



# Det frivillige Skyttervesen

## Del 2

### Retningslinjer for behandling av personopplysninger og informasjonssikkerhet i Det frivillige Skyttervesen

Etablert:	23/4-2018: Norges Skytterstyre sak 60-2018
Revisjon 1:	10/5-2019

## Innhold

DEL I:	INNLEDNING .....	4
1.	OM RETNINGSLINJENE.....	4
1.1.	Bakgrunn .....	4
1.2.	Definisjoner .....	5
1.3.	Lovgrunnlag .....	5
1.4.	Formål .....	5
1.6.	Virkeområde – hva retningslinjene regulerer .....	5
1.7.	Juridisk bindende vedavtale .....	7
DEL II:	ARBEIDET MED PERSONVERN OG INFORMASJONSSIKKERHET .....	8
2.	Oversikt .....	8
2.2.	Oversikt over oppgaver som omfattes av det daglige ansvaret for informasjonssikkerhet.....	8
DEL III:	STYRENDE DEL .....	9
3.	Styringssystem for personvern og informasjonssikkerhet .....	9
3.1.	Sikkerhetsmål.....	9
3.2.	Formål .....	9
3.3.	Overordnede føringer for organisasjonsleddets bruk av informasjonsteknologi	9
3.4.	Sentrale sikkerhetsformål.....	9
3.5.	Nivå for akseptabel risiko.....	10
3.5.1.	Konfidensialitet .....	10
3.5.2.	Integritet .....	10
3.5.3.	Tilgjengelighet .....	10
3.6.	Oversikt over behandlinger av personopplysninger .....	11
3.7.	Risikovurderinger .....	11
DEL IV:	GJENNOMFØRENDE DEL.....	13
4.	Ansvarliggjøring – taushetsplikt .....	13
4.1.	Tilgangsstyring .....	13
4.1.1.	Autentisering.....	13
4.1.2.	Autorisering.....	14
4.1.3.	Tilgang .....	14
4.1.4.	Utlevering av personopplysninger til andre land .....	14
4.1.5.	Kontrollerende tiltak .....	15
4.2.	Behandling av personopplysninger .....	15
4.2.1.	Prosedyre for bruk av informasjonssystemet .....	15
4.2.2.	Kontroll av tilgangsstyring .....	15
4.2.3.	Informasjon og samtykke .....	15
4.3.	Etablering og drift av informasjonssystemet .....	16
4.3.1.	Konfigurasjonskontroll .....	16
4.3.2.	Konfidensialitet og integritet .....	16
4.4.	Opplæring og kompetanse.....	17
4.5.	Datakommunikasjon.....	17
4.5.1.	Meldingsformidling og e-post med sensitive personopplysninger .....	17
4.5.2.	Kommunikasjon med personer.....	17
4.6.	Avtaler .....	17
4.6.1.	Databehandler .....	18

4.6.2.	Eksterne parter .....	18
DEL VI:	KONTROLLERENDE DEL .....	19
5.	Oppfølgingsansvar .....	19
5.1.	Sikkerhetsrevisjon .....	19
5.2.	Risikovurdering .....	19
5.3.	Avvikshåndtering .....	19
5.4.	Ledelsens gjennomgang .....	20
5.5.	Kontroll av tilganger .....	20

**Som del av retningslinjene inngår følgende:**

Vedlegg 1: Definisjoner, ord og uttrykk

Vedlegg 2: Krav til personvernerklæring i skyttersamlag og skytterlag, maler

Vedlegg 3: Kort beskrivelse av hvilke krav for behandling av personopplysninger som følger av personopplysningsloven med forskrifter

# DEL I: INNLEDNING

## 1. OM RETNINGSLINJENE

### 1.1. Bakgrunn

Det frivillige Skyttervesen (DFS) er forpliktet til å behandle personopplysninger fra sine medlemmer og brukere på en forsvarlig måte. Her kan du lese om hvordan vi samler inn, benytter og beskytter informasjon om våre medlemmer og andre brukere av dfs.no (med tilhørende nettsteder), og DFS' øvrige digitale kanaler og tjenester.

Når du melder deg inn i et skytterlag som er tilknyttet DFS blir du registrert i DFS' sentrale medlemsregister. Du får en egen SkytterID, og kan redigere personopplysninger om deg selv i «Mitt DFS». Disse opplysningene brukes for eksempel når du melder deg på et stevne eller annen aktivitet i DFS. DFS er forpliktet til å behandle personopplysninger fra sine medlemmer og brukere på en forsvarlig måte, i samsvar med personopplysningsloven.

DFS kan bruke dine personopplysninger til å kommunisere med deg vedrørende ditt medlemskap eller din bruk av DFS' tilbud og tjenester. DFS kan bruke personopplysninger til utsending av informasjon fra samarbeidspartnere, for eksempel tilbud på utvalgte medlemsfordeler. DFS forplikter seg til ikke å videreformidle personlige opplysninger til andre enn våre egne organisasjonsledd (samlag og skytterlag). Personopplysninger kan bare formidles til samarbeidspartnere etter eget samtykke.

De senere årene er det gjennom krav fra offentlig myndighet blitt stilt strengere krav til behandling av personopplysninger. Dette gjelder både i privat og offentlig virksomhet, samt i en viss utstrekning for frivillige organisasjoner som DFS. Økt bruk av data til registrering av medlemsrelaterte opplysninger, gir således større krav til personvern også innenfor DFS. Dette gjelder både i skytterlag, samlag og sentralt i DFS.

Med utgangspunkt i de personvernregler som siden 2005 har vært gjeldende i Norge, samt på grunnlag av den nye personopplysningsloven som trer i kraft 25. mai 2018, har Norges Skytterstyre vedtatt nye retningslinjer for personvern og databehandling i DFS.

Disse retningslinjene inneholder svært omfattende krav til rutiner for behandling av registrerte personopplysninger – krav som først og fremst er relevante for DFS sentralt og samarbeidende aktører. Samtidig vil en del av personvernlovgivningen også gjelde for skytterlag og samlag, og denne veilederen inneholder informasjon om de viktigste krav som følger av disse reglene.

Personvernlovgivningen stiller krav til personvern og informasjonssikkerhet. Disse kravene gjelder uavhengig av retningslinjene, og tilsynsmyndigheter (normalt Datatilsynet) kan kontrollere det enkelte organisasjonsledds etterlevelse av gjeldende lovgivning.

Det understrekes at opplæring og bevisstgjøring er av vesentlig betydning for å sikre forsvarlig håndtering av personopplysninger i det daglige arbeidet.

DFS har utarbeidet en veiledning til samlag og skytterlag, med maler for personvernerklæring.

## 1.2. Definisjoner

Definisjoner brukt i Retningslinjene er nærmere gitt i vedlegg 1. Det kan ikke utledes rettigheter eller plikter av definisjonene alene. De må leses i den sammenheng de benyttes i Retningslinjene.

## 1.3. Lovgrunnlag

Retningslinjene er basert på personvernlovgivningens krav til å etablere tilfredsstillende personvern og informasjonssikkerhet for systemer inneholdende personopplysninger, jf. Personopplysningsloven.

Retningslinjene anses av DFS å være i samsvar med gjeldende bestemmelser som omhandler behandling av personopplysninger. Dette gjelder blant annet bestemmelser om taushetsplikt, opplysningsplikt, dokumentasjonsplikt, innsynsrett mv. Videre omfattes også bestemmelser som pålegger organisasjonsledd å etablere systemer som sikrer at en person kan ivareta sine plikter, herunder taushetsplikt. Alle organisasjonsledd i organisasjonen har likevel et selvstendig ansvar for å ivareta kravene til informasjonssikkerhet og personvern som følger av lovverket.

Ved eventuell motstrid mellom retningslinjene og lover eller forskrifter, skal lov og forskrift gå foran retningslinjene.

