Førstelinjeforum UH-IT

26. okt 2018

Øivind Hope
IT sikkerhetsansvarlig
UiB/IT avdelingen

Førstelinjen som sikkerhetsventil rundt GDPR

- En sikkerhetsventil er en mekanisme som skal håndtere trykk eller temperatur som passerer et forhåndsinnstilt nivå.
- Vi må kunne svare på noen flere spørsmål enn de mest vanlige angående GDPR.

Agenda

- Fakta og generell informasjon (definisjoner)
- Virksomheters plikter
- Registrertes rettigheter
- Anbefalinger
  - Tre ting du må vite litt om

GDPR-General Data Protection Regulation

- Hvert enkelt land har hatt sine egne lover for behandling av personopplysninger
  ---
- GDPR i tillegg til egne lover en forordning som skal styrke og harmonisere personvernet ved behandling av personopplysninger
- For å støtte den økonomiske utviklingen i EU
- Ønske om at enkeltpersoner bedre skal ha kontroll om registrerte opplysninger om seg selv
- Omfatter alle utenlandske selskap som behandler data om innbyggere i EU
- Trådte i kraft 20. juli 2018

Personopplysningsloven med personvernforordningen

Lov om behandling av personopplysninger (personopplysningsloven)

Dato	LOV-2018-06-15-38
Departement	Justis- og beredskapsdepartementet
Ikrafttredelse	20.07.2018
Endrer	LOV-2000-04-14-31
Kunngjort	15.06.2018
Korttittel	Personopplysningsloven

Official Journal of the European Union

L 119

English edition

Legislation

Volume 59

4 May 2016

Contents

I *Legislative acts*

REGULATIONS

★ **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)** (1) 1

11 kapitler/99 artikler/knapt 90 sider

- Alminnelige bestemmelser
- Prinsipper
- Den registrertes rettigheter
- Behandlingsansvarlige og databehandler
- Trussel om store bøter dersom en ikke etterlever forordningen

GDPR-General Data Protection Regulation

- Mye av det en kjenner til fra POL gjelder
- Virksomheter får flere plikter:
  - Personvernombud
  - Oversikt/register over alle behandlinger av personopplysninger
  - Personvernerklæring

GDPR – prinsipper - art 5

Behandling av personopplysninger:

- Skal behandles lovlig, rettferdig og åpen
- Skal samles inn og behandles for spesifikke formål
- Være adekvate, relevante og begrenset til det som er nødvendig for formålet
- Lagres etter prinsipper for informasjonssikkerhet
- Behandles etter prinsipper for informasjonssikkerhet

GDPR – prinsipper - art 7

Vilkår for samtykke:

- Den behandlingsansvarlige må kunne påvise at den registrerte har samtykket til behandling
- Den registrerte skal ha rett til å trekke tilbake sitt samtykke til enhver tid (på en like enkel måte som en gir samtykket)

Hva er personvern?

- EMK artikkel 8:
  - Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
- Grunnlovens §102:
  - Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.

Hva er personopplysninger?

- Alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson
- navn, adresse, telefonnummer, epost adresse, fødselsnummer, id, et bilde, et lydopptak/videopptak, biometri, (dynamiske) ip-adresser, bilnummer, opplysninger om adferd (hva du handler og hvor, hva du ser på TV, hvor du fysisk beveger deg, og hva du søker etter på internettet er eksempler på dette)

GDPR – prinsipper - art 9

Sensitive personopplysninger/særlige kategorier

rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap, genetiske opplysninger, biometriske, helseopplysninger, seksuelle forhold, seksuell legning, straffedommer, lovovertredelser

GDPR – prinsipper - art 9

Sensitive personopplysninger/særlige kategorier

- Tidligere måtte en ha konsesjon fra datatilsynet for å behandle sensitive (Datatilsynet var ansvarlig)
- Nå trenger en ikke konsesjon (behandlingsansvarlige er ansvarlig)
  En må være i tråd med forordningen.

