|  |
| --- |
|  |
| Rutiner for håndtering av personopplysninger<virksomhet> DD. mÅNED 2018 |

Innhold

[1 Innledning 3](#_Toc509496666)

[1.1 Ansvarlig 3](#_Toc509496667)

[2 Rutine for iverksettelse av behandling 3](#_Toc509496668)

[2.1 Risikovurdering/konsekvensanalyse 4](#_Toc509496669)

[2.2 Avklaring om forhåndskonsultasjon 4](#_Toc509496670)

[2.3 Etablere tilfredsstillende tiltak for informasjonssikkerhet 5](#_Toc509496671)

[2.4 Sletterutiner 6](#_Toc509496672)

[3 Rutine ved bruk av databehandler 6](#_Toc509496673)

[4 Rutine for retting av mangelfulle personopplysninger 7](#_Toc509496674)

[5 Rutine for håndtering av innsynsbegjæring 8](#_Toc509496675)

[6 Rutine for utlevering av personopplysninger 9](#_Toc509496676)

[7 Rutine for oppfyllelse av informasjonsplikt 10](#_Toc509496677)

[8 Rutine for avviksbehandling 11](#_Toc509496678)

[8.2 Avviksmelding til Datatilsynet 11](#_Toc509496679)

[8.3 Avviksmelding til den registrerte 12](#_Toc509496680)

[9 Rutine for oppfyllelse av den registrertes rett til dataportabilitet 13](#_Toc509496681)

[10 Rutine for oppfyllelse av retten til å bli slettet 13](#_Toc509496682)

1. Innledning

Dette dokumentet inneholder <virksomhet> Norge AS’ (<virksomhet>) rutiner for håndtering av personopplysninger. Dokumentet skal sikre at virksomheten oppfyller lovpålagte krav knyttet til behandling av personopplysninger.

Rutinene har til formål å påse at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysningene.

Rutinene i dette dokumentet er rettet mot følgende ansatte i virksomheten:

* Enhver medarbeider med ansvar for prosesser hvor personopplysninger skal inngå eller inngår.
* Enhver medarbeider som jobber med en prosess eller et system hvor personopplysninger skal inngå eller inngår.

\*Strykes dersom ikke relevant: Dokumentet gjøres gjeldende for alle selskaper som er en del av <virksomhet>-konsernet, og hvor <virksomhet> har en eierandel på minst 50 % (heretter samlet referert til som <virksomhet>), og alle interne og eksterne ressurser som håndterer personopplysninger på vegne av <virksomhet>.

* 1. Ansvarlig

<sett inn rolle/funksjon> i <virksomhet> er ansvarlig for etablering og oppdatering av dette dokumentet. Kraveier for de ulike behandlingene av personopplysninger er ansvarlig for å påse at rutinene i dette dokumentet følges for den aktuelle behandlingen, med mindre noe annet fremkommer av den aktuelle rutinen.

Alle ansatte i <virksomhet> skal gjøre seg kjent med dette dokumentet og etterleve rutinene etter beste evne.

1. Rutine for iverksettelse av behandling
	* + 1. Formål

Rutinen har til formål å sørge for at <virksomhet> har et gyldig rettslig grunnlag for alle behandlinger av personopplysninger som foretas, og at personopplysningene bare brukes til uttrykkelig angitte formål som er saklig begrunnet i <virksomhet>s virksomhet. Videre skal rutinen sørge for at personopplysningene som behandles skal være tilstrekkelige og relevante for formålet med behandlingen, korrekte og oppdaterte og ikke lagres lenger enn det som er nødvendig ut fra formålet med behandlingen.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 6, jf. artikkel 7 og 9

* + - 1. Hva skal gjøres?

Før oppstart av enhver behandling av personopplysninger skal det foretas en vurdering av om personvernlovgivningen kommer til anvendelse eller ikke.

Dersom det konkluderes med at personvernlovgivningen kommer til anvendelse, skal det avklares og dokumenteres hvorvidt <virksomhet> vil være behandlingsansvarlig eller databehandler. Avklaringen får betydning for virksomhetens rettigheter og plikter, samt utarbeiding av rutiner for den konkrete behandlingen.

Videre skal følgende vurderinger foretas:

* Hva er formålet med behandlingen?
* Hvilket rettslig grunnlag har <virksomhet> for behandlingen?
* Hvilke typer personopplysninger er nødvendige å behandle for å oppnå formålet med behandlingen?

De ovennevnte vurderinger skal dokumenteres i vedlegg 1 til <virksomhet>s styringsdokument for behandling av personopplysninger (Oversikt over behandlinger av personopplysninger i <virksomhet>).

