2.4.3. Politik for behandling af personoplysninger

1. Indledning

I medfør af lov om finansiel virksomhed og bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. har bestyrelsen vedtaget følgende politik for behandling af personoplysninger (persondatapolitik).

Det er vurderingen, at behandling af personoplysninger, herunder manglende efterlevelse af databeskyttelseslovgivningen er en operationel risiko, som i videst muligt omfang skal minimeres. Dette skal blandt andet ske ved at forankre den nødvendige opmærksomhed og de nødvendige procedurer ned gennem hele organisationen. Et af midlerne til at sikre dette, er en persondatapolitik, som fastsætter de overordnede strategiske mål i relation til at overholde gældende databeskyttelseslovgivning, herunder ikke mindst de registreredes rettigheder (f.eks. kunder, medarbejdere og eksterne samarbejdspartnere).

Persondatapolitikken er inddelt i følgende hovedemner:

1. Indledning
2. Lovgrundlag
3. Anvendelsesområde
4. Risici reguleret af denne politik
5. Sparekassens risikoprofil på persondataområdet
6. Risikofaktorer
7. Risikobegrænsende tiltag
8. Organisatorisk ansvarsfordeling
9. Kontroller og rapportering

2. Lovgrundlag

Persondatapolitikken tager udgangspunkt i EU's databeskyttelsesforordning samt den nationale følgelovgivning, herunder databeskyttelsesloven, lov om finansiel virksomhed §§ 117-123, TV-overvågningsloven (databeskyttelseslovgivningen).

3. Anvendelsesområde

Denne politik finder anvendelse på enhver form for behandling af personoplysninger, hvad enten behandlingen sker automatisk eller manuelt, eller opbevaringen sker i et fysisk arkiv eller i et elektronisk system.

4. