507.04.52 Policy för behandling av personuppgifter

Uppdaterad: 2021-09-30 (ersätter 2020-09-30)

Ändamålet med detta styrdokument är att fastställa hur Sparbankens interna regler, principer och arbetssätt ska skydda hanteringen av kundernas, leverantörernas, anställdas och andra samarbetspartners personuppgifter för att deras grundläggande rättigheter och friheter inte ska utsättas för intrång eller annan olämplig behandling.

Rättslig grund

Policyn baseras på följande externa regelverk:

- Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
- Ny dataskyddslag – SOU 2017:39
- Artikel 29-arbetsgruppen för uppgiftsskydd
- Rätten till dataportabilitet
- Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande huruvida behandlingen ”sannolikt leder till hög risk” i den mening som avses i förordningen
- Riktlinjer om dataskyddsombudet
- Dataskyddsförordningen (GDPR, The General Data Protection Regulation) läs mer om Dataskyddsförordningen (GDPR) på Datainspektionens hemsida www.datainspektionen.se

1. Syfte och bakgrund

Eftersom Leksands Sparbank (”Sparbanken”) som en del av sin vardagliga verksamhet behandlar personuppgifter i stor omfattning, är det viktigt att banken förhåller sig till bestämmelserna i GDPR på ett sätt som tryggar de registrerades grundläggande rättigheter och friheter samtidigt som bestämmelserna i GDPR implementeras på ett ändamålsenligt och effektivt sätt i den dagliga verksamheten. Sparbankens mål är att bestämmelserna i GDPR ska genomsyra hela verksamheten och vara en del av det dagliga arbetet.

Ändamålet med detta styrdokument är att fastställa hur Sparbankens interna regler, principer och arbetssätt ska skydda hanteringen av kundernas, leverantörernas, anställdas och andra samarbetspartners personuppgifter för att deras grundläggande rättigheter och friheter inte ska utsättas för intrång eller annan olämplig behandling. Syftet är att de registrerade skall kunna känna sig trygga med Sparbankens behandling av deras personuppgifter och att denna behandling skall uppfylla de krav som GDPR ställer på banken.

2. Organisation och ansvar

2.1 Styrelsen

Styrelsen ansvarar för upprättandet av policyn i enlighet med Policy för styrdokument (507.04.43). Policyn ska årligen fastställas av Sparbankens styrelse även om inga ändringar

ska beslutas. Styrelsen för Sparbanken är ytterst ansvarig för bankens behandling av personuppgifter och för skyddet av den personliga integriteten hos de vars personuppgifter behandlas av Sparbanken.

2.2 VD

Det åligger Sparbankens VD att tillse att policyn hålls tillgänglig via Sparbankens system för policyer och instruktioner för samtliga som berörs av den. Ansvaret innebär att tillse att anställda, konsulter, samarbetspartners, ombud och uppdragstagare som berörs av policyn, känner till och följer innehållet i dessa.

VD är operativt ansvarig och är därmed ansvarig för att denna policy efterlevs av Sparbankens anställda. VD ansvarar även för den löpande hanteringen av personuppgifter på Sparbanken.

2.3 Personuppgiftsansvarig (Sparbanken)

Den verksamhet som bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till är personuppgiftsansvarig.

Den personuppgiftsansvarige har ett generellt ansvar att, utifrån de integritetsrisker som finns med behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Det är den personuppgiftsansvariga som bär ansvaret för behandlingen av personuppgifter inom den egna verksamheten.

2.4 Personuppgiftsbiträden

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvarige.

De personuppgiftsbiträden som Sparbanken anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställa att den registrerades rättigheter skyddas.

2.5 Sparbankens Dataskyddsombud (DSO)

Kontroll av efterlevnaden av policyn ska ske av Sparbankens dataskyddsombud.

Eftersom skyddet av kundernas personuppgifter är särskilt viktigt har banken en särskilt utsedd funktion som har till uppgift att skydda kunders personliga integritet, ett Dataskyddsombud.

Den övergripande och viktigaste uppgiften för Dataskyddsombudet är att övervaka att Sparbanken följer dataskyddsförordningen. Det innebär bland annat att

- samla in information om hur organisationen behandlar personuppgifter
- kontrollera att organisationen följer bestämmelser och interna styrdokument
- informera och ge råd inom organisationen.

Se Befattningsbeskrivning för Dataskyddsombud.

Sparbankens DSO-funktion rapporterar kvartalsvis, både muntligen och skriftligen till Sparbankens styrelse. Styrelsen fastställer också DSO-funktionens årsplan.

3. Säkerhet

Den som behandlar personuppgifter måste se till att ha en lämplig säkerhetsnivå för uppgifterna, både tekniskt och organisatoriskt. Till tekniska åtgärder räknas punkter som brandväggar, krypteringsfunktioner och anti-virus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation och rutiner, instruktioner och policyer.