Det skal i tillegg gjennomføres følgende aktiviteter før behandlingen av personopplysninger tar til:

* risikovurdering/konsekvensanalyse
* avklaring om forhåndskonsultasjon
* etablere tilfredsstillende tiltak for informasjonssikkerhet
* utarbeide konkrete slettefrister

I det følgende vil rutinene for disse aktivitetene bli presentert nærmere:

* 1. Risikovurdering/konsekvensanalyse
		+ 1. Formål

Rutinen har til formål å sørge for at <virksomhet> har kartlagt sannsynligheten for og konsekvenser av sikkerhetsbrudd knyttet til behandlingen av personopplysninger. Resultatet av risikovurderingen/konsekvensanalysen vil danne grunnlag for etablering av tilfredsstillende sikkerhetstiltak.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 35

* + - 1. Hva skal gjøres?

Det må avklares hvorvidt det er sannsynlig at behandlingen av personopplysninger kan innebære en høy risiko for at personvernet til den registrerte ikke blir ivaretatt. Dersom så er tilfelle må det gjennomføres en konsekvensanalyse («Data Protection Impact Assessment») for å kartlegge risikoen nærmere.

Konsekvensanalysen skal blant annet vurdere hvilke typer sikkerhetsbrudd som kan inntreffe, hva som eventuelt kan være årsaken til sikkerhetsbruddet, samt hvilken konsekvens sikkerhetsbruddet kan tenkes å ha for den/de registrerte.

Konsekvensanalysen skal som et minimum omfatte:

* En systematisk beskrivelse av de planlagte behandlingsaktiviteter og formålene med behandlingen. Dersom det rettslige grunnlaget for behandling av personopplysninger er at <virksomhet> har en legitim interesse for å gjennomføre behandlingen, skal den legitime interessen beskrives og dokumenteres.
* En vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene.
* En vurdering av risikoene for de registrertes rettigheter og frihetsrettigheter.
* Informasjon om de planlagte sikkerhetstiltakene som skal redusere disse risikoene.
* En vurdering av om hvorvidt det er sannsynlig at behandlingen av personopplysninger kan innebære en høy risiko for personvernet til den registrerte, samt eventuell konsekvensanalyse skal dokumenteres.

Resultatet av konsekvensanalysen skal rapporteres til personvernkoordinator som igjen rapporterer dette til ledelsen.

* 1. Avklaring om forhåndskonsultasjon
		+ 1. Formål

Rutinen har til formål å sørge for at <virksomhet> oppfyller lovbestemte krav til forhåndskonsultasjon hos Datatilsynet.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 36

* + - 1. Hva skal gjøres?

Dersom konsekvensanalysen tilsier at behandlingen av personopplysninger innebærer en uakseptabel risiko for personvernet, selv etter at rimelige sikkerhetstiltak er gjennomført, skal det sendes en skriftlig anmodning til Datatilsynet der det bes om forhåndskonsultasjon. Henvendelsen til Datatilsynet skal blant annet inneholde følgende opplysninger:

* Hvilke selskap i <virksomhet> som er involvert i behandlingen av personopplysninger, og hvem som er å anse som behandlingsansvarlig eller felles behandlingsansvarlige.
* Den planlagte behandlingens formål og hjelpemidler.
* Planlagte sikkerhetstiltak som skal beskytte de registrertes rettigheter og frihetsrettigheter i henhold til GDPR.
* Konsekvensanalysen vedrørende den aktuelle behandlingen.
* Andre opplysninger som Datatilsynet eventuelt ber om.

Dersom Datatilsynet finner at den planlagte behandlingen av personopplysninger vil være i strid med personvernlovgivningen, skal Datatilsynet innen åtte uker etter mottak av anmodning om forhåndskonsultasjon gi skriftlig tilbakemelding til <virksomhet>. I særskilt vanskelig saker kan denne fristen utsettes i seks uker. Datatilsynet skal i slike tilfeller gi tilbakemelding til <virksomhet> om slik utsettelse av frist, senest en måned etter mottak av henvendelsen fra <virksomhet>.

Personvernkoordinator er ansvarlig for å kontakte Datatilsynet for forhåndskonsultasjon.

* 1. Etablere tilfredsstillende tiltak for informasjonssikkerhet
		+ 1. Formål

Rutinen har til formål å påse at <virksomhet> gjennom planlagte og systematiske tiltak sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 24, 25 og 32

* + - 1. Hva skal gjøres?

<virksomhet> skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Dokumentasjonen på de planlagte og systematiske tiltak skal være tilgjengelig for alle ansatte i <virksomhet>, samt Datatilsynet og Personvernnemnda.

Ved vurderingen av hva som er å anse som tilfredsstillende informasjonssikkerhet skal det legges vekt på den risiko som den aktuelle behandlingen utgjør, herunder dersom opplysningene ved hendelig uhell eller bevisst handling bli slettet/mistet, endret, utlevert til utenforstående, ulovlig lagret eller på annen måte behandlet i strid med lovverket.

