Policy for Personvern

Innhold

1. Bakgrunn og formål med dokumentet

Policy for Personvern skal sikre styring av risiko knyttet til personvern, sikre etterlevelse av personopplysningsloven og GDPR og bidra til konsernets måloppnåelse.

2. Oppdatering av dokumentet

Styret skal hvert andre år gjennomgå og godkjenne Policy for Personvern. Styrets vurdering og konklusjon skal være nedfelt i styrereferatet. Forut for styrebehandlingen skal Policy for Personvern risiko vurderes av Balanse- og risikostyringskomiteen. Direktør Risikostyring og etterlevelse, innstiller ovenfor styret. Det er Risikostyring og etterlevelse som eier og har ansvaret for å oppdatere Policy for Personvern.

Administrerende direktør er ansvarlig for at policyen behandles i døtrenes styrer i etterkant av styrebehandling i konsernstyret.

3. Virkemåte

Policy for Personvern gjelder for hele konsernet. Ved implementering i bankens datterselskaper skal rammeverket implementeres i størst mulig grad, imidlertid hensyntatt det enkelte datterselskaps størrelse og risikobilde. Alle formelle lov- og forskriftskrav til virksomhetene skal oppfylles.

4. Forhold til annet særlig relevant regelverk

Det er en forutsetning at all lovgivning som konsernet er underlagt følges. Videre skal konsernet følge de til enhver tid gjeldende vedtekter, og vedtak fastsatt av styret. Enhver overskridelse i forhold til styrevedtatte rammer skal rapporteres uten unødig opphold til administrerende direktør og styret, i tillegg til annen etablert rapporteringslinje som skissert under avsnittet Kontrollmiljøet.

Denne policyen er underordnet Policy for Compliancerisiko.

Policyen må ses i sammenheng med bl.a. følgende myndighetskrav og retningslinjer:

- Personvernforordning (GDPR)
- Personopplysningsloven med forskrifter
- Datatilsynets retningslinjer for behandling av personopplysninger
- Markedsføringsloven
- Lov om elektronisk kommunikasjon
- Hvitvaskingsregelverket
- Policy for informasjonssikkerhet

5. Risikostrategi og -profil

Det skal etableres en overordnet risikostrategi og mer spesifikke risikostrategier for ulike risikokategorier konsernet er eksponert for. Risikostrategien er styrets overordnede retningslinje for konsernets risikoappetitt og skal gi en oversikt over risikoen konsernet er villig til å akseptere for å realisere sine målsetninger. Risikoappetitten skal defineres både gjennom risikoutsagn og risikorammer som er

knyttet opp mot ulike risikokategoriene. Risikostrategiene skal revurderes årlig eller når andre forhold tilsier det. Risikoprofilen på personvern skal være lav og er konkretisert gjennom prinsippene for personvern. Disse er beskrevet i veileder fra Datatilsynet og skal være retningsgivende for behandling av personopplysninger i selskapene i SpareBank 1 Østfold Akershus.

5.1 Personvernprinsippene

Behandling av personopplysninger må være lovlig, rettferdig og transparent.

- Formålsbegrensning - Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål

- Dataminimering - Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere innsamlingsformålet.

- Riktighet - Personopplysninger som behandles skal være korrekte. Opplysningene skal også oppdateres hvis det er nødvendig.

- Lagringsbegrensning - Prinsippet om lagringsbegrensning innebærer at personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble innhentet for.

- Integritet og konfidensialitet - Personopplysninger skal behandles slik at opplysningenes integritet og konfidensialitet beskyttes.

- Ansvarlighet - Prinsippet om ansvarlighet understreker den behandlingsansvarliges ansvar for å opptre i samsvar med reglene for behandling av personopplysninger

5.2 Databehandler og behandlingsansvarlig

I hovedsak er SØA behandlingsansvarlig etter lov om behandling av personopplysninger.

SpareBank 1 Østfold Akershus opptrer i noen tilfeller som databehandler på vegne av SamSpar banker eller som har inngått avtale om utkontraktering.

Som behandlingsansvarlig skal SØA ivareta personvernet til egne ansatte, kunder og andre personer tilknyttet SØA (samlet benevnt som «den Registrerte»). Alle personopplysninger om «den Registrerte» vil bli behandlet i samsvar med risikovurdering og bransjestandard for informasjonssikkerhet, og i full overensstemmelse med alle gjeldende lover og regler knyttet til behandling av personopplysninger.