## 1.4. Formål

Formålet med Retningslinjene er at et organisasjonsledd som

1. etterlever og innretter seg etter Retningslinjene har tilfredsstillende personvern og informasjonssikkerhet for sin behandling av personopplysninger, og
2. samhandler med en ekstern part som har forpliktet seg til å innrette seg etter Retningslinjenes krav, skal kunne stole på at den eksterne parten har tilfredsstillende personvern og informasjonssikkerhet for sin behandling av personopplysninger.

## 1.5. Virkeområde – hvem retningslinjene gjelder for

Disse Retningslinjene gjelder primært for DFS sentralt, samt eksterne parter og andre som behandler personopplysninger og som ved avtale har forpliktet seg til å følge Retningslinjene.

## 1.6. Virkeområde – hva retningslinjene regulerer

Medlemskap i skytterlag, med tilhørende rettigheter og plikter, innebærer at organisasjonsleddene må behandle personopplysninger i ulike sammenhenger som ved administrasjon av aktivitet, personer, forsikringer, kurs og kompetanse, rapportering til offentlige myndigheter med mer. Når en person melder seg inn i et skytterlag inngås det en medlemsavtale mellom personen og organisasjonen. Gjennom medlemsavtalen aksepterer medlemmet organisasjonens regler og bestemmelser iht. Skytterboka. Dette innebærer at organisasjonen har rett til å behandle personopplysninger som lagres i det sentrale medlemssystemet (Mitt DFS), og rett til å kommunisere elektronisk med medlemmer når e-post adresse og/eller mobilnummer er registrert på medlemmet.

DFS sentralt sørger for at alle opplysninger som lagres i Mitt DFS håndteres i samsvar med gjeldende personopplysningslov.

For behandling av personopplysninger som ikke følger av medlemsavtalen må det aktuelle organisasjonsleddet sørge for å innhente nødvendig samtykke dersom ikke annet behandlingsgrunnlag foreligger.

For behandling av personopplysninger som ikke følger av medlemsavtalen må det aktuelle organisasjonsleddet sørge for å innhente nødvendig samtykke dersom ikke annet behandlingsgrunnlag foreligger.

For barn under 15 år skal foresatte samtykke til innmelding, gjennom eget manuelt eller elektronisk innmeldingsskjema.

Retningslinjene stiller krav som supplerer lovverket og gir støtte til hvordan en skal møte lovens krav. Retningslinjene er bindende for hele organisasjonen. Oppfylles disse kravene, er det organisasjonens oppfatning at regelverket vedrørende tilfredsstillende personvern og informasjonssikkerhet oppfylles. Alle organisasjonsledd i organisasjonen har likevel et selvstendig ansvar for å ivareta kravene til informasjonssikkerhet og personvern som følger av lovverket.

Retningslinjene, og de kravene retningslinjene inneholder, blir juridisk bindende ved avtale med tredjepart i den grad innholdet ikke allerede fremgår av lov eller forskrift, se pkt. 1.7. Slik avtale gir begge avtaleparter grunnlag for å innrette seg i tillit til at den andre avtaleparten har tilfredsstillende personvern og informasjonssikkerhet.

Retningslinjene beskriver og stiller krav til organisasjonsleddenes arbeid med personvern og informasjonssikkerhet for personopplysninger som behandles i DFS. Personopplysninger skal være riktige og ajourførte, og skal kun benyttes til de formål som er nødvendig for å oppfylle medlemsavtalen, omfattet av den registrertes samtykke eller annet lovhjemlet behandlingsgrunnlag. Organisasjonsleddene har ansvar for at personopplysningene er riktige. Medlemmene selv får hvert år en påminnelse ved innlogging om å kontrollere personopplysningene som er registrert om seg selv i Mitt DFS. Medlemmene har således et medansvar for at personopplysningene er riktige.

DFS sentralt håndterer i tillegg personopplysninger om egne ansatte. Retningslinjenes krav gjelder også i denne sammenhengen, og organisasjonsleddet skal ivareta de ansattes personvern iht. gjeldende lover og forskrifter og spilleregler i arbeidslivet. Det er spesielt viktig at opplysninger om de ansattes bruk av informasjonssystemene (hendelsesregistrering) kun benyttes til overordnet systemovervåkning på gruppenivå eller generell kontroll av informasjonssystemene.

Et organisasjonsledd skal ikke overvåke enkeltpersoner unntatt i de tilfeller personvernlovgivningen eksplisitt gir hjemmel til det. Dette innebærer at organisasjonsleddet ikke skal kartlegge hvor mye tid en person bruker på internett eller hvilke nettsider som blir besøkt, eller bruke aktivitetslogger til å overvåke personers produksjon eller innsats.

En person har rett til innsyn i opplysninger som gjelder seg selv.

Retningslinjene regulerer organisasjonsleddets manuelle og elektroniske behandling av personopplysninger uavhengig om personopplysningene lagres i manuelle eller elektroniske arkiv, men er særlig innrettet mot behandling av elektroniske arkiv.

Organisasjonen og organisasjonsleddene skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med bruken av opplysningene. Dette innebærer at organisasjonen og organisasjonsleddene skal ha rutiner for hvordan og hvor ofte lagret informasjon skal gjennomgås. Personopplysninger oppbevares over tid bl.a. for å ivareta historisk informasjon om aktivitet (resultater, tillitsverv, kurs og liknende.).

Dersom en person krever informasjonen slettet fra DFS' systemer, og organisasjonen ikke har hjemmel for fortsatt lagring, skal de aktuelle opplysningene anonymiseres og slik at opplysningene ikke kan henføres til en bestemt person uten bruk av supplerende opplysninger. Slike supplerende opplysninger skal lagres separat og være underlagt tekniske og organisatoriske foranstaltninger for å sikre at de ikke kan brukes til identifisering.

Organisasjonsledd som har saklige behov for registrering av sensitive personopplysninger som f.eks. helseopplysninger, kan kun gjøre dette i samsvar med personopplysningslovens krav. Det kreves normalt konsesjon fra Datatilsynet for registrering og behandling av sensitive personopplysninger. Det er unntak fra konsesjonsplikten for legevirksomhet som utøves i samsvar med Helseregisterloven.

#### **1.7. Juridisk bindende ved avtale**

Retningslinjene er juridisk bindende for alle organisasjonsledd, deres eksterne parter og andre som gjennom avtale har forpliktet seg til å følge retningslinjene. Ved avtale om at retningslinjene skal være bindende for eksterne parter, skal det inntas egne bestemmelser som regulerer konsekvenser ved brudd på retningslinjene.

## **DEL II: ARBEIDET MED PERSONVERN OG INFORMASJONSSIKKERHET**

### **2. Oversikt**

#### **2.1. Ansvar**

Det er organisasjonsleddets ledelse som har ansvaret for å etablere og opprettholde tilfredsstillende personvern og informasjonssikkerhet. Denne delen av retningslinjene omhandler hvilke forpliktelser organisasjonsleddet har som behandlingsansvarlig i henhold til retningslinjene og personopplysningsloven.

Det daglige ansvaret tilligger som oftest daglig leder i organisasjonsleddet eller styreleder i organisasjonsledd uten daglig leder. Den som har det daglige ansvaret for informasjonssikkerheten, kan overføre oppgaver til egne ansatte. Oppgaver kan også overføres til eksterne, f.eks. kan man delegere oppgaver til eksterne parter. Dette må gjøres i form av skriftlige avtaler. Uansett om oppgaver er delegert eller ikke, ligger det juridiske ansvaret hos behandlingsansvarlig.

#### **2.2. Oversikt over oppgaver som omfattes av det daglige ansvaret for informasjonssikkerhet**

Den som har det daglige ansvaret for behandling av personopplysninger i et organisasjonsledd er behandlingsansvarlig, skal fastlegge hvordan arbeidet med personvern og informasjonssikkerhet i organisasjonsleddet skal organiseres og gjennomføres slik at det kommer klart frem hvem som er ansvarlig på alle nivåer, og hva de er ansvarlig for.

#### **2.3. Personvernombud**

DFS sentralt har et personvernombud.