IKT-ansvarlig er ansvarlig for å utarbeide en beskrivelse av informasjonssystemene som benyttes til behandling av personopplysninger, samt en overordnet IT-beredskapsplan.

* + - 1. Særlig om innebygget personvern

Innebygget personvern innebærer at <virksomhet> skal ta hensyn til personvern allerede ved utarbeidelsen og implementering av eventuelle nye behandlinger av personopplysninger, eller ved innføring av nye informasjonssystemer.

<virksomhet> skal treffe passende tekniske og organisatoriske sikkerhetstiltak, som for eksempel pseudonymisering, for å sørge for tilfredsstillende informasjonssikkerhet. Ved vurdering av innebygd personvern, skal det legges vekt på den aktuelle tekniske utvikling, implementeringsomkostninger og den pågående behandlingens karakter, omfang, sammenheng og formål, samt konsekvens av potensielle sikkerhetsbrudd for personers rettigheter og frihet, som behandlingen innebærer.

Sikkerhetstiltakene skal være utformet med henblikk på effektiv implementering av personvernprinsippene, for å oppfylle kravene i GDPR og beskytte de registrertes rettigheter.

Dersom det er mulig skal standardinnstillingene for <virksomhet>s informasjonssystemer stilles inn slik at kun personopplysninger som er nødvendige for å oppfylle hvert enkelt formål med behandlingen, behandles. Med dette menes at systemenes standardinnstillinger så langt det er mulig skal sørge for <virksomhet> ikke behandler flere opplysninger enn det som er nødvendig, at personopplysningene ikke behandles lengre enn det som er nødvendig, samt at personopplysningene ikke er tilgjengelige for flere personer enn de som har saklig og faglig behov for å ha slik tilgang.

Disse sikkerhetstiltakene skal særlig sørge for at standardinnstillingene i informasjonssystemet sikrer at personopplysninger ikke gjøres tilgjengelig for et ubegrenset antall personer uten en persons handling.

Personvernkoordinator i <virksomhet> skal, sammen med IKT-ansvarlig identifisere sikkerhetstiltak for de ulike behandlingene av personopplysninger i <virksomhet>, herunder IT-systemer. Sikkerhetstiltakene skal ta utgangspunkt i resultatet fra risikovurderingen/ konsekvensanalysen og skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

Tiltakene skal dokumenteres.

* 1. Sletterutiner
		+ 1. Formål

Rutinen har til formål å påse at <virksomhet> ikke lagrer personopplysninger lenger enn det som nødvendig ut fra formålet med behandlingen, eller som det foreligger lovbestemt oppbevaringsplikt for.

* + - 1. Bakgrunn for rutinene:

GDPR artikkel 24

* + - 1. Hva skal gjøres?

Sletting av personopplysninger skal gjennomføres så snart formålet med behandlingen er oppnådd, forutsatt at det ikke er andre regler som begrenser adgang til å slette personopplysninger, herunder regnskapsloven, bokføringsloven e.l.

Før hver behandling av personopplysninger tiltar skal det, så langt det er praktisk mulig, tas stilling til om det foreligger lovregler som fastsetter hvor lenge personopplysningene skal lagres, samt hvor lenge det er nødvendig å oppbevare personopplysningene for å oppfylle det aktuelle formålet. Dersom ikke annet er bestemt, fastsettes slettefrist med bakgrunn i hva <virksomhet> anser som nødvendig lagringstid. Slettefristene må fremstå som proporsjonale etter en vurdering av <virksomhet>s behov for opplysningene opp mot den personverninngripen lagring av opplysningene utgjør for den registrerte.

De aktuelle lagringsfristene skal dokumenteres.

Kraveier er ansvarlig for å påse at personopplysningene slettes fortløpende i henhold til de fastsatte fristene. Personvernkoordinator skal årlig be om bekreftelse fra kraveier på at personopplysningene er slettet i henhold til denne rutinen.

Så langt det er mulig skal det innstilles på automatisk sletting til forhåndsbestemte tidspunkt i det informasjonssystemet som benyttes til den aktuelle behandlingen. Dersom slettingen skjer automatisk, skal det påses at det ikke arkiveres kopier av slettet informasjon. Sletting kan også skje ved destruksjon av det lagringsmedium som personopplysningene oppbevares på.

Anonymisering av personopplysningene kan være et alternativ til sletting. Anonymiseringen må være reell. Dette innebærer at når anonymiseringsprosessen er gjennomført skal det ikke være mulig å gjenfinne koblingen mellom person og informasjonen, når man tar i betraktning de hjelpemidlene som med rimelighet kan tenkes brukt for å identifisere vedkommende.