Det samles ikke inn personopplysninger ut over informasjon som «den Registrerte» frivillig gir fra seg, eller der «den Registrerte» gir fullmakt til SØA, slik at SØA kan samle inn slik informasjon.

Samtlige personopplysninger «den Registrerte» gir fra seg på denne måten, vil utelukkende bli brukt av SØA og SØAs samarbeidspartnere/produktselskaper i samsvar med formålet med innsamlingen.

Dersom opplysninger/dokumenter som sendes til SØA inneholder informasjon som er unødvendig for saksbehandlingen, skal det etter retningslinjer gitt av Datatilsynet slettes eller sendes tilbake.

Personopplysninger skal behandles på en sikker måte, se eget kapittel om datasikkerhet.

Når det benyttes underleverandør for databehandlingen skal det inngås databehandleravtale som skal beskrive behandlingsansvarliges krav, kreve samsvar med disse, kreve sikringstiltak i tråd med risikovurdering og bransjestandard, og pålegge leverandørens leverandører tilsvarende krav.

5.3 Innhenting av personopplysninger

SØA innhenter personopplysninger fra kunder i kraft av avgitt samtykkeerklæring og fullmakt i den kanal kunden benytter. Personopplysninger innhentes fra ansatte i kraft av ansettelsesavtale og samtykke. Den Registrerte skal informeres om hvilke opplysninger som registreres, hvem som får tilgang til dem, den registrertes rettigheter, og hvor den registrerte skal henvende seg for spørsmål om databehandlingen, innsyn, retting eller sletting. Når behandlingsgrunnlaget er samtykke, skal det informeres om hvordan samtykket kan trekkes tilbake. Personvern skal være innebygget i alle løsninger som behandler personopplysninger og standardvalget skal alltid gi best mulig beskyttelse av den registrertes personopplysninger. Ref. personvernerklæring for kunder og personvernerklæring for ansatte.

5.3.2 KI kunstig intelligens

Banken benytter kunstig intelligens (KI) i flere operasjonelle aktiviteter og utvidet bruk vil forutsette i stor utstrekning. Banken har blant annet tatt i bruk og gitt alle ansatte tilgang til å benytte Microsoft- copilot.

Det samles inn og benyttes store mengder data for at det skal kunne tas intelligente avgjørelser. Potensialet for bedre tjenester og økonomisk gevinst setter derfor KI høyt på agendaen.
Ved utvikling av systemer og tjenester hvor det benyttes KI skal det sikres og besørges at personverninteressene blir ivaretatt.

5.4 Behandling av personopplysninger

Behandling av personopplysninger er regulert av «Lov om behandling av personopplysninger». De personopplysninger som innhentes dersom en kunde henvender seg om banktjenester, skal være nødvendige for at SØA skal kunne gi tilbud, administrere tjenester, oppfylle SØAs avtaleforpliktelser, og for øvrig kundenes ønsker. Opplysningene vil kunne bli benyttet for å vurdere og fatte beslutninger om kundens behov av tjenester. «Den Registrerte» kan reservere seg mot automatisk behandling.

Anonymiserte og pseudonymiserte personopplysninger kan benyttes for å utarbeide rapporter og markedsanalyser. Ved anonymiseringen skal prosessen dokumenteres.

Dersom SØA har opplysningsplikt overfor offentlig myndighet gjennom lovverket, vil opplysninger bli overlevert i henhold til myndighetenes krav. SØA har plikt til å gjennomføre visse kontrolltiltak regulert av «Lov om tiltak mot hvitvasking og terrorfinansiering mv». (Hvitvaskingsloven).

SØA skal informere «den Registrerte» når overlevering av opplysninger kan finne sted.

Personopplysninger som SØA behandler skal beskrives i en egen behandlingsoversikt. Behandlingsoversikten angir behandlingsgrunnlag, opplysningenes opphav, hvordan de behandles, behandling utenfor EU/EØS, grunnlaget for risikovurderingen og hvilket program for sletting som er anvendt. Ved endringer i behandlingen av personopplysninger skal det alltid foretas en risikovurdering.