Personvernombudet skal:

- Involveres tidlig i alle saker som handler om behandling av personopplysninger
- Være kontaktpunkt for personer som er registrert i registre i forbindelse med spørsmål eller krav knyttet til behandlingen av deres personopplysninger.
- Gi råd til virksomheten og ansatte i personvernspørsmål
- Bidra til etterlevelse av personvernlov og personvernkravene som følger av retningslinjene.
- Gi råd og delta i konsekvensanalyser
- Være kontaktpunkt mellom virksomheten og Datatilsynet.
- Være bundet av taushetsplikt.
- Være ha en uavhengig rolle i organisasjonen, og skal rapportere til generalsekretæren/ organisasjonsleddets daglige leder, eller styreleder dersom administrativ leder ikke finnes.



## **DEL III: STYRENDE DEL**

### **3. Styringssystem for personvern og informasjonssikkerhet**

Organisasjonsleddets ledelse skal etablere et styringssystem for personvern og informasjonssikkerhet som en del av organisasjonsleddets internkontrollsystem. Dette styringssystemet angir aktiviteter for å veilede og styre organisasjonsleddet når det gjelder informasjonssikkerhet.

I det følgende er det gitt en nærmere beskrivelse av sentrale elementer i styringssystemet.

#### **3.1. Sikkerhetsmål**

Det skal fastsettes sikkerhetsmål for organisasjonsleddet. Sikkerhetsmålene skal beskrive:

- Behovene for og formålene med behandling av personopplysninger
- Overordnede føringer for organisasjonsleddets bruk av informasjonsteknologi

#### **3.2. Formål**

Det skal fastslås hva som er behovene for og formålene med behandlingene av personopplysninger i organisasjonsleddet. Utgangspunktet er følgende:

Personopplysninger skal kun innhentes og behandles i den grad dette gjøres for ivaretagelsen av medlemsavtalen, organisasjonens aktivitet og for å ivareta interessene til personer tilknyttet organisasjonen.

#### **3.3. Overordnede føringer for organisasjonsleddets bruk av informasjonsteknologi**

Sammen med formålene med behandlingene av personopplysninger i organisasjonsleddet skal overordnede føringer for organisasjonsleddets bruk av informasjonsteknologi beskrives i sikkerhetsmål. De overordnede føringene for bruk av informasjonsteknologi beskriver hvordan informasjonsteknologi er tatt i bruk og integrert i organisasjonsleddets drift.

#### **3.4. Sentrale sikkerhetsformål**

Grunnleggende forutsetninger for å behandle personopplysninger er bl.a. at all bruk av personopplysninger skal være i samsvar medlemsavtalen, innhentet samtykke og/ eller annet behandlingsgrunnlag, at opplysningene skal være fullstendige, oppdaterte og korrekte, og at omfanget av behandling av personopplysninger skal begrenses til det som er nødvendig.

Sentrale sikkerhetsmål er at personopplysninger skal:

- Være tilgjengelig for rett personell til rett tid i henhold til fastsatte prinsipper for tilgangsstyring etter pkt. 4.1 nedenfor.
- Behandles i tråd med reglene om taushetsplikt og være beskyttet slik at uvedkommende ikke får kjennskap til opplysningene. Uvedkommende omfatter blant annet personell som ikke har tjenstlig behov.

Organisasjonsleddets ledelse skal, på bakgrunn av ovenstående og kravene i pkt. 3.5, fastsette nivå for akseptabel risiko.

Eksempler på hendelser organisasjonsleddet ønsker å beskytte seg mot:

- Felles hendelser for brudd på konfidensialitet, integritet og tilgang.
  - Innbrudd i organisasjonsleddets lokaler eller nettverk.
  - Uvedkommendes bruk av brukerkonti.
  - Angrep av virus eller andre ondartede program.
- Brudd på konfidensialitet (personopplysninger kommer på avveie).
  - Tap av bærbart utstyr.
  - Tap av lagringsmedium.
  - Utskrift liggende på skriver.
  - Utsiktet utlevering av personopplysninger via e-post
- Brudd på integritet (personopplysninger blir endret).
  - Ulike versjoner av dokumenter med personopplysninger.
  - Feilregistrering.
- Brudd på tilgang (personopplysninger er utilgjengelige).
  - Nettverk eller system ute av drift.
  - Brann, vannskade og strømsvikt.
  - Hærverk.
  - Tjenestenektangrep (Denial of Service).

### 3.5. Nivå for akseptabel risiko

De overordnede krav for organisasjonsleddets behandling av personopplysninger som skal legges til grunn for etablering av sikkerhetstiltak, omfatter følgende:

#### 3.5.1. Konfidensialitet

Konfidensialitet skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysningene. Dette innebærer blant annet:

- Personer utenfor organisasjonsleddet uansett ressurser og kunnskap skal ikke kunne få uautorisert tilgang til personopplysninger.
- Personer i organisasjonsleddet skal gis tilgang i henhold til fastsatte prinsipper for tilgangsstyring i henhold til pkt. 4.1 nedenfor.

#### 3.5.2. Integritet

- Organisasjonsledd som eier eller leier egne fagsystemer skal registrere i fagsystemet hvem som har foretatt registrering, endring og sletting. På denne måten sikres sporbarhet.
- Sikkerhetstiltak skal iverksettes slik at personer eller teknologi, i eller utenfor organisasjonsleddet, ikke skal kunne endre personopplysninger uten autorisasjon.
- Personopplysninger skal henføres til rett identifisert person.
- Personopplysninger skal være fullstendige og ajourført i forhold til behandlingen av opplysningene.

#### 3.5.3. Tilgjengelighet

- For de som har tilgang, hvor taushetsplikten er vurdert og ivaretatt, skal person-

opplysninger være tilgjengelige når det er tjenstlig behov for dem.

På bakgrunn av disse overordnede kravene og organisasjonsleddets sikkerhetsmål, se pkt. 3.1-3.4, må organisasjonsleddet selv fastsette nivå for akseptabel risiko som skal gjelde i eget organisasjonsledd.

### **3.6. Oversikt over behandlinger av personopplysninger**

En samlet og oppdatert oversikt over all behandling av personopplysninger i organisasjonsleddet er et viktig styringsdokument for personvern og informasjonssikkerhet, og et praktisk redskap i det gjennomførende arbeidet. Oversikten vil også gi bidrag til den generelle internkontrollen i organisasjonsleddet. Oversikten kan f.eks. utarbeides som en database med oversikt over systemer og registre for behandling av personopplysninger som til enhver tid er i bruk i organisasjonsleddet. Dette skal omfatte IT-systemer, databaser, prosjekter med bruk av persondata og manuelle registre mv.

På et overordnet nivå skal oversikten inneholde følgende opplysninger:

- Kategorier av personopplysninger
- Formålet med behandlingen
- Juridisk hjemmelsgrunnlag for behandlingen
- Angivelse av hvor lenge ulike personopplysninger eller typer av personopplysninger skal lagres
- Angivelse av system/register/utstyr, og om det er elektronisk eller manuelt
- Grunnlaget for behandlingen
- Om opplysningene er sensitive eller ikke-sensitive
- Konsesjonsplikt/meldeplikt/hjemmel for unntak
- Oversikt over eventuelle databehandlere eller eksterne parter (IT-leverandører, revisorer, regnskapsførere mv.)
- Internt ansvarlig for det enkelte system/register/utstyr

På et mer detaljert nivå kan oversikten inneholde nærmere opplysninger og kommentarer relatert til punktene ovenfor, samt informasjon om hvilke sikkerhetstiltak som er iverksatt for det enkelte system, register eller utstyr og dato for siste gjennomførte risikovurdering.

### **3.7. Risikovurderinger**

Risikovurderinger har betydning både i det styrende, gjennomførende og kontrollerende informasjonssikkerhetsarbeidet.

Før behandling av personopplysninger igangsettes skal det gjennomføres risikovurderinger for å kartlegge risikoområder, sannsynlighet for og konsekvens av uønskede hendelser. Ny risikovurdering skal gjennomføres ved endringer som har betydning for personvernet og informasjonssikkerheten. I tillegg skal organisasjonsleddets ledelse jevnlig gjennomføre risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten, se pkt. 5.2.