1. Rutine ved bruk av databehandler
	* + 1. Formål

Denne rutinen kommer til anvendelse når virksomheten setter ut behandling av personopplysninger til eksterne (databehandlere). Med databehandler menes «en som behandler personopplysninger på vegne av den behandlingsansvarlige», eksempelvis, ekstern tjenesteleverandør av IT-systemer, rekrutteringsbyrå o.l.

Rutinen har til formål å sørge for at <virksomhet> ikke overlater personopplysninger til andre (databehandler) for lagring eller bearbeiding uten at det er inngått en databehandleravtale som regulerer hvordan databehandler skal behandle personopplysningene. Rutinen skal også sørge for at <virksomhet> ikke selv behandler personopplysninger på vegne av andre uten at det er inngått slik databehandleravtale.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 28, 29 og 32

* + - 1. Hva skal gjøres?

Dersom <virksomhet> bruker en underleverandør som skal behandle personopplysninger på vegne av <virksomhet>, eller dersom <virksomhet> skal behandle personopplysninger på vegne av et annet selskap, skal det inngås en databehandleravtale som regulerer den aktuelle behandlingen av personopplysninger.

Databehandleravtalen skal fortrinnsvis være en selvstendig og uttømmende avtale som benevnes «databehandleravtale». Databehandleravtalen kan også være et vedlegg til en tjenesteavtale inngått mellom de samme parter. Følgende opplysninger skal som et absolutt minimum fremgå av databehandleravtalen:

* Formålet med behandlingen av personopplysningene.
* Hva databehandler skal gjøre med opplysningene.
* Det skal fremgå av avtalen at databehandler kun skal behandle opplysningene i henhold til formålet <virksomhet> har definert.
* Databehandlers eventuelle bruk av underleverandører av tjenester skal klart framgå.
	+ <virksomhet> skal godkjenne alle eventuelle underleverandører.
* Hvordan den registrertes rettigheter skal ivaretas.
	+ Avtalen bør regulere hvem som eventuelt skal besvare henvendelser om innsyn og retting/sletting.
* Databehandleren pålegges å ha tilfredsstillende informasjonssikkerhet.
	+ Avtalen må klargjøre hva databehandler skal ha på plass av sikringstiltak for å ivareta konfidensialitet, integritet og tilgjengelighet for behandling av personopplysninger.
* Avtalens varighet.
* Hva som skal skje med opplysningene etter at avtalen er opphørt.
	+ Skal personopplysningene tilbakeføres eller slettes?
* <virksomhet>s rett til å foreta sikkerhetsrevisjoner.
* Hvor ofte det skal foretas sikkerhetsrevisjon.

IKT-ansvarlig skal involveres dersom avtalene gjelder drift eller vedlikehold av informasjonssystemer.

Kraveier plikter å påse at databehandleravtaler inngås før personopplysninger utleveres, og at virksomheten til enhver tid har nødvendige databehandleravtaler.

Personvernkoordinator skal bistå kraveier ved behov.

1. Rutine for retting av mangelfulle personopplysninger
	* + 1. Formål

Denne rutinen har til formål å påse at <virksomhet> ikke behandler personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 16

* + - 1. Hva skal gjøres?

Dersom en gjennomgang viser at det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal virksomheten rette de mangelfulle opplysningene. På begjæring fra en som er registrert skal også personopplysningene rettes eller slettes.

Begjæring om retting av personopplysninger fra en som er registrert skal straks videreformidles til personvernkoordinator. Personvernkoordinator skal videre påse at <virksomhet> retter de mangelfulle opplysningene, men den praktiske oppfølgingen kan delegeres. <virksomhet> skal om mulig sørge for at feilen ikke får betydning for den registrerte, f.eks. ved å varsle mottakere av utleverte opplysninger.

Retting av uriktige eller ufullstendige personopplysninger som kan ha betydning som dokumentasjon, skal skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger. Den registrerte har også, dersom ønskelig, rett til å fremlegge en supplerende erklæring med informasjon som han/hun mener er nødvendig.

Retting eller sletting foretas uten unødig opphold og senest innen tre dager fra <virksomhet> mottok begjæringen, eller fra det tidspunkt <virksomhet> ble oppmerksom på de mangelfulle personopplysningene.

1. Rutine for håndtering av innsynsbegjæring
	* + 1. Formål

Denne rutinen har til formål å sørge for at enkeltpersoner får innsyn i hvilke personopplysninger <virksomhet> behandler, og at registrerte får innsyn i de opplysninger som er registrert om seg.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 15

* + - 1. Hva skal gjøres?