5.5 Lovlig behandlingsgrunnlag

Behandlingsgrunnlag er det rettslige grunnlaget som gir SØA rett til å behandle personopplysninger. Behandling av personopplysninger skal alltid være basert på et av følgende behandlingsgrunnlag:

Samtykke: den Registrerte har gitt klart og tydelig aksept for behandling av deres personopplysninger. Det skal informeres om at samtykke fritt kan trekkes tilbake. Samtykke skal dokumenteres.

Samtykket skal tilfredsstille samtlige av følgende krav:

- Informert: det vil si at det tydelig skal fremgå hva det samtykkes til
- Frivillig: det vil si at det ikke foreligger fordeler eller ulemper knyttet til samtykke
- Spesifikt: det vil si at samtykke må være konkret for behandlingen det samtykkes til
- Utvetydig: det vil si at samtykke aktivt må avgis
- Gitt gjennom en aktiv handling
- Dokumenterbart
- Mulig å trekke tilbake like lett som det ble gitt

Avtale: behandlingen er nødvendig for å kunne effektuere en avtale med den registrerte, eller fordi den registrerte har bedt SØA om å gjøre handlinger før avtalen inngås.

Rettslig forpliktelse - (POL Artikkel 6 c) : behandlingen er nødvendig for å etterleve lover og reguleringer. Dette gjelder for eksempel lønnsinnberetning.

Vitale interesser: behandlingen er nødvendig for å beskytte noens liv eller det er fare for helse.

Offentlig oppgave: behandlingen er nødvendig for å utføre oppgaver på vegne av offentlige interesser og dette har klar forankring i loven.

Berettiget Legitime interesser, (POL Artikkel 6F): behandlingen er nødvendig for at SØA skal kunne utøve sine legitime interesser. Legitime interesser skal i forbindelse med personvern kunne begrunnes med rettsregler. SØA`s interesse for behandling av personopplysninger avveies mot den registrertes rett til personvern.

5.6 Innsyn og retting

I henhold til personopplysningsloven har man krav på innsyn i de opplysninger som er registrert. «Den Registrerte» kan benytte seg av sin rett til å få tilgang til, korrigere, komme med innvendinger mot eller slette personopplysninger ved henvendelse til SØA. Opplysningene skal overleveres til «den Registrerte» på en sikker måte.

SØA skal informere om konsekvensene av forespørselen på et entydig og lettfattet språk.

Identiteten på «den Registrerte» skal alltid kontrolleres før forespørselen utføres. Henvendelsen må inneholde personnummer, samt «den Registrertes underskrift». Dersom de registrerte opplysninger ikke er riktige eller de er ufullstendige, kan man kreve disse rettet i henhold til personopplysningsloven.

Forespørsler fra «den Registrerte» om informasjon, innsyn, retting og sletting av personopplysninger skal vurderes av SØAs Personvernombud.

5.7 Oppbevaring og sletting

I henhold til personopplysningsloven skal opplysninger som ikke lenger er nødvendig ut fra det formål de er lagret for slettes. SØA har etablert egen rutine for sletting av personopplysninger

som bygger på gjeldende rutine utarbeidet i alliansen om sletting. Databehandleravtaler forplikter leverandører og underleverandører til å følge dette.

Sletting av personopplysninger – «Retten til å bli glemt»

Sletting skal skje når:

* Opplysningene ikke lenger er nødvendig for å oppnå formålet med behandlingen

* Samtykket til behandlingen er trukket tilbake og det ikke finnes et annet rettslig grunnlag for behandlingen

* Den registrerte har fremsatt en berettiget innsigelse, for eksempel at vedkommende ikke ønsker direkte markedsføring

* Personopplysninger er blitt behandlet på en måte som ikke er lovlig

* Sletteplikten gjelder ikke dersom videre behandling er nødvendig for at den behandlingsansvarlige skal oppfylle en rettslig forpliktelse med den registrerte.

5.8 Reservasjon (Markedsføring)

I henhold til Markedsføringsloven § 13 kan de registrerte reservere seg mot direkte markedsføring fra SpareBank 1 Østfold Akershus og våre samarbeidspartnere.

5.9 Elektronisk kommunikasjon

Hvis behandlingen baserer seg på samtykke eller kontrakt, og behandlingen utføres automatisk, har «den Registrerte» rett til å motta opplysninger om seg selv som han eller hun selv har gitt til den behandlingsansvarlige samt å overføre disse til andre.

