Utdrag av Policy for Personvern GDPR

Innhold

Innledning.

Dette dokumentet inneholder et sammendrag av hovedpunktene i bankens Policy for Personvern. Fullstendig versjon av dokumentet er kun tilgjengelig internt i banken.

Policy for Personvern revideres årlig. Gjeldende versjon ble vedtatt av bankens styre den 27.10.2021.

Bakgrunn og formål med dokumentet

Oppdatering av dokumentet

Styret skal en gang per år gjennomgå og godkjenne policy for personvern GDPR.

Virkemåte

Policy for Personvern GDPR 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.

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.

Denne policyen er underordnet Overordnet 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.

Risikostrategi og -profil

Risikoprofilen på personvern GDPR, er konkretisert gjennom prinsippene for personvern. Disse er beskrevet i veileder fra Datatilsynet og skal være retningsgivende for behandling av personopplysninger i selskapene i SpareBank1 Østfold Akershus.

Personvernprinsippene:

- Behandling av personopplysninger må være lovlig
- 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

Ansvar og organisering av personvern

SpareBank 1 Østfold Akershus 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.

Styret er overordnet ansvarlig for behandlingen av personopplysninger. Administrerende direktør er fra administrasjonen ansvarlig for behandling av personopplysninger i SpareBank 1 Østfold Akershus.

SpareBank 1 Østfold Akershus som omfatter bankvirksomhet skal ha eget personvernombud. Det er utarbeidet en egen instruks for personvernombud i tråd med personopplysningsloven.

Databehandler og behandlingsansvarlig

I hovedsak er SpareBank 1 Østfold Akershus behandlingsansvarlig etter lov om behandlingsansvar 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 banken ivareta personvernet til egne ansatte, kunder og andre personer tilknyttet SpareBank 1 Østfold Akershus (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 vedrørende behandling av personopplysninger.

Innhenting av personopplysninger

SpareBank 1 Østfold Akershus 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.

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 SpareBank 1 Østfold Akershus skal kunne gi tilbud, administrere tjenester, oppfylle SpareBank 1 Østfold Akershus 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.

Personopplysninger som SpareBank 1 Østfold Akershus 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.

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 SpareBank 1 Østfold Akershus. Opplysningene skal overleveres til den Registrerte på en sikker måte.

Oppbevaring og sletting

I henhold til personopplysningsloven skal opplysninger som ikke lenger er nødvendig ut fra det formål de er lagret for slettes.

Reservasjon (Markedsføring)

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

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.

Brudd på personopplysningssikkerheten og varsling

I tilfellet det skjer brudd på personopplysningssikkerheten skal SpareBank 1 Østfold Akershus (SpareBank 1 Østfold Akershus), 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.

Datasikkerhet

Data avgitt til SpareBank 1 Østfold Akershus systemer skal overføres, lagres og behandles på en sikker måte. Sikringstiltakene skal ta utgangspunkt i bransjestandard, kundekrav og risikovurderinger, som er ivaretatt gjennom SpareBank 1 Østfold Akershus policy, rutiner og retningslinjer for Informasjonssikkerhet.

Kategorier av personopplysninger

Personopplysninger

Etter personvernforordningen er personopplysninger definert som enhver opplysning og vurdering som kan knyttes til en enkeltperson. I SpareBank 1 Østfold Akershus er personopplysninger delt inn i tre kategorier:

* Nøytrale personopplysninger

* Dybde personopplysninger

* Særlige kategorier av personopplysninger

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 SpareBank 1 Østfold Akershus, 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.

Type risiko

Konsernet har valgt å standardisere prosessen knyttet til håndtering av Personvern og GDPR. Dette skal sikre effektivitet og kvalitet i prosessen. Prosessen knyttet til håndtering av Personvern og GDPR 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.

Kontrollmiljøet

Ansvar og organisering er personvern

Sparebank 1 Østfold Akershus, kan være både behandlingsansvarlig og databehandler, dette varierer avhengig av rolle. SpareBank 1 Østfold Akershus 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.

Styret er overordnet ansvarlig for behandlingen av personopplysninger. Administrerende direktør er fra administrasjonen ansvarlig for SpareBank 1 Østfold Akershus behandling av personopplysninger.

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.

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.