En som er registrert i <virksomhet>s registre har rett til å få bekreftet om <virksomhet> behandler personopplysninger om han/henne, og dersom så er tilfelle, få adgang til opplysningene og videre følgende informasjon:

* Formålet med behandlingen.
* Hvilke kategorier av personopplysninger som behandles.
* Eventuelle mottagere eller kategorier av mottagere som personopplysningene eventuelt vil bli utlevert til.
* Om mulig, hvor lenge personopplysningene vil bli lagret, eller dersom dette ikke er mulig, hvilke kriterier som legges til grunn for å fastslå lagringstid.
* Retten til å anmode <virksomhet> om retting/sletting av personopplysninger, eller å kreve begrensning av behandling av personopplysninger om den registrerte eller retten til å bestride denne behandlingen.
* Retten til å rette en klage til Datatilsynet.
* Enhver tilgjengelig informasjon om hvor personopplysningene blir innhentet fra dersom personopplysningene ikke samles inn fra den registrerte.
* Eventuell bruk av automatiserte avgjørelser, herunder profilering inkl. informasjon om logikken som ligger bak slik profilering, og de forventede konsekvenser dette vil ha for den registrerte.
* Hvilke sikkerhetstiltak som ligger til grunn for overføring av personopplysningene til tredjeland (land utenfor EU), dersom dette er aktuelt.

<virksomhet> skal utlevere en kopi av de personopplysninger som behandles om den som ber om innsyn. For ytterligere kopier som den registrerte anmoder om kan <virksomhet> kreve et rimelig gebyr basert på de administrative omkostningene. Hvis den registrerte sender anmodningen om innsyn elektronisk, og med mindre den registrerte ber om noe annet, skal personopplysningene utleveres i en alminnelig brukt elektronisk form.

Retten til å motta en kopi av personopplysningene som behandles må ikke krenke andres personvern eller rettigheter.

Før det gis innsyn skal den registrerte levere inn en skriftlig og undertegnet begjæring. Av hensyn til konfidensialitet, må den registrerte også inngi en bekreftet kopi av legitimasjon.

Den som mottar en begjæring om innsyn skal varsle <virksomhet>s personvernkoordinator umiddelbart og senest innen 24 timer. Personvernkoordinator er ansvarlig for at informasjon sendes skriftlig til den registrerte, men den praktiske gjennomføringen kan delegeres videre.

Hvis informasjonen skal sendes elektronisk, for eksempel ved bruk av e-post, må informasjonen sikres, for eksempel ved bruk av kryptert e-post.

Postsendinger som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten.

Det skal ikke kreves betaling for å utgi informasjon etter begjæring om innsyn, med unntak av eventuelle ekstra kopier av personopplysninger som behandles som nevnt ovenfor.

* + - 1. Når innsyn skal gis

<virksomhet> skal besvare henvendelser om innsyn uten ugrunnet opphold og senest innen 30 dager fra den dagen henvendelsen kom inn.

Dersom særlige forhold gjør det umulig å svare på henvendelsen innen 30 dager, kan gjennomføringen utsettes inntil det er mulig å gi svar. Den registrerte må i så fall gis et foreløpig svar med opplysninger om årsaken til forsinkelsen og sannsynlig tidspunkt for når svar kan gis.

1. Rutine for utlevering av personopplysninger
	* + 1. Formål

Personopplysninger kan bare utleveres dersom det foreligger et rettslig grunnlag eller en rettslig kjennelse for slik utlevering. Med utlevering menes oversendelse av personopplysninger til en tredjepart som vil være ansvarlig for videre bruk av personopplysningene. Oversendelse av personopplysninger til en databehandler som skal behandle personopplysningene på vegne av <virksomhet> regnes ikke som en utlevering.

Utlevering av personopplysninger regnes som en behandling av personopplysninger og det må derfor foreligge rettslig grunnlag. Rettslig grunnlag kan enten være samtykke fra den som opplysningene gjelder, at utlevering er nødvendig for å oppfylle en avtale som et selskap har med denne personen, eller at det er fastsatt i lov at slik utlevering er tillatt, eller at utlevering er nødvendig for at <virksomhet> eller tredjepersoner som opplysningene utleveres til kan ivareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Denne rutinen har til formål å sørge for at <virksomhet> ikke utleverer personopplysninger uten at det foreligger et gyldig rettslig grunnlag slik behandling av personopplysninger.

* + - 1. Bakgrunn for rutine

GDPR artikkel 7

* + - 1. Hva skal gjøres?

Dersom <virksomhet> mottar henvendelser fra politiet, revisor, skattemyndighetene, bostyrere, forsikringsselskap eller andre tredjeparter som ønsker å få utlevert personopplysninger, herunder materiale fra overvåkningskamera, adgangskontrollsystem o.l. skal personvernkoordinator kontaktes umiddelbart, og senest innen 24 timer.