Opplysningene skal være i et strukturert, alminnelig anvendt og maskinlesbart format.

«Den Registrerte» har rett til å få overført personopplysningene direkte fra en behandlingsansvarlig til en annen i den utstrekning det er teknisk mulig. Databehandleravtalen bør bestemme vilkårene og prosedyrene for overføring av personopplysninger.

Cookie samtykke
Bruk av informasjonskapsler (cookies) og lignende sporingsteknologier, krever et samtykke som er gyldig etter personvernregelverket. Det betyr blant annet at samtykket skal være frivillig, spesifikt, informert og utvetydig.

Ekomloven § 3-15 bestemmer at bruk av informasjonskapsler (cookies) og lignende teknologier krever et forhåndssamtykke som er gyldig etter *personvernforordningen*. Dette innebærer at internettbrukere i Norge får et sterkere vern mot *sporing* på nett.

5.10 Brudd på personopplysningssikkerheten og varsling

I tilfellet det skjer brudd på personopplysningssikkerheten skal SpareBank 1 Østfold Akershus (SØA), uten opphold undersøke hvor stor sannsynlighet og risiko bruddet har på den Registrertes rettigheter og frihet, f.eks. tap av kontroll over egne personopplysninger eller skade på omdømme.

Dersom det er sannsynlig at bruddet medfører risiko for den Registrertes rettigheter og frihet skal bruddet uten opphold og senest innen 72 timer rapporteres til Datatilsynet.

I de tilfeller der SØA ikke selv er behandlingsansvarlig, og dersom det er høy sannsynlighet for at bruddet medfører risiko for den Registrertes rettigheter og frihet skal bruddet uten opphold og senest innen avtalt frist, rapporteres til den behandlingsansvarlige om de registrerte som er involvert. Det skal informeres om strakstiltak for skadebegrensning.

Varslingen skal utføres i tråd med dokumentert prosedyre og i henhold til databehandler avtale med den behandlingsansvarlige. Det skal dokumenteres relevante beredskapsplaner for brudd på informasjonssikkerheten og personopplysningssikkerheten.

5.11 Datasikkerhet

Data avgitt til SØAs systemer skal overføres, lagres og behandles på en sikker måte. Sikringstiltakene skal ta utgangspunkt i bransjestandard, kundekrav og risikovurderinger, som er ivaretatt gjennom SØAs policy, rutiner og retningslinjer for Informasjonssikkerhet. Beskyttelse av personvern og informasjonssikkerheten er underlagt SØAs retningslinjer for internkontroll. SØAs retningslinjer for informasjonssikkerhet bestemmer rammene for sikringstiltak.

SpareBank 1 har et eget styringssystem for informasjonssikkert (ISMS) basert på ISO/IEC 027001. I styringssystemet finnes alle dokumenter som er relevante for informasjonssikkerheten i deres forhold til hverandre og med lenker til de ulike dokumenter som blant annet IT-arkitektur i Alliansesamarbeidet – Policy (gjelder bare for Banksamarbeidet), IT-Strategi, Konunitetsledelse, Krise og konunitet – Policy, samt Sikkerhetspolicy som er det grunnleggende styringsdokumentet for all behandling av informasjon i SpareBank 1-alliansen.

5.12 Kategorier av personopplysninger

Personopplysninger

Etter personvernforordningen er personopplysninger definert som enhver opplysning og vurdering som kan knyttes til en enkeltperson. I SØA er personopplysninger delt inn i tre kategorier:

* Nøytrale personopplysninger
* Dybde personopplysninger
* Særlige kategorier av personopplysninger

Det er definert fire beskyttelsesklasser for informasjon, som følger av Standard for klassifisering av informasjon:

- Åpen informasjon. Dette er informasjon som er offentlig, og kan deles fritt med alle både innenfor og utenfor SpareBank 1-alliansen
- Intern informasjon. Dette er informasjon som er åpen for alle ansatte, vikarer og innleide, og kan fritt deles mellom medarbeidere i et eller flere selskaper i SpareBank 1-alliansen.
- Fortrolig informasjon. Dette er informasjon som trenger beskyttelse og kun være tilgjengelig for store eller små grupper.
- Strengt fortrolig informasjon. Dette er informasjon som har et høyt behov for beskyttelse, og som kun er tilgjengelig for en svært begrenset gruppe ansatte.