Risikovurdering tar utgangspunkt i kravet om forholdsmessig sikring av opplysninger. Formålet med vurderingen er å avdekke om behandlingsansvarlig har iverksatt tilstrekkelige tiltak slik at dette blir oppnådd, eller om ytterligere tiltak må iverksettes. Vurderingen gjøres basert på fastlagte sikkerhetsmål og sikkerhetsstrategi.

En viktig del av oppgaven er kartlegging av de opplysninger som må sikres, og å kartlegge det miljø opplysningene befinner seg i. Her vil oversikten over behandlinger av personopplysninger være et utgangspunkt, se pkt. 3.6. Risikovurderingen skal i tillegg identifisere behov for risikoreduserende tiltak ved å sammenligne avdekket risiko med nivå for akseptabel risiko. Nivå for akseptabel risiko bygger på fastlagte sikkerhetsmål og sikkerhetsstrategi, se pkt.3.3.

Risikobegrepet rommer to størrelser: sannsynlighet for at noe skal skje, og hvilke konsekvenser en hendelse kan få. Når vi snakker om sikkerhetsrisiko for informasjonssystemer vil de hendelsene som på denne måten vurderes være knyttet til konfidensialitet, integritet og tilgjengelighet.

Risikovurderingen starter med utgangspunkt i nivå for akseptabel risiko og består av følgende trinn:

- Forberedelser med planlegging og organisering
- Kartlegging og vurdering av behandlingen
- Identifisere uønskede hendelser
- Konsekvensvurderinger
- Sannsynlighetsvurderinger
- Risikoberegning og vurdering
- Tiltak som iverksettes

Risikovurdering skal som minimum gjennomføres før det;

- iverksettes førstegangsbehandling av personopplysninger, eller når det behandles personopplysninger på en ny måte eller når en ny type personopplysninger behandles
- etableres nye informasjonssystemer eller registre som inneholder personopplysninger
- iverksettes organisatoriske endringer som kan påvirke informasjonsbehandlingen
- iverksettes tekniske endringer i utstyr og/eller programvare som kan påvirke informasjonsbehandlingen
- iverksettes andre endringer med betydning for informasjonssikkerheten
- gis tilgang til personopplysninger til eksterne parter.

Risikovurderingen skal dokumenteres. Konklusjonene fra vurderingen skal sammenlignes med fastlagt nivå for akseptabel risiko. Er risikoen høyere enn fastsatt nivå for akseptabel risiko skal det iverksettes tiltak (nye/endrede) for å oppnå akseptabel risiko.

## DEL IV: GJENNOMFØRENDE DEL

### 4. Ansvarliggjøring – taushetsplikt

For å sikre konfidensialitet for personopplysninger skal organisasjonsleddets leder sikre at alle som gis tilgang har taushetsplikt, både gjennom avtaleregulering og ved å informere om avtalefestet og/eller lovpålagt taushetsplikts innhold og omfang. Det skal som minimum:

- Beskrives konsekvenser ved brudd på taushetsplikten.
- Beskrives konsekvenser ved å tilegne seg eller forsøke å tilegne seg opplysninger man ikke har tjenstlig behov for (ulovlig tilegnelse).
- Beskrives konsekvenser ved å endre/forsøk på å endre opplysninger man ikke har autorisasjon til å endre.

Brudd på taushetsplikten og/eller ulovlig tilegnelse skal som konsekvens minimum medføre en advarsel for den som begår bruddet, og bruddet skal behandles iht. avviksprosedyre. Ved alvorlige eller gjentatte brudd på taushetsplikten må konsekvenser for personen (ansettelsesforhold etc.) vurderes.

Brudd på taushetsplikten og/eller ulovlig tilegnelse er forbudt og varsling til tilsynsmyndighetene og anmeldelse må vurderes.

#### 4.1. Tilgangsstyring

Dette berører hvordan man foretar:

- Autentisering som sikrer identifisering av autorisert bruker.
- Autorisering som er tildeling av rettigheter til å kunne lese, registrere, redigere, og/eller slettepersonopplysninger.
- Tilgjengeliggjøring av personopplysninger om bestemte personer for autorisert personell.
- Kontrollerende tiltak.

Autorisering og tilgang er kun aktuelt for personer som;

- Er underlagt eget organisasjonsledds instruksjonsmyndighet (f.eks. egne ansatte, tillitsvalgte osv.)
- Arbeider under instruksjonsmyndighet av organisasjonsleddets eventuelle databehandlere.

Autorisasjon kan bare gis i den grad det er nødvendig for personens rolle/arbeid, er begrunnet i tjenstlige behov og er i henhold til bestemmelser om taushetsplikt. Det er kun slikt personell som kan gis tilgang til personopplysninger.

Tilgangsstyring skal etableres for alle fagsystemer.

##### 4.1.1. Autentisering

En og samme person kan ha ulike roller i organisasjonen. Autorisering skal skje selvstendig for hver enkelt rolle og autentisering skal sikre identifisering i korrekt rolle i hvert enkelt tilfelle.

- Ulike roller skal identifiseres, og om nødvendig gis ulike autentiseringskriteria

(brukernavn, passord mv.)

- Flere personer skal ikke benytte samme autentiseringskriteria (brukernavn, passord).
- Tildeling av autentiseringskriteria skal gjennomføres på en betryggende måte.
- En risikovurdering må vise at autentiseringsløsningen gir tilstrekkelig sikkerhet.

#### 4.1.2. Autorisering

Behandlingsansvarlig er ansvarlig for at autorisasjoner tildeles, administreres og kontrolleres.

Behandlingsansvarlig skal sørge for at det finnes et autorisasjonsregister. Registeret skal som minimum inneholde;

- Informasjon om hvem som er tildelt autorisasjon
- Til hvilken rolle autorisasjonen er tildelt (formålet)
- Tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt
- Informasjon om hvilke(t) organisasjonsledd den autoriserte er knyttet til.

Behandlingsansvarlig delegerer myndighet for å tildele autorisasjon til det enkelte organisasjonsleddets ansvarlige ledelse, dvs. daglig leder, styreleder og styremedlemmer.

For personer som har ulike roller i organisasjonsleddet, skal autorisering skje for hver rolle uavhengig av vedkommendes øvrige roller.

Det skal etableres prosedyre for tildeling og administrasjon av tilgangsrettigheter:

- Autorisasjon for å lese, registrere, redigere, og/eller slette personopplysninger skal gis til dem som har tjenstlig behov. Også tekniske tiltak skal iverksettes for å ivareta krav til konfidensialitet ved aktivt å hindre uvedkommende i å få tilgang og for å sikre dokumentasjon av tildelt autorisasjon.
- Ved autorisasjon for tilgang til sensitive personopplysninger skal slik autorisasjon tildeles i henhold til betryggende prosedyrer. Lovbestemt taushetsplikt skal vurderes og overholdes.
- Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder personopplysninger. Det skal iverksettes tiltak slik at mulig misbruk skal kunne avdekkes.

#### 4.1.3. Tilgang

Bare autorisert personell kan få tilgang til personopplysninger. Tilgang til fagsystemer skal gis på bakgrunn av beslutninger om tjenstlig behov. Organisasjonsleddet skal sikre at taushetspliktreglene overholdes.

#### 4.1.4. Utlevering av personopplysninger til andre land

Utlevering betyr at personopplysninger overlates til annen behandlingsansvarlig i utlandet. Dette er en ny behandling, og det kreves et eget behandlingsgrunnlag (for eksempel samtykke eller lovhjemmel). Dersom ikke annet behandlingsgrunnlag finnes og samtykke ikke allerede er avgitt, må det innhentes samtykke fra den registrerte.

Overføring av personopplysninger til andre land må kun skje i samsvar med de krav som følger av personopplysningslovens kap. 5 og 6. Se nærmere informasjon på [datatilsynet.no](https://datatilsynet.no).