Personvernkoordinator skal deretter påse at det foreligger rettslig grunnlag for utlevering av personopplysninger. Personvernkoordinator er ansvarlig for å vurdere om <virksomhet> har rettslig grunnlag for å utlevere personopplysningene. Om nødvendig kan personvernkoordinator be om bistand fra juridisk enhet.

Forespørsel om utlevering av personopplysninger skal være skriftlig og alltid inneholde henvisning til rettslig grunnlag, eller rettslig kjennelse.

Det skal foreligge signatur fra den som ber om utlevering på at det som forespørres har gyldig rettslig grunnlag og at eventuell rettslig kjennelse foreligger dersom dette er relevant.

1. Rutine for oppfyllelse av informasjonsplikt
	* + 1. Formål

Denne rutinen har til formål å sørge for at <virksomhet> oppfyller lovpålagt informasjonsplikt til de som er registrert i <virksomhet>s systemer.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 13 og 14

* + - 1. Hva skal gjøres?

Når det samles inn personopplysninger fra den registrerte selv, skal <virksomhet> på eget initiativ først informere den registrerte om følgende:

* Navn og adresse på den behandlingsansvarlige.
* Formålet med behandlingen.
* Rettslig grunnlag for behandlingen.
	+ Dersom det rettslige grunnlaget er basert på at behandlingen er nødvendig for at <virksomhet> skal kunne ivareta en berettiget interesse, skal denne interessen beskrives.
* Eventuelle mottagere eller kategorier av mottagere som personopplysningene eventuelt vil bli utlevert til.
* Om mulig, hvor lenge personopplysningene vil bli lagret, eller dersom dette ikke er mulig, hvilke kriterier som legges til grunn for å fastslå lagringstid.
* Dersom <virksomhet> vil overføre personopplysninger til et tredjeland (land utenfor EU) eller til en internasjonal organisasjon; henvisning til hvorvidt EU kommisjonen har besluttet at landet personopplysningene skal utleveres til, har et tilfredsstillende beskyttelsesnivå, eller eventuell henvisning til tilfredsstillende sikkerhetstiltak. Det skal også opplyses om hvordan den registrerte kan få informasjon om disse sikkerhetstiltakene.
* Retten til å be om innsikt, retting og/eller sletting av personopplysninger eller begrensning av behandlingen av personopplysninger, eller til å rette en innvending mot behandlingen.
* Retten til dataportabilitet.
* Retten til å rette en klage til Datatilsynet.
* Retten til å trekke samtykket tilbake, dersom behandlingen er basert på samtykke fra den registrerte.
* Om meddelelse av personopplysninger er lovpålagt eller et krav i henhold til en kontrakt eller et krav som må være oppfylt for å inngå en kontrakt, samt om den registrerte har plikt til å gi opplysningene og de eventuelle konsekvensene av å ikke gi disse opplysningene.
* Eventuell forekomst av automatiserte avgjørelser, herunder profilering, og som et minimum meningsfulle opplysninger om logikken som benyttes i denne behandlingen, og de forventede konsekvenser av denne behandlingen for de registrerte.

Hvis <virksomhet> skal bruke personopplysningene for et annet formål enn de opprinnelig var innsamlet for, skal <virksomhet>, før den nye behandlingen tar til, gi den registrerte opplysninger om det nye formålet, samt eventuelle andre relevante opplysninger.

De ovennevnte krav til informasjon som skal gis den registrerte gjelder ikke i den utstrekning den registrerte allerede kjenner til denne informasjonen.

* + - 1. Når skal opplysningene gis?

Dersom personopplysningene innsamles fra den registrerte skal <virksomhet> gi nødvendig informasjon på det tidspunkt opplysningene samles inn.

1. Rutine for avviksbehandling
	* + 1. Formål

Rutiner for rapportering av hendelser og håndtering av avvik skal sikre læring og kontinuerlig forbedring i internkontrollen samt at eventuelle sikkerhetsbrudd rapporteres til ansvarlig person.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 33 og 34

* + - 1. Hva skal gjøres?

Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på informasjonssikkerhet, skal dette behandles som et avvik.

Alle ansatte er ansvarlig for å rapportere avvik fra gjeldende rutiner og andre hendelser til den som er ansvarlig for det aktuelle området eller sikkerhetsansvarlig. Feil i programvare og maskinvare rapporteres til IKT-ansvarlig.

Sikkerhetshendelser og beredskapshendelser krever ofte en rask reaksjon og må rapporteres omgående, muntlig eller helst gjennom e-post.

Avviket skal registreres, og på en slik måtte at det er enkelt å få oversikt over status på avvik og korrigerende tiltak. Personvernkoordinator er ansvarlig for å påse at avviket håndteres, men den praktiske oppfølgingen av dette kan delegeres.

Dersom det avdekkes tegn på bevisste sikkerhetsbrudd fra ansatte skal personvernkoordinator varsle personalansvarlig og disse skal sammen avgjøre tiltak.