MERK

- ✓ *Personopplysninger kan finnes i alle de fire klassene, men særlige kategorier av personopplysninger bør være klassifisert som begrenset eller strengt fortrolig.*

- ✓ *Datatilsynet har uttalt at fødselsnummer er en personopplysning hvor konfidensialitet er nødvendig og at fødselsnummer derfor må sendes på en sikker måte slik at fødselsnummeret ikke er tilgjengelig for andre enn adressaten, for eksempel ved bruk av kryptering.*

Nøytrale personopplysninger

Med nøytrale kundeopplysninger menes navn, adresser, fødselsdato, i hvilke av selskapene kunden har sitt avtaleforhold og hvilke produkter som er en del av kundeforholdet.

Nøytrale kundeopplysninger kan utveksles mellom finansforetak i samme konsern og i SØA, uten at det må innhentes skriftlig samtykke fra kundene.

Dybdeopplysninger

Mer detaljerte opplysninger utover nøytrale kundeopplysninger regnes som dybdeopplysninger. Dette kan for eksempel være betalingsvilje og –evne, informasjonskapsler og informasjon om aktivitet på nett og inntekt.

Særlige kategorier av personopplysninger

Personvernforordningen artikkel 9 definerer særlige kategorier av personopplysninger til å omfatte:

- rasemessig eller etnisk opprinnelse
- politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap
- genetiske opplysninger
- biometriske opplysninger
- helseopplysninger og
- opplysninger om en persons seksuelle forhold eller seksuelle orientering

Lovbestemmelsene som er knyttet til håndtering av særlige kategorier av personopplysninger skal avspeiles i behandlingsrutinene.

Det er egne regler for personopplysninger som omhandler straffedommer og lovovertredelser. I praksis må slike personopplysninger behandles som særlige kategorier av personopplysninger.

6. Rammeverk for styring og kontroll av personvern

Konsernet har valgt å standardisere prosessen knyttet til håndtering av Personvern. Dette skal sikre effektivitet og kvalitet i prosessen. Prosessen knyttet til håndtering av Personvern er bygd opp rundt følgende elementer:

1. Kontrollmiljøet
2. Identifisere personvern og GDRP risiko
3. Vurdere personvern og GDPR risiko
4. Risikostyringsstrategier
5. Kontrollkartlegging og -vurdering

6. Overvåking og oppfølging
7. Rapportering
8. Kontinuerlig forbedring

Innenfor hvert av elementene er det definert et sett prinsipper for hvordan prosessen skal gjennomføres. Disse elementene er beskrevet under.

6.1 Kontrollmiljøet

Ansvar og organisering er personvern

Sparebank 1 Østfold Akershus (SØA) kan være både behandlingsansvarlig og databehandler, dette varierer avhengig av rolle. SØA er ansvarlig for at behandling av personopplysninger er i tråd med lover og regler. Roller, ansvar og oppgaver knyttet til personvern følger organisasjonsstrukturen**.**

Alle ansatte som har tilgang til og som behandler personopplysninger, skal ha nødvendig kunnskap og opplæring for å kunne etterleve lover og forskrifter.

SpareBank 1 Østfold Akershus som omfatter bankvirksomhet skal ha eget personvernombud. Det skal settes av tilstrekkelige ressurser for at personvernombudet kan utføre sine oppgaver. Det er utarbeidet en egen instruks for personvernombud i tråd med personopplysningsloven. Personvernombudet skal være ansvarlig for kontakten med Datatilsynet og sentral personvernrådgiver i SamSpar.

Roller og ansvar for de ulike organisasjonsnivåene er definert i Policy for risiko- og kapitalstyring, se vedlegg 3 Roller og Ansvar.

6.2 Identifisere risiko

Følgende prinsipper skal legges til grunn for å identifisere selskapets risiko knyttet til avvik på personvernregelverket:

SØA som behandlingsansvarlig og databehandler skal, i samråd med personvernombudet, utviklingsprosjekter og andre ansvarlige, sørge for at det blir gjennomført risikovurderinger med fokus på forhold som kan påvirke sikkerheten (konfidensialitet, integritet og tilgjengelighet) knyttet til personopplysninger som blir behandlet. Formålet med risikovurderingen er å sikre at den risikoen som avdekkes ved behandling av personopplysninger er innenfor akseptabelt nivå.
SpareBank 1 sin prosess og metode for risikostyring av informasjonssikkerhet er nærmere beskrevet i Standard for risikostyring av informasjonssikkerhet.