All behandling av personuppgifter inom Sparbanken omfattas av Policy för IT- och kommunikationsteknologi (IKT) (507.04.49) och tillhörande instruktioner.

Sparbanken ska vara tydlig med att personuppgifter ska behandlas på ett säkert sätt. Detta gäller för information som är avsedd både för intern och extern behandling.

Utgångspunkten för behandling av personuppgifter på Sparbanken är att endast medarbetare inom organisationen som behöver personuppgifter för att utföra sina arbetsuppgifter ska ha tillgång till dem.

Sparbanken ska också se till att bankens personuppgiftsbiträden kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna. Ett personuppgiftsbiträde får behandla personuppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige och är skyldig att vidta de säkerhetsåtgärder som den personuppgiftsansvarige kräver/instruerar om.

4. Behandling av personuppgifter

4.1 Principer för behandling av personuppgifter

All behandling av personuppgifter i Sparbanken måste uppfylla de grundläggande principer för behandling av personuppgifter som anges i dataskyddsförordningen.

- Laglighet, korrekthet och öppenhet

Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

- Ändamålsbegränsning

Personuppgifter ska bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål.

- Uppgiftsminimering

Principen om uppgiftsminimering innebär att personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

- Korrekthet

Personuppgifterna ska vara korrekta och uppdaterade.

- Lagringsminimering

Personuppgifter får inte sparas, det vill säga förvaras i en form som möjliggör identifiering av den registrerade, under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

- Integritet och konfidentialitet

Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Sparbanken har vidtagit tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

- Ansvarsskyldighet

Den som behandlar personuppgifter ansvarar för att principerna om personuppgiftsbehandling följs och måste kunna visa på vilket sätt man följer dem.

4.2 Rättslig grund för personuppgiftsbehandling

Kravet på att behandlingen av personuppgifter ska vara laglig innebär bland annat att det måste finnas en rättslig grund för behandlingen. De rättsliga grunderna är följande:

- Avtal

Behandling av personuppgifter är nödvändig i bankens verksamhet, för att banken ska kunna fullgöra sina plikter mot kunder och myndigheter. För sådan behandling av personuppgifter krävs inget samtycke från kunder.

- Samtycke

Sparbanken får behandla personuppgifter om banken har ett samtycke från den som personuppgifterna avser.

- Rättslig förpliktelse

Sparbanken får behandla personuppgifter om det är nödvändigt för att uppfylla en rättslig förpliktelse.

- Skydd för grundläggande intressen

Behandling av personuppgifter är tillåten om det är nödvändigt för att skydda intressen som är av grundläggande betydelse för den registrerade eller för någon annan person.

- Allmänt intresse

Behandling av personuppgifter är tillåten om den är nödvändig för att utföra en uppgift av allmänt intresse.

- Intresseavvägning

Det kan vara tillåtet att behandla personuppgifter efter en intresseavvägning. Det krävs då att behandlingen är nödvändig för berättigade intressen och att den registrerades intresse av skydd för sina personuppgifter inte väger tyngre.

4.3 Känsliga personuppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd. Huvudregeln är, att det är förbjudet att behandla känsliga personuppgifter.

Undantag kan förekomma vid uttryckligt samtycke från kund angående uppgifter som kan behövas för vissa produkter, exempelvis försäkringar. Undantag kan också förekomma vid HR-funktionens behandling av personuppgifter. Känsliga personuppgifter är uppgifter om bl.a. etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning.

5. Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel:

- diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning
- finansiell förlust
- brott mot sekretess eller tystnadsplikt.

För att kunna leva upp till de nya skyldigheterna enligt dataskyddsförordningen är det viktigt att Sparbanken har rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.

Hanteringen av personuppgiftsincidenter sker enligt Sparbankens Instruktion för incidenthantering (507.10.28), se regelverket.

6. Definitioner och begrepp

Begrepp	Förklaring
Personuppgifter	varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Behandling	en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
DSO	Data Protection Officer, Dataskyddsombud
GDPR	General Data Protection Regulation 2016/679, dataskyddsförordningen
Personuppgiftsansvarig	en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Personuppgiftsbiträde	en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Samtycke	av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Fastställd av	Fastställd av styrelsen i Leksands Sparbank
Datum för fastställande	2021-09-30
Gäller för	Alla medarbetare
Dokumentägare	Styrelsen
Dokumenttyp	Policy
Instruktionsnummer	507.04.52
Supporterade dokument	Instruktion för behandling av personuppgifter (201.22) Policy för IT- och kommunikationsteknologi (IKT) (507.04.49) Instruktion för IT- och kommunikationsteknologi (IKT) (507.10.74) Policy för styrdokument (507.04.43)
Informationsklass	Öppen