#### 4.1.5. Kontrollerende tiltak

Det skal i størst mulig utstrekning benyttes tekniske tiltak for å oppfylle kravene ovenfor. All autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene skal registreres og registeret skal oppbevares til det av ikke lenger antas å bli bruk for det. Hendelsesregistrene skal analyseres med henblikk på å oppdage brudd.

- Det skal etableres prosedyrer for å analysere hendelsesregistrene slik at hendelser oppdages før de får alvorlige konsekvenser.
- Det skal etableres prosedyrer for ved behov å kunne sammenholde hendelsesregistrene med autorisasjonsregister.
- Dersom brudd avdekkes skal reaksjoner mot bruker iverksettes.
- Dersom reaksjoner mot bruker ikke har nødvendig effekt over tid, dvs. det er gjentatt tilgang av flere personer som ikke er autorisert, skal nødvendige tekniske tiltak iverksettes.
- Hendelsesregistrene og autorisasjonsregister skal sikres mot endring og sletting av uautorisert personell.

#### 4.2. Behandling av personopplysninger

Organisasjonsleddets ledelse skal påse at det utarbeides og iverksettes prosedyrer for behandling av personopplysninger. Brudd på prosedyrer skal behandles som avvik. Følgende prosedyrer skal som minimum foreligge:

##### 4.2.1. Prosedyre for bruk av informasjonssystemet

Regler for bruk av informasjonssystemet skal nedfelles i prosedyre som minimum skal ivareta at:

- Det ikke skal søkes annen informasjon enn den man er autorisert for og har behov for i den aktuelle arbeidssituasjon.
- Autentiseringskriteria skal beskyttes, bl.a. ved at passord skal hemmeligholdes.
- Personopplysninger som registreres skal være relevante og nødvendige.
- Registrering skal gjøres snarest mulig etter at informasjonen har fremkommet.

##### 4.2.2. Kontroll av tilgangsstyring

Gjennomgang og kontroll av tilgangsstyring, herunder tildelte autorisasjoner, skal foretas av den enkelte leder:

- Ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling, endring av arbeidsområde eller ved endring av tillitsvalgte mv.
- Minimum årlig (enten i forbindelse med sikkerhetsrevisjon eller etter avholdt årsmøte/ting).
- Ved sikkerhetsbrudd; for det informasjonsområdet som blir berørt av bruddet.

##### 4.2.3. Informasjon og samtykke

Det skal etableres prosedyrer og gjennomføres tiltak for å sikre at:

- Det innhentes samtykke fra personen med mindre slikt samtykke ikke er påkrevd etter lov eller annet gyldig grunnlag. Behandling av medlemsopplysninger basert på

medlemsavtalen krever ikke samtykke. Samtykke skal innhentes fra foresatte når personen er et barn under 15 år. Samtykke innhentes i tråd med alminnelige regler for samtykke. Det kreves ikke særskilt samtykke for at et organisasjonsledd skal kunne distribuere markedsmateriell fra sine sponsorer direkte til personer tilknyttet organisasjonsleddet, med mindre slik distribusjon innebærer at sponsor gis tilgang til personopplysninger.

- Personen får informasjon om organisasjonsleddets behandling av personopplysninger, og sine rettigheter til innsyn i, retting, sletting og sperring av registrerte opplysninger om seg selv.
- Personen sikres innsyn i egne personopplysninger.
- Personens rettigheter til retting/sletting av personopplysninger ivaretas.

#### **4.3. Etablering og drift av informasjonssystemet**

Dette omhandler de tiltak som må iverksettes for at personopplysninger skal være sikret mot at personer som ikke er autoriserte får tilgang og at opplysningene er tilgjengelige ved behov. Med informasjonssystemet menes det samlede utstyr og programvare som behandler eller kan behandle personopplysninger.

##### **4.3.1. Konfigurasjonskontroll**

Det er en forutsetning at organisasjonen har oversikt over programvare som benyttes i behandlingen av personopplysninger. Konfigurasjonen skal sikre at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt.

Konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, skal ikke settes i drift før følgende tiltak er gjennomført:

- Risikovurdering som viser at nivå for akseptabel risiko er oppfylt
- Test som sikrer at forventede funksjoner er ivaretatt
- Implementeringsplan som sikrer mot uforutsette hendelser
- Ny konfigurasjon er dokumentert
- Konfigurasjonsendringer er godkjent av organisasjonsleddets leder eller den ledelsen bemyndiger.

Konfigurasjonskontroll skal reguleres gjennom avtale ved bruk av databehandler.

##### **4.3.2. Konfidensialitet og integritet**

Dette omhandler de tekniske tiltak og organisatoriske tiltak som skal iverksettes for å hindre at personer uten autorisasjon får tilgang til personopplysninger.

- Tekniske tiltak og organisatoriske tiltak skal iverksettes slik at personer ikke skal kunne få tilgang til personopplysninger de ikke er autorisert for.
- Tekniske tiltak skal iverksettes slik at personer i eller utenfor organisasjonsleddet uansett ressurser og kunnskap ikke skal kunne endre personopplysninger uten at det registreres i fagsystemet hvem som har endret og hva som er endret.
- Tekniske tiltak skal iverksettes slik at uautorisert programvare ikke skal kunne endre personopplysninger.
- Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, redigere, og/eller slette personopplysninger. All tildeling av autorisasjon skal registreres i et autorisasjonsregister.



- Alle systemer skal ha mekanismer som hindrer uautoriserte endringer av personopplysninger.
- Alle fysiske lagringsmedia, dvs. disk, minnepinne, CD, mv., skal merkes, og alle personopplysninger skal slettes når lagringsmediet tas ut av bruk. Plikt til arkivering av opplysningene må uansett overholdes.

For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres hendelsesregistre over følgende:

- Sikkerhetsbarrierene skal registrere sikkerhetsrelevante hendelser, bl.a. forsøk på uautorisert bruk av informasjonssystemet.
- Systemer som bruker DFS' sentrale database skal registrere alle forsøk på uautorisert bruk.
- Hendelsesregistre skal sikres mot endring og sletting av uautorisert personell.

#### **4.4. Opplæring og kompetanse**

Organisasjonsleddet skal iverksette tiltak som ivaretar at alle som gis tilgang til og/eller drifter informasjonssystemene og tilhørende informasjon skal ha tilstrekkelig kunnskap til å utnytte systemene for sin rolle og til å ivareta personvern og informasjonssikkerheten.

Kompetansebygging må skje kontinuerlig og være tilpasset de ulike roller og brukergrupper. Særskilte opplæringstiltak må vurderes for nye personer og ved endringer i informasjonssystemene eller i behandlingen av personopplysninger.

#### **4.5. Datakommunikasjon**

Når det benyttes datakommunikasjon skal hvert enkelt organisasjonsledd enten selv ivareta de påfølgende krav, eller sørge for at de som utfører oppgaven/leverer tjenesten ivaretar kravene. Internettbaserte løsninger som håndterer personopplysninger skal sikre kommunikasjonen mellom brukere og systemet ved bruk av TLS/SSL-sertifikat og protokoll.

##### **4.5.1. Meldingsformidling og e-post med sensitive personopplysninger**

DFS har per dato ikke system som håndterer meldingsformidling og e-post med sensitive personopplysninger. Sensitive personopplysninger skal sendes med brevpost.

##### **4.5.2. Kommunikasjon med personer**

Organisasjonsleddet er ansvarlig for at:

- Samtykke fra personen er innhentet til å formidle personopplysninger elektronisk i den grad formidlingen ikke følger av medlemsavtalen eller et annet behandlingsgrunnlag.
- Avgitt samtykke og informasjon om omfanget av dette blir oppbevart.
- Organisasjonsleddet skal påse at det gjennomføres tilstrekkelige tiltak for å sikre at meldinger sendes til rett mottaker. Dersom personen har oppgitt digital kontaktinformasjon kan dette anses som et samtykke til at organisasjonsleddet kan sende e-post og SMS forutsatt at slik kommunikasjon følger av medlemsavtalen, samtykke gitt av den registrerte eller annet behandlingsgrunnlag.
- Personen entydig identifiseres.