Følgende prosesser for identifikasjon av risikoer for avvik på personvernregelverket:

#	Handling:	Ansvarlig:	Frekvens:
1	Kartlegging av etterlevelse av POL i forbindelse med årlig lederbekreftelse.	Avdeling Risikostyring og etterlevelse	Årlig
2	Kartlegging av etterlevelse av POL – AFR rådgivere i forbindelse med lederbekreftelsen	Avdeling Risikostyring og etterlevelse	Årlig

#	Handling:	Ansvarlig:	Frekvens:
3	Risikoanalyse POL inkludert i ROS analysen	HR med bistand fra Risikostyring og etterlevelse	Årlig
4	Gjennomgang av uønskede hendelser – (Betr)	Risikostyring og etterlevelse	Løpende
5	Gjennomgang av behandlingsoversikten	Personvernombudet/ Risikostyring og etterlevelse	Årlig
6	Identifisere og dokumentere risikoer knyttet til personvernregelverket ved nye og endringer av tjenester, produkter, prosesser, systemer og leverandører/utkontrakterte tjenester.	Personvernombudet/ Risikostyring og etterlevelse	Ved behov

6.3 Vurdere risiko for avvik knyttet til personvernregelverket

Følgende prinsipper skal legges til grunn for å vurdere risiko for avvik på personvernregelverket.

- Vurderingen skal bygge på identifiseringen av risiko og danne grunnlag for hvordan konsernet skal forstå og styre risikoene.
- Alle risikoer skal i størst mulig grad vurderes og dokumenteres. Vurderingene skal være både kvantitativt og kvalitativt.

- Vurderingene skal ta utgangspunkt i «sannsynligheten» for at risikoen blir en utfordring og mulige «konsekvens» av det.

- Vurderingene skal bidra til at det foretas en kvalifisert og strukturert vurdering og dokumentasjon av de kontroll- og styringstiltak som er etablert, og om disse tiltakene er forsvarlig ivaretatt i virksomhetene.

Følgende prosesser for vurdering av risiko for avvik knyttet til personvernregelverket skal gjennomføres:

#	Handling:	Ansvarlig:	Frekvens:
1	Vurderer funn i ROS-analysen	Risikostyring og etterlevelse	Årlig
2	Vurdere funn i kartlegging som gjennomføres årlig i forbindelse med lederbekreftelsen.	Risikostyring og etterlevelse	Årlig
3	Vurdere funn i årlig kartlegging POL som besvares av AFR rådgivere i forbindelse med lederbekreftelsen	Risikostyring og etterlevelse	Årlig
4	Vurdere risiko knyttet til risikoscoring av eksisterende og nye produkter, tjenester, systemer og prosesser	Personvernombudet/Risikostyring og etterlevelse	Ved behov
5	Uønskede hendelser (Betr) og avvik som treffer POL, og vurdere melding til Datatilsynet	Personvernombudet/Risikostyring og etterlevelse	Løpende

6.4 Risikostyringsstrategier

Risikostyringsstrategiene skal bygge på vurderingene av risikoene og sikre at selskapet styrer risikoene i tråd med akseptable og godkjente risikoprofiler, slik at samlet risikoeksponering er i samsvar med selskapets overordnede risikoprofil.

I hovedsak kan fire ulike risikostyringsstrategier benyttes:

- Unngå
- Redusere
- Beholde
- Øke

Følgende prinsipper skal legges til grunn ved valg av risikostyringsstrategi:

- Risikostyringsstrategiene skal gjenspeile selskapets overordnede mål og strategier.
- Risikostyringsstrategiene skal være en integrert del av selskapets løpende aktiviteter.
- Risikostyringsstrategiene må stå i forhold til selskapets vilje.