Behandle

Fra art 4, hva menes med «behandling»?

enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke

f. eks.

innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring

Virksomheters plikter – art 24-43

Overordnet

- Gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at behandlingene er i tråd med GDPR
- Innebygd personvern skal være standard
- Dersom en behandlingsansvarlig engasjerer en ekstern databehandler, skal det etableres en databehandleravtale

Virksomheters plikter – art 24-43

fastsette **formål**, ha **behandlingsgrunnlag**, informasjon og åpenhet, tillate retting og sletting, legge til rette for registrertes retter, ha **personvernombud**, gjennomføre DPIA og forhåndsdrøftelser, innebygd personvern, etablere internkontroll, informasjonssikkerhet, **protokoll/register over behandlingsaktiviteter**, databehandleravtaler, **håndtering av avvik**, overføringer

Virksomheters plikter – art 24-43

Formål med behandlingen

- For å kunne administrere et studie/kurs/arrangement/søknad
- For å kunne administrere ansatt slik at de f eks kan føre timer og få lønn
- For å kunne drive forskning eller undervisning
- For å kunne informere
- For å kunne tilby en tjeneste
- For å oppfylle avtaler med leverandører
- Myndighetspålagt (for skatteetaten)

Virksomheters plikter – art 24-43

Behandlingsgrunnlag

- Samtykke
- For å tilby en tjeneste
- Nødvendig for å oppfylle avtale
- Nødvendig for å oppfylle en rettslig forpliktelse

Virksomheters plikter – art 24-43

Oversikt over behandlinger

Hver behandling skal inneholde følgende:

- Internt ansvarlige
- Funksjonsområde
- Virksomhetsområde
- Formål
- Kategorier av registrerte
- Kategorier av personopplysninger
- Kilde
- Mottakere
- Behandlingsgrunnlag art 6
- Behandlingsgrunnlag art 9 eller art 10
- Rettslig forpliktelse
- Tjeneste opplysningene behandles i
- Frister for sletting
- Tekniske/organisatoriske sikkerhetstiltak
- Kan behandlingen innebære høy personvernrisiko (DPIA)
- Behandlingsansvarlig (navn)
- Databehandler (navn)
- Navn på tredjeland/internasjonal organisasjon som personopplysninger overføres til
- Nødvendige garantier ved overføringer til tredjeland/internasjonale organisasjoner

Virksomheters plikter – art 24-43

Oversikt over behandlinger - verktøy

Protokoll over behandlingsaktiviteter etter artikkel 30 i personvernforordningen

Behandlingsansvarlig virksomhet

Kontaktopplysninger:

	Behandlingsansvarlig	Personvernombud Hvis aktuelt	Behandlingsansvarliges representant Fylles inn dersom den behandlingsansvarlige er etablert utenfor EØS-området
Navn			
Postadresse			
Telefon			
Epost			