#### **4.6. Avtaler**

I dette punktet omtales kun de avtalemessige forhold som angår personvern og informasjonssikkerhet.

Under er listet eksempler på kommunikasjons-parter hvor det utveksles identifiserbare personopplysninger, og/eller parter som har/får adgang til utstyr og/eller programvare hvor slike opplysninger behandles. Det skal alltid inngås skriftlige databehandleravtaler med slike eksterne parter. Avtalene skal inkludere forpliktelser om at partene skal oppfylle de krav og tiltak som følger av den til enhver tid gjeldende retningslinjer for behandling av personopplysninger og informasjonssikkerhet og personopplysningslovgivning, samt regulering av sanksjoner ved brudd på retningslinjene og avtalen for øvrig.

- Databehandlere, som utfører behandling av personopplysninger på vegne av organisasjonsleddet.
- Eksterne parter som integrasjonspartnere eller leverandører av utstyr og/eller programvare som må ha adgang for vedlikehold, feilretting, oppdatering, ved hjelp av online tilkobling og/eller fysisk oppmøte.
- Sikkerhetsleverandører.
- Eventuelle personer som ikke er underlagt behandlingsansvarliges instruksjonsmyndighet.

For mer informasjon om personopplysningslovens krav til databehandleravtaler, se Datatilsynets veiledning og mal:

<https://www.datatilsynet.no/regelverk-og-skjema/veiledere/databehandleravtale/>

#### **4.6.1. Databehandler**

Databehandler har et selvstendig ansvar for personvern og informasjonssikkerhet etter personopplysningsloven. I avtalen må sikkerhetsforhold reguleres konkret. Databehandlerens selvstendige plikt til å etterleve personopplysningsforskriften må presiseres. I tillegg skal det stilles kriterier for akseptabel risiko hos databehandleren, samt at behandlingsansvarlig skal sikres innsynsrett for å forsikre seg om at kravene etterleves. Utover dette skal det fremgå av avtalen at databehandler tilfredsstillere kravene i retningslinjene.

Databehandler skal ikke behandle personopplysninger på annen måte enn det som er avtalt med behandlingsansvarlig.

#### **4.6.2. Eksterne parter**

Organisasjonsleddet skal for å ivareta konfidensialitet, integritet og tilgjengelighet for personopplysninger inngå databehandleravtaler med eksterne parter for å sikre at:

- Eksterne parters personale har undertegnet taushetserklæring som innebærer en absolutt taushetsplikt med henblikk på alle personopplysninger.
- Eksterne parter etterlever retningslinjene med tanke på behandlingsansvarliges plikter vedrørende sikkerhetsrevisjoner og avviksbehandling.
- Eksterne parters utstyr som benyttes ved online oppkobling ved hjelp av kommunikasjonsnett eller medbrakt utstyr som knyttes til organisasjonsleddets utstyr, ikke har ondsinnet programvare som inneholder virus e.l. og at utstyret er sikret mot adgang fra uvedkommende.
- Tilgjengelighet til personopplysninger skal om mulig opprettholdes når eksterne part utfører arbeid på organisasjonsleddets utstyr/programvare, slik at organisasjonsleddet kan ivareta sine oppgaver.
- Eksterne partner pålegges å innhente organisasjonsleddets godkjenning ved bruk av ev. underleverandører som kan få tilgang til persondata.

## DEL VI: KONTROLLERENDE DEL

### 5. Oppfølgingsansvar

Organisasjonsleddets ledelse skal følge opp at sikkerheten ivaretas, se også pkt. 5.2.8. Det skal gjennomføres fem typer oppfølging, i tillegg til den daglige oppfølging:

- Sikkerhetsrevisjoner
- Risikovurderinger
- Avvikshåndtering
- Ledelsens gjennomgang
- Kontroll av tilganger

#### 5.1. Sikkerhetsrevisjon

Organisasjonsleddets ledelse skal følge opp at sikkerheten ivaretas ved minimum årlige sikkerhetsrevisjoner. Det skal foreligge en godkjent plan for sikkerhetsrevisjoner.

Sikkerhetsrevisjonen skal som minimum omfatte vurderinger av:

- Plassering av ansvar og organisering av sikkerhetsarbeidet
- Kvalitet på sikkerhetsmål og sikkerhetsstrategi
- Overholdelse av prosedyrer for bruk av informasjonssystemer og personopplysninger
- Resultat av opplæring
- Forvaltning og bruk av personopplysninger
- Tilgang til personopplysninger og tiltak mot uautorisert innsyn
- Effekten av etablerte sikkerhetstiltak
- Ivaretagelse av personvern og informasjonssikkerhet hos kommunikasjonspartnere, databehandlere og eksterne parter

Resultatene og konklusjonene fra sikkerhetsrevisjonene skal dokumenteres. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemene som ikke er forutsatt, skal dette behandles som avvik.

#### 5.2. Risikovurdering

Organisasjonsleddets ledelse skal også jevnlig gjennomføre risikovurderinger for å kartlegge risikoområder og klarlegge sannsynlighet for og konsekvens av uønskede hendelser (pkt. 3.8).

#### 5.3. Avvikshåndtering

Organisasjonsleddets ledelse, eller det organ ledelsen bemyndiger, skal behandle avvik med det formål å gjenopprette normal tilstand, fjerne årsaken til avviket og å hindre gjentagelse.

Avviksbehandlingen iverksettes ved sikkerhetsbrudd og/eller når behandling av personopplysninger er utført i strid med gjeldende regelverk, retningslinjer eller prosedyrer. Avviksbehandling kan også iverksettes ved tilfeller av manglende eller uhensiktsmessige prosedyrer.

- Hver enkelt person er ansvarlig for å rapportere oppdagede avvik på fastsatt elektronisk skjema på [www.dfs.no/varsel](http://www.dfs.no/varsel)
- For hvert rapportert avvik skal det foretas en innsamling av fakta om hendelsesforløpet og foretas en vurdering som grunnlag for iverksettelse av korrigerende tiltak.

- Det skal foreslås tiltak og eventuelle alternative tiltak med beskrivelse av plan for gjennomføring for å gjenopprette normal tilstand og forhindre gjentakelse.
- Tiltak og plan på det nivå som er gjennomførbart skal vedtas. Tiltaket skal være slik at det hindrer eller reduserer sannsynligheten for gjentakelse.
- Tiltaket iverksettes iht. plan med rapportering til organisasjonsleddets ledelse, eller det organ ledelsen bemyndiger.
- Det sendes statusrapport til organisasjonsleddets ledelse eller det organ ledelsen bemyndiger, som dokumenterer resultatet av avviksbehandlingen.
- Ved gjentatte avvik skal det gjennomføres ny risikovurdering.

Dersom det har blitt foretatt en uautorisert utlevering av personopplysninger skal Datatilsynet varsles.

#### **5.4. Ledelsens gjennomgang**

Organisasjonsleddets ledelse skal selv følge opp at personvern og informasjonssikkerheten ivaretas ved minimum årlig gjennomgang. Ledelsens gjennomgang må sees i sammenheng med økonomi- og virksomhetsplanleggingen da beslutningene kan få økonomiske konsekvenser.

Formålet med gjennomgangen er en kontroll av status på sikkerhetsnivået og om dette er i samsvar med organisasjonsleddets mål og strategi. Følgende skal som minimum gjennomgås:

- Resultat fra sikkerhetsrevisjoner.
- Resultat fra risikovurderinger.
- Resultater fra avviksbehandling. Organisasjonsleddets ledelse skal regelmessig følge opp at tiltak på grunnlag av avvik blir fastlagt, planlagt og gjennomført.
- Ansvarsforhold og organisering mht. sikkerhet.
- Behovet for og formålet med behandling av personopplysninger og oversikt over personopplysninger som behandles i organisasjonsleddet. I gjennomgangen skal det vurderes hvor lenge ulike personopplysninger og typer av personopplysninger skal lagres.
- Konfigurasjonskart over informasjonssystemene.
- Sikkerhetsmål, nivå for akseptabel risiko og strategier for informasjonssikkerhet.
- Kontroll og oppfølging av inngåtte avtaler (ref. pkt. 4.6).

