også må ha en viss kompetanse om hvilke regler som gjelder på informasjonssikkerhetsområdet og hvordan reglene kan etterleves.[15]

Andre plikter

I tillegg til reglene om informasjonssikkerhet, skal personvernrådgiverne informere om og gi veiledning til universiteter og høgskoler om hvordan de øvrige reglene i det nye regelverket kan etterleves. Rådgiverne skal føre kontroll med at universiteter og høgskoler etterlever regelverket.

Nærmere informasjon om personvernrådgivernes stilling og arbeidsoppgaver finnes i Datatilsynets veileder «Personvernombud etter nytt regelverk». Veilederen er tilgjengelig på

[15] Det er fortsatt noe uklart om dagens ombudsordning for forskning, som ivaretas av Norsk senter for forskningsdata (NSD), vil bli videreført i sin nåværende form, jf. «Ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett», side 39 (tilgjengelig på https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/). Universiteter og høgskoler kan i tillegg bli pålagt å utnevne personvernrådgivere for andre deler av kjernevirksomheten, for eksempel studentadministrasjon.

https://www.datatilsynet.no/regelverk-og-skjema/veiledere/personvernombudsordningen-etter-nytt-regelverk/.

Databehandlere og databehandleravtaler

I forordningens artikkel 28, kreves det at universiteter og høgskoler (behandlingsansvarlige) ikke engasjerer databehandlere som ikke etterlever reglene i forordningen. Det kreves videre at universitetet eller høgskolen inngår en særskilt avtale med databehandlerne som regulerer hvordan de skal håndtere institusjonenes personopplysninger (databehandleravtale).

Informasjonssikkerhet

Universiteter og høgskoler kan bare engasjere databehandlere som er i stand til å ivareta personopplysningenes informasjonssikkerhet på en tilfredsstillende måte. Institusjonene må selv undersøke og ta stilling til om informasjonssikkerheten i databehandlernes IT-løsninger er god nok. Dette gjøres ved å gjennomføre en risikovurdering av den aktuelle IT-løsningen før løsningen tas i bruk. Dersom risikovurderingen viser at informasjonssikkerheten ikke er tilfredsstillende, kan ikke IT-løsningen tas i bruk på lovlig måte.

Videre kreves det at avtalen mellom universitetet eller høgskolen og databehandleren regulerer hvordan databehandleren skal beskytte personopplysningene mot brudd på informasjonssikkerheten. Etter at avtalen med databehandleren er inngått, må universitetet eller høgskolen forsikre seg om at avtalevilkårene overholdes. Dette inkluderer kontroll med at databehandleren overholder de krav som avtalen stiller til informasjonssikkerheten.

Sekretariatet for informasjonssikkerhet i UH-sektoren har laget en sjekkliste som viser hvilke forhold som skal reguleres i avtalen med databehandleren. Sjekklisten er tilgjengelig på Sekretariatets hjemmesider på internett (https://www.uninett.no/infosikkerhet).

Andre plikter

Dersom bruk av databehandlerens IT-løsning innebærer at personopplysninger overføres til land utenfor EU/EØS-området, må universitetet eller høgskolen forsikre seg om at det finnes et lovlig grunnlag for overføringen. Et slikt lovlig grunnlag kan for eksempel være at personopplysningene overføres til land som EU har godkjent som trygge mottakerland. Dersom personopplysningene overføres til ikke-godkjente land, kan overføringen likevel skje på visse

vilkår, for eksempel på grunnlag av EUs standard dataoverføringsavtaler[16] eller til private virksomheter i USA som har sluttet seg til Privacy Shield-ordningen.[17]

Reglene om overføring av personopplysninger til tredjeland (land utenfor EU/EØS-området), finnes i forordningens kapittel fem.

Atferdsnormer og sertifisering

I forordningens artikkel 40-43 finnes regler om etablering av atferdsnormer (bransjenormer) og sertifiseringsordninger som skal sikre bedre etterlevelse av reglene i forordningen (og i den nye norske personopplysningsloven). I hvilken grad det vil bli etablert slike normer eller ordninger som har betydning for arbeidet med informasjonssikkerhet i UH-sektoren, gjenstår å se.

[16] EUs standard dataoverføringsavtaler er tilgjengelige på http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

[17] Informasjon om Privacy Shield-ordningen er tilgjengelig på http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.

Del 4: Datatilsynet, sanksjoner og erstatning

I denne delen av veilederen gis en kort oversikt over Datatilsynets oppgaver og myndighet, hvilke sanksjoner som Datatilsynet kan ilegge universiteter og høgskoler og reglene om erstatning ved krenkelser av de registrertes personvern.

Datatilsynet

I forordningens artikkel 57 og 58 gis regler om Datatilsynets organisering og myndighet. Datatilsynet skal blant annet føre kontroll med og håndheve etterlevelsen av det nye regelverket. Det skal videre ha informasjons- og rådgivingsoppgaver.

De registrerte (studenter, ansatte, osv.) har rett til å klage til Datatilsynet dersom de mener at universitetet eller høgskolen behandler deres personopplysninger i strid med regelverket (jf. også artikkel 77).

Overtredelsesgebyr

Datatilsynet kan ilegge universiteter og høgskoler overtredelsesgebyr for brudd på mange av reglene i forordningen (og i den nye norske personopplysningsloven).

For manglende etterlevelse av grunnprinsippene ved behandling av personopplysninger, inkludert kravet til sikring av personopplysningenes konfidensialitet og integritet, er gebyret begrenset oppad til 20 millioner euro (jf. artikkel 83 nr. 5 bokstav a).

For brudd på forordningens øvrige regler om informasjonssikkerhet, er gebyret begrenset oppad til 10 millioner euro (jf. artikkel 83 nr. 4 bokstav a).

Tvangsmulkt

Datatilsynet kan ilegge universiteter og høgskoler tvangsmulkt dersom vedtak om retting av regelavvik ikke oppfylles innen den fristen som Datatilsynet har satt.

Tvangsmulkt kan gis for manglende oppfyllelse av vedtak om retting av avvik som gjelder reglene om informasjonssikkerhet.

Erstatning

Universiteter og høgskoler har et erstatningsansvar overfor alle som har lidd skade som følge av manglende etterlevelse av regelverket. Dette gjelder uavhengig av om universiteter eller høgskoler er behandlingsansvarlige eller databehandlere.

Erstatning kan kreves for skade som følge av manglende etterlevelse av reglene om informasjonssikkerhet.

Straff

Det er ikke bestemt om straffebestemmelsene i dagens personopplysningslov (§ 48) vil bli videreført i det nye regelverket. Justisdepartementet vil ta stilling til dette spørsmålet etter at den nye norske personopplysningsloven har vært på høring.

Uavhengig av om straffebestemmelsene videreføres eller ikke, kan brudd på informasjonssikkerheten sanksjoneres i straffeloven. Dette gjelder for eksempel brudd på taushetsplikten (jf. straffeloven §§ 209 og 210).

Klage på vedtak

Personvernnemnda foreslås videreført i det nye regelverket (www.personvernnemnda.no/). Det betyr at universiteter og høgskoler kan klage vedtak fattet av Datatilsynet inn for nemnda. Dette omfatter vedtak som gjelder reglene om informasjonssikkerhet.