Brudd på den generelle taushetsplikten fra ansatte eller tidligere ansatte skal rapporteres til personalansvarlig som vurderer hvilke tiltak som skal iverksettes.

Personvernkoordinator er ansvarlig for å vedlikeholde og ajourføre avvikslisten for <virksomhet>. Avvikslisten skal holdes løpende oppdatert og kan inneholde:

* Dato
* Beskrivelse
* Kilde
* Avdeling/systemområde
* Alvorlighet
* Status
* Ansvarlig for oppfølging
* Frist for neste oppfølgingspunkt
* Kommentar/korrektivt tiltak
	1. Avviksmelding til Datatilsynet
		+ 1. Hva er en uautorisert utlevering?

Med «uautorisert utlevering av personopplysninger» menes når personopplysninger befinner seg utenfor den behandlingsansvarliges kontroll, og personer som ikke er godkjent for tilgang til personopplysningene kan ha fått tilgang. En utlevering kan være tilsiktet eller utilsiktet. Det har skjedd en utlevering selv om det er usikkert om noen har fått personopplysningene i hende.

Eksempler på uautorisert utlevering er:

* Forsendelsesfeil:
	+ Personopplysninger er sendt til feil mottaker pr. post eller e-post.
	+ Digitale forsendelser som avslører andres e-postadresse i en kontekst hvor mottakerne skal beskyttes.
	+ Forsendelser til riktig mottaker, men som ved en feil også inneholder personopplysninger om andre.
	+ Postforsendelser til riktig mottaker, men hvor det er informasjon om mottakeren som skal skjermes for andre, som er synlig utenpå forsendelsen. Eksempler på dette er synlig fødselsnummer på en konvolutt.
	+ Postforsendelser hvor innholdet mangler eller innholdet er der, men konvolutten er revet opp.
* Hacking / datainnbrudd, hvor personopplysninger har blitt hentet ut eller det er sannsynlig at dette har skjedd.
* Snoking gjennomført av egne ansatte. Dette er en utlevering fordi ansatte har ervervet opplysningene til sine private formål, og arbeidsgiver har derfor tapt kontrollen med opplysningene.
* Tilgangsstyring feilet, er mangelfull eller manglende, slik at uvedkommende fra utsiden av virksomheten har fått tilgang til beskyttelsesverdige personopplysninger.
* Nettpublisering av personopplysninger som ikke skulle ha vært publisert, eller at personopplysningene ikke har blitt anonymisert.
* Fysisk innbrudd hvor digitale data eller papirdokumenter med personopplysninger er forsvunnet.
* Avhending uten sletting eller makulering.
* Mistet/gjenglemt/forlagt:
	+ Papirdokumenter.
	+ Laptop, nettbrett eller telefoner der innholdet ikke er kryptert.
	+ Minnepinner eller andre små lagringsmedier der innholdet ikke er kryptert.
		- 1. Hvilke personopplysninger gjelder det?

Med «personopplysninger hvor konfidensialitet er nødvendig» menes blant annet:

* Sensitive personopplysninger.
* Fødselsnummer.
* Taushetsbelagte personopplysninger.
* Personopplysninger som etter sin mengde og art er følsomme.
* Opplysninger som en virksomhet anser som konfidensielle i forholdet mellom seg og kundene. For eksempel saldo på konti eller hva en person har kjøpt i en nettbutikk.
	+ - 1. Hva skal gjøres?

Med mindre det er usannsynlig at avviket innebærer en risiko for personers rettigheter og frihet, skal avvik meldes til Datatilsynet uten unødig forsinkelse, og dersom mulig, senest 72 timer etter at <virksomhet> ble kjent med avviket.

Dersom avviket ikke meldes innen 72 timer skal det foreligge en skriftlig begrunnelse for forsinkelsen. Avviksmeldingen til Datatilsynet skal inneholde følgende informasjon:

* Beskrivelse av sikkerhetsbruddet, herunder hvis det er mulig, kategoriene og det omtrentlige antall berørte registreringer av personopplysninger.
* Navn og kontaktinformasjon på <virksomhet>s kontaktperson.
* Beskrivelse av de sannsynlige konsekvenser av sikkerhetsbruddet for personvernet.
* Beskrivelse av de tiltak som <virksomhet> har truffet eller som foreslås truffet for å håndtere avviket, herunder, om relevant, tiltak for å begrense mulige skadevirkninger.

Dersom det ikke er mulig å gi ovennevnte opplysninger samlet, kan informasjonen gis trinnvis uten unødig ytterligere forsinkelse.