Følgende prosesser for risikostyringsstrategier skal gjennomføres:

#	Handling:	Ansvarlig:	Frekvens:
1	Ved gjennomføring av årlig kartlegging og risikoworkshop skal det utarbeides og iverksettes tiltak for de største risikoene som blir avdekket.	Ledere/Risikostyring og etterlevelse	
2	Risikovurdering av eksisterende, endrede og nye produkter, tjenester, systemer og prosesser	Personvernombud/ Risikostyring og etterlevelse	
3	Løpende oppfølging av uønskede hendelser som treffer POL/GDPR for vurdering og melding til Datatilsynet.	Personvernombud/ Risikostyring og etterlevelse	
4	Bruk av felles personvernrådgiver i SamSpar i saker som treffer SØA og SamSpar bankene.	Personvernombudet	

6.5 Kontrollkartlegging og -vurdering

Kontrollkartleggingen skal bygge på vurderingene og risikostyringsstrategiene og danne grunnlag for at selskapet har hensiktsmessig styring og kontroll på personvernrisiko.

Følgende prinsipper skal legges til grunn ved identifisering og vurdering av kontrolltiltak:

- Kontrolltiltak skal dokumenteres for å sikre åpenhet og kjennskap til kontroller.

- Kontrollene skal kategoriseres i en av følgende kategorier: forebyggende og manuelle, forebyggende og automatiske, avdekkende og manuelle og avdekkende og automatiske.

- Kontroller skal vurderes ut fra hvor dekkende og effektive de er i forhold til de risikoene som skal styres og kontrolleres.

Følgende prosesser for identifisering og vurdering av kontrolltiltak skal gjennomføres:

#	Handling:	Ansvarlig:	Frekvens:
1	For de vesentligste risikoene som konsernet er eksponert for skal det gjøres en kartlegging og vurdering av tilhørende kontrolltiltak.	Risikostyring og etterlevelse	Årlig
2	For nye risikoer som konsernet er eksponert for skal det gjøres en kartlegging og vurdering av tilhørende kontrolltiltak.	Ledere, prosesseiere, fagansvarlige, produktansvarlige, Personvernombud, Risikostyring og etterlevelse	Løpende
3	For risikoer knyttet til eksisterende, endrede og nye tjenester, produkter, prosesser, systemer og leverandører/utkontrakterte tjenester skal det gjøres en kartlegging og vurdering av tilhørende kontrolltiltak.	Personvernombud/Risikostyring og etterlevelse	Løpende

6.6 Oppfølging og overvåking

Formålet med oppfølgingen er å vurdere om selskapets risikoeksponering er i henhold til risikostyringsstrategien og om nødvendige tiltak blir iverksatt og gjennomført på en tilstrekkelig måte. Det er også en hensikt å vurdere hvor effektiv prosessen knyttet til risiko for avvik iht. personvernregelverket er over tid, og sikre at nødvendige handlinger eller endringer blir gjennomført.

Følgende prinsipper skal legges til grunn for oppfølging og overvåking:

- Status risikorammer og måltall skal rapporteres kvartalsvis i risikorapporten.

- Den etablerte prosessen knyttet til avvik iht. personvernregelverket og gjennomføringen av den skal løpende følges opp. Oppfølgingen av de viktigste risiko skal være del av den løpende virksomheten, så vel som periodiske evalueringer utført av fagområdene. Herunder inkluderes periodiske aktiviteter som blant annet kontrollplaner.
- Uønskede hendelser skal registreres og rapporteres.

- Svakheter i prosessen knyttet til avvik iht. personvernregelverket skal uten unødig opphold rapporteres til relevant ledelsesnivå. Svikt av vesentlig betydning skal rapporteres til ledelsen og styret.

6.7 Rapportering

Følgende prinsipper skal legges til grunn for rapportering:

- Selskapets styre og ledelse skal få tidsriktig informasjon om de strategier og retningslinjer som er vedtatt blir fulgt.

- Rapportering knyttet til avvik på Personvernregelverket skal sikre at alle relevante organisasjonsnivåer har tilgang på tilstrekkelig, pålitelig og relevant informasjon om aktuelle avvik og eventuelle avdekkede svakheter i prosessen for håndtering av personvern slik at det kan iverksettes hensiktsmessige tiltak til å forbedre selskapet.

- Ledere skal for sine respektive ansvarsområder rapportere oppover i organisasjonen hvordan risikostyringen er gjennomført i forhold til godkjent rammeverk og risikoeksponering. Dette skal gi administrerende direktør og styret tilstrekkelig materiale for å ta stilling til om håndtering av personvernregelverket er forsvarlig ivaretatt. Rapporteringen innarbeides i internkontrollrapporten/lederbekreftelsen.