Internt ansvarlig F.eks. avdeling, rolle, eller person	Funksjonsområde Hvilket overordnet funksjons- eller virksomhetsområde faller behandlingen under?	Hva gjelder behandlingen Virksomhetsområde, overordnet behandlingsaktivitet	Formål med behandlingen	Kategorier av registrerte	Kategorier av personopplysninger	Hvor kommer personopplysningene fra? (Kilde)	Kategorier av mottakere Dersom aktuelt også i tredjestater eller internasjonale organisasjoner	Behandlingsgrunnlag artikkel 6	Rettslig forpliktelse, berettiget interesse mv Henvise til dersom beh.grunnlag er 6.1.c,e eller f Dersom relevant	Behandlingsgrunnlag artikkel 9 eller 10 Med ev henvisning også til annen lovgivning Dersom relevant	I hvilke av våre systemer behandles opplysningene?	Planlagte tidsfrister for sletting Av de forskjellige kategorier av personopplysninger Dersom mulig	Generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak Som nevnt i artikkel 32. nr 1 Dersom mulig	Kan behandlingen innebære høy personvernrisiko? Blant annet med hensyn til ev gjennomføring av DPIA	Navn på databehandlere (Husk databehandleravtalen!) Dersom relevant	Navn og kontaktopplysninger til felles behandlingsansvarlig Dersom relevant	Navn på tredjeland eller internasjonale organisasjoner som personopplysninger overføres til Dersom relevant	Nødvendige garantier ved overføring til tredjeland eller internasjonale organisasjoner Dersom relevant
HR-direktør	Intern administrasjon og økonomi	Personaladministrasjon	Rekruttering	Tilsatte kandidater	Kontaktopplysninger	Den registrerte	_	Artikkel 6(1)(b) - avtale	_	_	Sak/arkiv	x måneder etter avslutning av rekrutteringsprosess	kryptert lagring, tilgangskontroll	Nei	_	_	_	_
HR-direktør	Intern administrasjon og økonomi	Personaladministrasjon	Rekruttering	Søkere som ikke har fått jobben	Søknad og CV	Den registrerte	_	Artikkel 6(1)(a) - samtykke	_	_	Sak/arkiv	x måneder etter avslutning av rekrutteringsprosess	Tilgangskontroll	Nei	_	_	_	_
HR-direktør	Intern administrasjon og økonomi	Personaladministrasjon	Personalmappe	Ansatte	Kontaktopplysninger	Den registrerte	_	Artikkel 6(1)(b) - avtale	_	_	Sak/arkiv	x år etter avslutning av arbeidsforhold	tilgangskontroll	Nei	_	_	_	_
HR-direktør	Intern administrasjon og økonomi	Personaladministrasjon	Rekruttering	Tilsatte kandidater	Kontaktopplysninger	Den registrerte	_	Artikkel 6(1)(b) - avtale	_	_	Sak/arkiv	x år etter avslutning av arbeidsforhold	Kryptert lagring og overføring	Nei	_	_	_	_
Lønningssjef	Intern administrasjon og økonomi	Lønn	Lønnskjøring og utbetaling	Ansatte	Skatt og arbeidsgiveravgift	Egen virksomhet	Regnskapsbyrået (lønnskjører)	Artikkel 6(1)(c) - rettslig forpliktelse	Skattebetalingsloven, A-meldingsloven	_	Employ	x år etter avslutning av arbeidsforhold	Kryptert lagring og overføring	Nei	Lønnsskjøring AS	_	_	_
Lønningssjef	Intern administrasjon og økonomi	Lønn	Lønnskjøring og utbetaling	Ansatte	Kontaktopplysninger	Den registrerte	Regnskapsbyrået (lønnskjører)	Artikkel 6(1)(c) - rettslig forpliktelse	Skattebetalingsloven, A-meldingsloven	_	Employ	x år etter avslutning av arbeidsforhold	Kryptert lagring og overføring	Nei	Lønnsskjøring AS	_	_	_
Salgsdirektør	Salg og kundekontakt	Salg	Direkte markedsføring	Eksisterende kunder	Kontaktopplysninger	Den registrerte	Databehandler, markedsføring	Artikkel 6(1)(a) - samtykke	_	_	CRM	Straks kundeforholdet er avsluttet	_	Nei	_	_	_	_
Salgsdirektør	Salg og kundekontakt	Salg	Direkte markedsføring	Potensielle kunder	Kontaktopplysninger	Adressemekler	Databehandler, markedsføring	Artikkel 6(1)(a) - samtykke	_	_	CRM	x uker etter at kampanjen er avsluttet	_	Nei	_	_	_	_