<virksomhet> skal dokumentere alle avvik, herunder de faktiske omstendigheter ved bruddet på personvernet, dets virkninger og gjennomførte avhjelpende tiltak. Denne dokumentasjonen skal sette Datatilsynet i stand til å kontrollere at forordningens bestemmelser om avviksbehandling er fulgt.

* 1. Avviksmelding til den registrerte

Dersom det er sannsynlig at avviket vil innebære en høy risiko for personers rettigheter, skal <virksomhet> uten unødig forsinkelse varsle den registrerte om avviket.

Varselet skal i et klart og forståelig språk beskrive sikkerhetsbruddet og som et minimum inneholde følgende informasjon:

* Navn og kontaktinformasjon på <virksomhet>s kontaktperson.
* Beskrivelse av de sannsynlige konsekvenser av sikkerhetsbruddet for personvernet.
* Beskrivelse av de tiltak som <virksomhet> har truffet, eller som foreslås truffet, for å håndtere avviket, herunder, om relevant, tiltak for å begrense mulige skadevirkninger.

Det er ikke nødvendig å varsle den registrerte dersom en av følgende betingelser er oppfylt:

* <virksomhet> har implementert tilfredsstillende tekniske og organisatoriske sikkerhetstiltak, og disse er benyttet på de personopplysninger som er berørt av avviket. Dette gjelder særskilt sikkerhetstiltak, eksempelvis kryptering, som gjør personopplysningene uleselige for alle som ikke har autorisert adgang til disse.
* <virksomhet> har implementert etterfølgende sikkerhetstiltak som sikrer at den høye risikoen for den registrertes rettigheter og frihetsrettigheter ikke lengre er reell.
* Det vil kreve en uforholdsmessig innsats. I slike tilfeller skal <virksomhet> i stedet publisere en offentlig meddelelse eller tilsvarende som sikrer at de registrerte kan bli informert på en effektiv måte.
1. Rutine for oppfyllelse av den registrertes rett til dataportabilitet
	* + 1. Formål

Formålet er å sørge for at <virksomhet> etterlever kravet om å sørge for dataportabilitet.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 20

* + - 1. Hva skal gjøres?

Dersom det rettslige grunnlaget for <virksomhet> behandling av personopplysninger er samtykke eller oppfyllelse av en kontrakt med den registrerte, har den registrerte rett til å motta personopplysningene som de selv har gitt til <virksomhet> på et strukturert og maskinlesbart format. Den registrerte har videre rett til å overføre disse personopplysningene til en annen behandlingsansvarlig uten hindring fra <virksomhet>.

Når den registrerte utøver sin rett til dataportabilitet, har den registrerte rett til å få overført personopplysningene direkte fra <virksomhet> til en annen behandlingsansvarlig hvis det er teknisk mulig.

Retten til dataportabilitet må ikke krenke andres rettigheter eller frihetsrettigheter.

Dersom <virksomhet> mottar en henvendelse fra en registrert som vil utøve sin rett til dataportabilitet, skal personvernkoordinator kontaktes umiddelbart. Personvernkoordinator er ansvarlig for å påse at den registrerte mottar opplysninger som nevnt ovenfor, men den praktiske oppfølgingen kan delegeres til andre.

1. Rutine for oppfyllelse av retten til å bli slettet
	* + 1. Formål

Formålet er å sørge for at <virksomhet> etterlever anmodninger fra den registrerte om sletting av personopplysninger om seg selv.

* + - 1. Bakgrunn for rutinen

GDPR artikkel 17

* + - 1. Hva skal gjøres?

Den registrerte har rett til å få personopplysninger om seg selv slettet av <virksomhet> uten unødig forsinkelse dersom en av følgende betingelser er oppfylt:

* Personopplysningene er ikke lengre nødvendige for å oppfylle formålet for behandlingen.
* Den registrerte trekker tilbake samtykket, i de tilfeller der samtykke fra den registrerte er det rettslige grunnlaget for behandlingen.
* Den registrerte har innsigelse mot behandlingen og det ikke foreligger legitime grunner for behandlingen som overstiger innsigelsen.
* Dersom formålet med behandlingen er direkte markedsføring eller profilering, og den registrerte har innsigelse mot behandlingen.
* Personopplysningene har blitt behandlet ulovlig.
* Personopplysningene skal slettes for å overholde en rettslig forpliktelse i EU-retten eller norsk rett.
* Personopplysningene er blitt innsamlet fra sosiale medier.

<virksomhet> er ikke pålagt å slette personopplysninger i den grad behandlingen av personopplysninger er nødvendig:

* For å utøve retten til ytrings- og informasjonsfrihet.
* For at et rettskrav kan fastsettes, gjøres gjeldende eller forsvares.

Personvernkoordinator er ansvarlig for å påse at de aktuelle personopplysninger slettes som nevnt i denne rutinen, men den praktiske oppfølgingen kan delegeres.