Dersom gjennomgangen avdekker at virkelig situasjon ikke når opp til fastsatt nivå for akseptabel risiko skal det vedtas tiltaksplan for å oppnå fastsatt nivå for akseptabel risiko, med plassering av ansvar.

Gjennomgangen skal danne grunnlag for eventuelle endringer av sikkerhetsmål og/eller sikkerhetsstrategi.

#### **5.5. Kontroll av tilganger**

Organisasjonsleddets ledelse skal påse at det jevnlig gjennomføres kontroll av hvem som har elektronisk tilgang til personopplysninger i et fagsystem.

Dersom kontrollen fører til mistanke om at det har skjedd urettmessig tilgang, skal organisasjonsleddets ledelse varsles. Forøvrig skal hendelsen behandles iht. etablerte prosedyrer for avviksbehandling, særlig med henblikk på å få avklart om eksisterende tilgangskontroll er god nok.

## Vedlegg 1: Definisjoner, ord og uttrykk

Det kan ikke utledes rettigheter eller plikter av definisjonene alene. De må leses i den sammenheng de benyttes i retningslinjene.

Med «**administratorrettighet**» menes øverste tilgangsnivå til system, server, database, og sikkerhetsbarrierer. Tilgangsnivået har som oftest rettigheter til å utføre alle operasjoner.

Med «**advarsel**» menes en skriftlig reaksjon fra organisasjonsleddet overfor en person som har brutt prosedyrer e.l. Det skal klart fremgå at det dreier seg om en advarsel, årsaken til advarselen og hva som kan bli konsekvensene av nye brudd på prosedyrer e.l.

Med «**akseptabel risiko**» menes hvor stor risiko organisasjonen kan akseptere for at det inntreffer en hendelse som kan forårsake brudd på konfidensialitet, tilgjengelighet eller integritet for personopplysninger. Risikoens størrelse avhenger av hvor stor sannsynlighet det er for at hendelsen skal inntreffe og av konsekvensen av en slik hendelse.

Retningslinjene beskriver et nivå for akseptabel risiko i organisasjonen. Hvert enkelt organisasjonsledd må foreta en konkret vurdering av hvordan akseptabel risiko for vedkommende organisasjonsledd skal oppnås.

Med «**aktivitet**» menes administrasjon, planlegging og utøvelse av aktiviteter som f.eks. trening, dømming, konkurranser samt styre/ledelse, kurs og oppnådd kompetanse, og annen oppfølging av slik aktivitet.

Med «**anonymisert**» menes personopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson.

Med «**autentisering**» menes prosessen som gjennomføres for å bekrefte en påstått identitet.

Med «**autorisere/autorisert/autorisasjon/autorisering**» menes at en person i en bestemt rolle kan gis eller er gitt bestemte rettigheter til lesing, registrering, redigering, retting, sletting og/eller sperring av personopplysninger.

Med «**autorisasjonsregister**» menes et register over utstedte autorisasjoner somføres eller på annen måte dokumenterer autorisasjonene.

Med «**avvik**» menes enhver håndtering av personopplysninger som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer, samt andre sikkerhetsbrudd.

-B-

Med «**barn**» menes en person som er under 15 år. I alle spørsmål knyttet til sitt medlemskap har en person som har fylt 15 år, fulle rettigheter.

Med «**behandling**» menes enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Med «**behandlingsansvarlig**» menes den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes, hvis ikke behandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven (her benyttes begrepet «**behandlingsansvarlig**»). Det er organisasjonsleddet som er behandlingsansvarlig for behandling av personopplysninger. Ansvaret skal ivaretas av den daglige ledelsen av organisasjonsleddet. I organisasjonsledd uten daglig ledelse er styret ansvarlig. Utføringen av behandlingen kan settes bort til for eksempel en ekstern part (se «**databelandler**»), men ansvaret kan ikke delegeres bort.

## -D-

Med «**databehandler**» menes den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. personopplysningsloven. Det presiseres at en databehandler er en ekstern part eller et organisasjonsledd utenfor den behandlingsansvarliges organisasjonsledd. Det vil si at den behandlingsansvarliges egne medarbeidere ikke er dennes databehandlere.

## -E-

Med «**ekstern part**» menes en juridisk enhet som f.eks. en leverandør som yter tekniske og/eller administrative tjenester til organisasjonsleddet. Eksempler er konsulentselskap, leverandør av programvare eller utstyr mv. Eksterne virksomheter som gis avtale om integrasjon mot DFS' databaser for å tilby et fagsystem til organisasjonen er også en ekstern part.

## -F-

Med «**fagsystem**» menes en applikasjon eller et IT-system som behandler personopplysninger. Begrepet systemløsning brukes også om et fagsystem. Eksempler på fagsystem er Mitt DFS, arkivsystem, eLæring etc.

## -H-

Med «**hendelsesregister**» menes et logisk register (logg) der hendelser i informasjonssystemet er nedtegnet, se neste definisjon.

Med «hendelsesregistrering» menes logging av hendelser i et informasjonssystem, bl.a. med sikte på å forebygge, avdekke og hindre gjentakelse av sikkerhetsbrudd.

## -I-

Med «**SkytterID**» menes en personkode som er en unik identifisering av en person uten bruk av fødselsnummer.

Med «**indirekte identifiserbare personopplysninger**» menes personopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson, og hvor identitet bare kan tilbakeføres ved sammenstilling med de samme opplysninger som tidligere ble fjernet. For å regnes som indirekte identifiserbare personopplysninger, skal dataene være bearbeidet slik at de uten koblingsnøkkel ikke kan knyttes til en enkeltperson.

Med «**autentiseringsløsning**» menes den autentiseringsløsning som til enhver tid brukes av DFS sentrale IT-løsninger med bruker-id knyttet til SkytterID, som gjennom en risikovurdering viser at den har tilstrekkelig sikkerhet for DFS sine organisasjonsledd daglige bruk av IT-løsninger.

Med «**integritet**» menes at personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting og være korrekte, oppdaterte, relevante og tilstrekkelige som grunnlag for DFS' aktivitet.

Med «**internkontroll**» menes planlagte og systematiske tiltak som skal sikre at organisasjonsleddets aktiviteter planlegges, organiseres, utføres og vedlikeholdes i samsvar med krav fastsatt i lovgivningen.

## -K-

Med «**koblingsnøkkel**» menes en personentydig kode som refererer til de identifiserte opplysningene som gjør det mulig å identifisere et enkeltindivid med indirekte identifiserbare personopplysninger.

Med «**konfidensialitet**» menes at personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene.

Med «**konfigurasjon**» menes informasjonssystemets utforming inkludert både teknisk utstyr og

programvare.

Med «**konfigurasjonsendring**» menes en endring av informasjonssystemets utforming som følge av installasjon, oppgradering eller fjerning av utstyr eller programvare.

-M-

«**Medlem**» og «**medlemsopplysninger**», se person og personopplysninger.

Med «**medlemsavtalen**» menes aksept for medlemskap mellom en person og et organisasjonsledd når personen tas opp som medlem i organisasjonsleddet og medlemskapet er godkjent.

-O-

Med «**organisasjonen**» menes sentralleddet Det frivillige Skyttervesen.

Med «**organisasjonsledd**» menes ethvert organisasjonsledd som er tilsluttet Det frivillige Skyttervesen.

-P-

Med «**person**» menes fysiske, levende personer, uavhengig av om vedkommende er tilknyttet et skytterlag eller ikke, og uavhengig av hvilken rolle vedkommende eventuelt har, som medlem, tillitsvalgt, utøver, ansatt osv.

Med «**personopplysninger**» menes opplysninger og vurderinger som kan knyttes til en enkeltperson, jf. personopplysningsloven § 2 nr. 1.

Med «**personvernombud**» menes en formelt oppnevnt kontakt for personvern og informasjonssikkerhet mot behandlingsansvarlig (organisasjonsleddets ledelse), den registrerte og eksternt mot Datatilsynet.

