Sparebanken Vest

Datasikkerhet og personvern i Sparebanken Vest

1. Personvern

Informasjonssikkerhet innebærer å beskytte data på en tilfredsstillende måte mot uønskede handlinger eller hendelser. Kravene til konfidensialitet, integritet og tilgjengelighet skal ivaretas.

Konsernet skal ha god og hensiktsmessig styring og kontroll med personvern, og den samlede risikoen for brudd på eksterne og interne regler skal være lav. Det er ingen toleranse for brudd på lov og forskrift foretatt med viten og vilje.

Å hindre at personopplysninger kommer på avveie, er et prioritert område innen vårt arbeid med informasjonssikkerhet. Dette arbeidet er en del av vår personvernstrategi som ble vedtatt av styret i 2018.

Banken vil behandle personopplysninger med formål om å forebygge, avdekke, oppklare og håndtere bedrageri og andre straffbare handlinger rettet mot kunder eller banken. Opplysninger innhentet med dette formål vil også kunne bli innhentet fra og utlevert til andre banker og finansinstitusjoner, politiet og andre offentlige myndigheter. Opplysningene som registreres blir oppbevart inntil ti år etter registreringen.

Banken vil behandle personopplysninger for å forebygge og avdekke transaksjoner med tilknytning til utbytte fra straffbare handlinger eller med tilknytning til terrorfinansiering. Banken har undersøkelses- og rapporteringsplikt for mistenkelige transaksjoner etter hvitvaskingsloven. Banken er videre pålagt til å rapportere mistenkelige opplysninger og transaksjoner til Økokrim. Banken behandler personopplysninger til ulike formål. Formålene er beskrevet i bankens personvernerklæring. Det er for eksempel med formål om å forebygge, avdekke, oppklare og håndtere bedrageri

Les mer om vår personvernerklæring og bruk av informasjonskapsler (Cookies) på bankens nettsider: https://www.spv.no/personvern.

2. Policy for personvern og ansvar

Sparebanken Vests Policy for personvern er forankret hos konsernsjef og skal sikre at banken, på en systematisk måte, sørger for at alle plikter, som følger av fastsatt strategi og lov om behandling av personopplysninger, blir ivaretatt på en definert og systematisk måte.

Konsernsjefen har det daglige ansvaret for etterlevelse av personvernlovgivningen, herunder sikre at «Strategi for behandling av personopplysninger» blir implementert i virksomheten, blant annet gjennom vedtakelsen av «Policy og retningslinjer for behandling av personopplysninger». Konsernsjefen skal rapportere oppfølging av avvik og anbefalinger fra personvernombudet til styret.

Banken har oppnevnt et eget personvernombud, som skal kontrollere overholdelsen av personvernlovgivningen og andre relevante regelverk med personvernbestemmelser, samt virksomhetens egne interne retningslinjer for personvern. Personvernombudet har en selvstendig plikt til å samarbeide med Datatilsynet.

Sparebanken Vest holder seg oppdatert med forskjellige standarder, men har ikke funnet det hensiktsmessig å sertifisere virksomheten til én standard. Sparebanken Vest forholder seg til strenge regulatoriske krav i tillegg til både intern- og eksternrevisjon.

3. Varsling

GDPR-forordningen krever at vi må varsle Datatilsynet innen 72 timer ved persondata på avveie, i tillegg krever Finanstilsynet at vi varsler innen rimelig tid ved alvorlige avvik. Gjør vi vesentlige endringer i Personvernerklæringen er vi pliktig å informere alle kunder om endringen.

Dette er nedfelt i vårt policy-dokument for personvern (policy og retningslinjer for behandling av personopplysninger i Sparebanken Vest).

4. Opplæring

Vi gjennomfører trening, bevisstgjøringstiltak og opplæring for å øke kompetansen om datasikkerhet hos de ansatte, for å minimere risiko regelmessig. Behovet blir hele tiden vurdert opp mot trusselbilde og risiko knyttet mot bankens virksomhet og satsningsområder.

Sammen med automatiserte varslinger rundt potensiell skadelig programvare og phishing, er trening og bevisstgjøring av alle ansatte viktige virkemidler for å øke datasikkerheten og hindre at personopplysninger kommer på avveie.

5. Overvåking

Sparebanken Vest måler og overvåker systemkritiske systemer til enhver tid i tillegg til flere lag av beskyttelse for å unngå lekkasje av data og beskytte data mot innbrudd og for å holde risiko på et akseptabelt nivå.

6. Tredjepartsvurdering og testing

I tillegg til egne kontrollrutiner, blir bankens arbeid med informasjonssikkerhet årlig revidert av ekstern- og internrevisjon (årlig og halvårlig). Det gjøres også periodisk interne risikovurderinger knyttet til GDPR og informasjons-sikkerhet. I tillegg til dette blir det foretatt eksterne penetrasjon- og sikkerhetstester av infrastruktur og egenutviklede løsninger. Alle egenutviklede løsninger må gjennom flere lag med testing før det blir satt i produksjon.

Alle tredjeparter må kunne levere sikkerhetstester og revisjoner som viser at nødvendige sikkerhetstiltak er iverksatt og fungerer etter hensikten. Leverandører definert som systemkritiske for kjernevirksomheten må i tillegg levere ISAE3402 foretatt av uavhengig part årlig.

Databehandleravtaler med tredjeparter regulerer krav i forhold til behandling av persondata på vegne av Sparebanken Vest. Tredjeparter definert som systemkrise blir monitorert og målt opp mot avtalemessige vilkår for tilgjengelighet, konfidensialitet og integritet. I tillegg er det etablert møtepunkt og kontaktpunkter om avvik skulle oppdages for å raskt kunne agere på hendelser. Leverandører må tilfredsstille regulatoriske krav innfor finans, og levere oppdaterte revisjonsrapporter og sikkerhetstester regelmessig.

Finanstilsynet utfører i tillegg tilsyn av IT-området årlig. Etter egen risikovurdering blir det også utført eksterne sikkerhetstester på områder med høy risiko, ofte i samband med utviklingsaktiviteter.