Virksomheters plikter – art 24-43

Behandling av personopplysninger

Behandlingsansvarlig: Universitetet i Bergen

Behandling	Tjeneste	Databehandler
Administrasjon av brukerkonto (SEBRA)	Administrasjon av brukerkonto (SEBRA)	Universitetet i Bergen, IT-avdelingen
Alumnidatabasen	(	gen, IT-avdelingen
Ansettelsesprosessen	S	gen, IT-avdelingen
Avviksmelding	(	gen, IT-avdelingen
Behandling av personinformasjon i AD	(	gen, IT-avdelingen
Behandling av personinformasjon i Azure-AD	(	gen, IT-avdelingen
Behandling av personinformasjon i UH-AD	(	gen, IT-avdelingen
Bekreftelse studentstatus EVU	(	gen, IT-avdelingen
bioCEEDnews - Nyhetsbrev fra senter for fremragende utdanning i biologi - bioCEED	(	gen, IT-avdelingen

Behandling av persondata

Ansettelsesprosessen

Skrevet av st10836 4. juli 2018 - 10:24

Tjeneste:
Saksbehandlings- og arkivsystem (ePhorte)

Behandlingsansvarlig:
Universitetet i Bergen

Internt ansvarlig:
HR-avdelingen

Kontaktperson for behandlingen:
Terje Askvik

Beskrivelse:
Søkerliste og utvidet søkerliste, innstilling m/ vurderinger og ansettelsesvedtak

Formålet med behandlingen:
Ansettelse

Behandlingsgrunnlag:
- Samtykke
- Nødvendig for å oppfylle avtale mv
- Nødvendig for å oppfylle en rettslig forpliktelse

Behandlingssted:
ePhorte

Personopplysninger:
Navn, kontaktinformasjon, personalia, utdanning, praksis, sensitive opplysninger (nedsatt funksjonsevne/ etnisitet) samt vurderinger av personen

Opphav:
JobbNorge, den registrerte, referanser

Informasjon gitt til de registrerte:
- Ukjent

Strukturerte data:
- Ja

Sletting:
Ihht arkivlov

Særlige kategorier:
- Ja

Virksomheters plikter – art 24-43

Ved avvik skal behandlingsansvarlige melde fra:

- til tilsynsmyndigheter innen 72 timer etter å ha fått kjennskap til bruddet.
  Beskrive bruddet, oppgi antall berørte og eventuelle tiltak for å redusere skadeomfang.
  (Datatilsynet har en egen portal for dette der personvernombudet med flere i en virksomhet, skal ha tilgang til å registrere avvik)
- til den registrerte

Virksomheters plikter – art 24-43

Personvernombud/personrådgiver

- Alle offentlige virksomheter skal ha personvernombud
- Alle som behandler personopplysninger som en del av hovedaktiviteten i virksomheten skal ha personvernombud

Virksomheters plikter – art 24-43

Personvernombud/personrådgiver

- Skal **involveres** på riktig måte og i rett tid i alle spørsmål som gjelder vern av personvern.
- **Informere og gi råd** til behandlingsansvarlige, databehandlere og ansatte som utfører behandling
- **Kontrollere** at en følger forordningen, fordeler ansvar, **gjøre holdningsskapende tiltak** og **opplæring av ansvarlige og utførende** av behandling + tilhørende revisjoner
- På anmodning **gi råd om vurdering av konsekvenser** i henhold til art 35
- **Samarbeide med tilsynsmyndigheter**
- **Kontaktpunkt** for tilsynsmyndigheter/kan ved behov rådføre seg med tilsynsmyndigheter
- Ved utførelse av egne oppgaver, **ta behørig hensyn** til risikoer forbundet med behandlingsaktivitetene

Virksomheters plikter – art 24-43

Personvernombud/personrådgiver

- Virksomheter kan **behandle særlige kategorier** av personopplysninger (tidligere kalt *sensitive personopplysninger*) **uten *samtykke***. I disse tilfellene har den behandlingsansvarlige *plikt til å rådføre seg med* personvernombudet.
  (gjelder f eks forskningsprosjekter)

Personvernerklæring

- Gi overordnet informasjon om behandling av personopplysninger.
- Hvem som er ansvarlig for behandling av dine personopplysninger
- For hvilke formål behandles personopplysninger
- Hvilke plikter har en når en behandler opplysningene.
- Hvilke rettigheter en har som registrert.