-R-

Med «**Retningslinjene**» menes dette dokumentet. Andre dokumenter i tilknytning til Retningslinjene, som for eksempel veiledninger, er ikke omfattet av begrepet.

Med «**register**» menes en logisk sammenstilling av opplysninger. En database eller et regneark er en teknisk løsning for et register, jf. personopplysningslovens §2 nr. 3.

Med «**registrert/den registrerte**» menes en person som en personopplysning kan knyttes til, jf. personopplysningsloven § 2 nr. 6. Eksempler og begreper som brukes om den registrerte er ansatt, medlem, utøver, tillitsvalgt mv.

-S-

«**Skytter**», se person.

Med «**samtykke**» menes en skriftlig eller elektronisk erklæring som er avgitt frivillig, informert og uttrykkelig av den registrerte til behandling av bestemte personopplysninger. For barn under 16 år må slikt samtykke gis av foresatte.

Med «**sensitive personopplysninger**» menes opplysninger om:

- a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
- b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
- c) helseforhold/helseopplysninger
- d) seksuelle forhold
- e) medlemskap i fagforeninger

## -T-

Med «**tillitsvalgt**» menes et medlem som er blitt valgt eller oppnevnt til å fylle en funksjon eller utføre bestemte oppgaver for et organisasjonsledd, se også person.

Med «**taushetsplikt**» menes lovpålagt eller avtalt plikt til å hindre at andre får adgang eller kjennskap til personopplysninger, jf. personopplysningsforskriften § 2-9. Taushetsplikt innbefatter både en passiv plikt til å tie og en plikt til aktivt å hindre uvedkommende i å få kunnskap om taushetsbelagte opplysninger.

Med «**tekniske tiltak**» menes tiltak av teknisk karakter som ikke kan påvirkes eller omgås av medarbeidere, og ikke er begrenset av handlinger som den enkelte forutsettes å utføre. Eksempler på slike tiltak kan være ulike løsninger for autentisering eller konfigurering av en brannmur slik at den kun tillater bestemt trafikk eller en meldingstjeneste som er laget slik at alle meldinger automatisk blir kryptert.

Med «**tilgang**» menes at personopplysninger om en eller flere bestemte personer er eller gjøres tilgjengelige for autorisert personell. Tilgang til fagsystemer gis basert på tjenstlig behov som følger den funksjonen respektive person utøver i organisasjonsleddet.

Med «**tilgjengelighet**» menes at personopplysninger som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene.

Med «**tjenstlig behov**» menes at personer som følge av å skulle utføre bestemte oppgaver for et organisasjonsledd, behandler personopplysninger som er nødvendige for å utføre administrasjon av medlemskap, verv, aktiviteter eller andre forhold i forbindelse med dette.

## -U-

«**Utøver**», se person.

Med «**ulovlig tilegnelse**» menes å bryte forbudet mot å lese, søke eller på annen måte tilegne seg, bruke eller besitte personopplysninger, uten at det er begrunnet i tjenstlig behov.



## **Vedlegg 2: Krav til personvernerklæring i samlag og skytterlag (vi lager en mal basert på DFS personvernerklæring).**

Følgende må kort beskrives i en personvernerklæring i samlag og skytterlag:

**Hvem er behandlingsansvarlig?** Oppgi hvem som er hovedansvarlig for behandlingen av personopplysningene. Dette kan være en person eller en virksomhet med utgangspunkt i hvem som bestemmer formålet og hvordan opplysningene behandles. Hvis den behandlingsansvarlige har delegert myndighet, skal virksomheten oppgi hvem som har det daglige ansvaret.

**Hva er formålet?** Forklar formålet med behandlingen av personopplysningene, det vil si hvorfor opplysningene behandles.

**Hva er det rettslige grunnlaget?** Oppgi hva som er behandlingsgrunnlaget for hver enkelt behandling, det vil si virksomhetens hjemmel for å behandle personopplysningene.

**Hvilke personopplysninger behandles?** Gi en beskrivelse av hvilke typer personopplysninger som samles inn.

**Hvor hentes opplysningene fra?** Gi informasjon om hvor personopplysningene hentes fra.

**Er det frivillig å gi fra seg opplysningene?** Hvis opplysningene hentes direkte fra den registrerte, må virksomheten opplyse om det er frivillig for vedkommende å oppgi personopplysningene.

**Utleveres opplysningene til tredjeparter?** Opplys hvilke typer opplysninger som utleveres og hvilke tredjeparter som er mottakere, dersom opplysningene utleveres til andre.

**Hvordan slettes og arkiveres opplysningene?** Beskriv hvilke rutiner virksomheten har for å slette og arkivere personopplysningene.

**Hvilke rettigheter har den registrerte og hvilket lands lovverk gjelder?** Beskriv hvilke rettigheter og plikter allmennheten og den registrerte har etter personopplysningsloven. Dette gjelder retten til innsyn i egne personopplysninger, samt krav om retting eller sletting av mangelfulle eller uriktige opplysninger. Det bør komme tydelig frem hvilket lands lovverk som gjelder.

**Hvordan sikres opplysningene?** Beskriv hvilke sikringstiltak virksomheten har ved behandling av personopplysningene, så langt åpenhet om dette ikke svekker sikkerheten.

**Kontaktinformasjon.** Oppgi kontaktinformasjon og eventuelt skjema for innsyn, retting eller sletting, slik at brukeren enkelt kan ta kontakt ved behov.

DFS sentralt har utarbeidet en mal for hhv. skyttersamlag og skytterlag, som følger med veiledningen til samlag og skytterlag.

### **Vedlegg 3: Kort beskrivelse av hvilke krav for behandling av personopplysninger som følger av personopplysningsloven med forskrifter.**

#### 1 INTERNKONTROLL – INNLEDNING

Det er vanlig å dele opp oppgavene på følgende måte:

Styrende elementer – handler om de beslutninger og føringer ledelsen i en virksomhet er ansvarlig for.

Gjennomførende elementer – gjelder hvilke rutiner som må etableres for de ansattes håndtering av personopplysninger.

Kontrollerende elementer – Rutiner for å fange opp brudd på retningslinjene.

Personvernlovgivningen stiller krav om at dokumentasjon av at ovennevnte rutiner er på plass.

#### 2. INNLEDENDE OPPGAVER FOR INTERNKONTROLL

Ledelsen må ha kunnskap om regelverket:

Det må utpekes hvem som er behandlingsansvarlig.

Det bør etableres prosjekt for å innføre internkontroll.

Det må foretas en kartlegging av hvordan personopplysningene behandles i virksomheten.

Det må etableres kontroll av at virksomhetens behandling av personopplysningene til enhver tid er lovlig.

#### 3. RUTINER FOR INTERNKONTROLL

Det må etableres:

Rutiner for iverksettelse av behandling av personopplysninger.

Rutiner for opphør av behandling.

Rutiner for sletting.

Rutiner for utlevering til andre.

Rutiner for kvalitetssikring.

Rutine for samtykke/innmeldingsprosedyre.

Rutiner for informasjon til den registrerte.

Rutiner for innsyn, retting og supplering av personopplysninger

#### 4. INFORMASJONSSIKKERHET

Dette blant annet om såkalt konfidensialitet – altså at uvedkommende ikke får adgang til personopplysninger:

Tilgjengelighet – hvem skal ha tilgang på opplysningene

Hva er akseptabelt risikonivå – her må det foretas:

Risikovurdering:

Uønskede hendelser.

Konsekvenser av uønskede hendelser.

Sannsynlighet for uønskede hendelser.

Vurdering av beskyttelsesbehov.

Hva er akseptabel risiko.

Hvilke rutiner for informasjonssikkerhet skal man ha.

Hvilke tiltak skal iverksettes.

## 5. OPPFØLGING

Hvordan håndtere avvik/brudd på rutinene.  
Hvilke kontrollrutiner har virksomheten.  
Hvordan skal uønskede hendelser rapporteres.

## 6. OPPLÆRING AV BRUKERNE

Det må etableres systemer for opplæring av de som har ansvar for å behandle personopplysninger.