Følgende prosesser for rapportering skal gjennomføres:

#	Rapport	Ansvarlig	Frekvens:	Mottaker:
1	Risikorapport	Ansvarlig for Risikostyring og etterlevelse	Kvartalsvis	Styret
2	Internkontrollrapport/lederbekreftelsen	Ansvarlig for Risikostyring og etterlevelse og administrerende direktør	Årlig	Styret

6.8 Kontinuerlig forbedring

Prosessen knyttet til Personvernregelverket skal bidra til kontinuerlig forbedring gjennom løpende forbedret risikohåndtering, styring og kontroll og prosessendringer. Første forsvarslinje for risikostyring og etterlevelse har det løpende ansvaret for dette. Andre forsvarslinje for risikostyring og etterlevelse skal følge opp konsernets vesentligste risikoer og de største kontrollgapene slik at disse kommer innenfor selskapets ønskede grenser.

Følgende prinsipper skal legges til grunn for kontinuerlig forbedring:

- Det skal gjennomføres en effektiv prosess for oppfølging av avvik på personvernregelverket identifisert gjennom internkontrollprosessen inkludert prosessen knyttet til risikoscoring av nye produkter, tjenester, systemer og prosesser og hendelsesrapportering. Læring skal være en viktig del av prosessen.

Revidering og endringer

Versjonskontroll:

Versjon:	Endring:	Ansvarlig:	Styregodkjent:
1.0	Opprettet policy	Gro Østerud	12.06.2019
1.1	Omhandler hele konsernet	Annicken S. Herje/Gro Østerud	10.02.2020
2.0	Ny mal	Gro Østerud	27.10.2021
2.1	Årlig oppdatering	Annicken S. Herje/Gro Østerud	21.11.2022
2.1	Årlig oppdatering	Annicken S. Herje	21.11.2022
2.2	Årlig oppdatering	Gro Østerud og Annicken S Herje	2023
2.2.1	Årlig oppdatering	Annicken Herje S.	2023
2.3	Årlig oppdatering	Gro Østerud og Annicken S. Herje	12.11.2024
2.4	Tilføring av punkt 5.9 Elektronisk kommunikasjon	Gro Østerud og Annicken S. Herje	19.11.2025

Vedlegg

Definisjoner

Ord / uttrykk	Definisjon
Internkontroll:	En kontinuerlig prosess, iverksatt, gjennomført og overvåket av selskapets styre, ledelse og øvrige ansatte. Internkontrollen utformes for å gi rimelig sikkerhet for måloppnåelse innen følgende områder: målrettet, effektiv og hensiktsmessig drift, pålitelig intern og ekstern rapportering, overholdelse av lover og regler, samt interne retningslinjer.
Kompleksitet:	Hvor komplekst det er å etterleve kravet. Kompleksiteten vurderes ut fra både finansielle, operasjonelle og strategiske implikasjoner.
Konsekvens:	Hvilken innvirkning en gitt hendelse (f.eks. manglende etterlevelse av krav knyttet til Personvernregelverket) har for selskapet om denne inntreffer. Enkelte hendelser kan ha innvirkning på flere av selskapets prosesser, avdelinger etc.
Måltall:	Uttalt mål selskapet skal tilstrebe å nå. Ikke absolutt grense.
Policy:	Policy beskriver grenser for hva som er akseptabelt innenfor gitte områder i selskapet. Policyer skal sikre at selskapet opptrer ensartet og i tråd med eksterne rammebetingelser (lover og regler) og internt definert risikonivå (risikoeksponering, kvalitet etc.).
Prosess:	En strukturert og målbar flyt av aktiviteter som har som formål å produsere et resultat til en spesifikk kunde internt eller eksternt.
Risiko:	Forhold som kan hindre selskapet i å nå sine målsettinger inklusive risikoen for å påføre selskapet økonomisk eller annen form for tap.
Risikostyring:	En prosess gjennomført av virksomhetens styre, ledelse og ansatte. Prosessen anvendes i fastsettelse av strategi og på tvers av virksomheten. Den er utformet for å identifisere potensielle hendelser som kan påvirke virksomheten og for å håndtere risiko slik at den er i samsvar med virksomhetens risikotoleranse. Dette skal gi rimelig grad av sikkerhet for virksomhetens måloppnåelse.
Strategi:	Overordnet beskrivelse av hva selskapet skal prioritere for å nå sine målsettinger.