PERSONVERNERKLÆRING

Personvernerklæring for Universitete…en

Denne erklæringen redegjør for hvordan Universitetet i Bergen (UiB) samler inn og bruker p…
Målet med personvernerklæringen er å gi overordnet informasjon om UiBs behandling av p…

- Dine rettigheter
- Hva registreres når du besøker nettsidene våre?
- Opplysninger om studenter og søkere t…
- Behandling av ansattes personopplysni…
- Behandling av opplysninger om forskni…
- Behandling av opplysninger om pasien…
- Utlevering og innsyn
- Sikring av personopplysninger i IT-logg…
- Sikring av UiBs lokaler
- Behandling av personopplysninger i dokumentasjonsforvaltning, saksbehandling og arkiv

Denne personvernerklæringen handler om

- Hvem som er ansvarlig for behandling av dine personopplys…
- For hvilke formål UiB behandler personopplysninger
- Hvilke plikter UiB har når vi behandler opplysningene.
- Hvilke rettigheter du har som registrert hos oss.

PERSONVERNOMBUD

UiBs personvernombud er: Janecke Helene Veim

Kontaktinformasjon til personvernombudet: personvernombud@uib.no

BEHANDLINGSANSVARLIG

Den som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

HVA ER PERSONOPPLYSNINGER?

Personopplysninger er alle former for data, informasjon, opplysninger og vurderinger som kan knyttes til deg som enkeltperson, jf. personvernforordningen artikkel 4 nr. 1. Det avgjørende for om en opplysning er en personopplysninger er om opplysningene kan identifisere en konkret person. Eksempler på personopplysninger om deg som blir registrert og behandlet ved UiB er opplysninger som navn, bilde, kontaktinformasjon, undervisnings- og eksamensmeldinger og karakterer.

SÆRLIGE KATEGORIER (SENSITIVE) ER PERSONOPPLYSNINGER OM

Rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, gentiske og bometriske opplysninger, helseopplysninger eller opplysninger om seksuelle forhold.

Registrertes rettigheter – art 12-23

- Det overordnede målet med reglene er å gi vanlige folk bedre kontroll over hvilke personopplysninger ulike virksomheter har og behandler.

Registrertes rettigheter – art 12-23

Har rett til:

Innsyn, retting, sletting, begrensing, rett til å protestere, retter ved automatiserte behandlinger og rett til dataportabilitet.

- Alle virksomheter skal legge til rette for at brukere/kunder får oppfylt rettighetene sine på en enkel måte
- Skal gjøres uten kostnader for den registrerte innen 30 dager
  (adm gebyr kan forekomme dersom forespørsel er grunnløs, overdrevet eller gjentatt)

Registrertes rettigheter – art 12-23

Innsyn

- Hva er formålet?
- Hvilke opplysninger om deg har virksomheten lagret?
- Utlevering av opplysninger, til hvem?
- Hvor lenge lagres de?
- Rett til retting, sletting, avgrensing eller protestere
- Hvor kommer opplysningen fra?
- Automatiseres behandlinger?

Registrertes rettigheter – art 12-23

Begrensninger i innsyn dersom opplysningene sikrer

den nasjonale sikkerhet, forsvaret, den offentlige sikkerhet, forebyggende etterforskning, avsløringer av straffbare forhold, økonomiske forhold, brudd på yrkesetiske regler i lovregulerte yrker, vern av registrert eller andres interesser, sivilrettslige krav mm

Dette bør en vite noe om:

- Oppgaver til og kontaktinformasjon til personvernombudet
- Hvor finnes og sette seg inn i oversikten over behandlinger
- Hvor er og hva sier personvernerklæringen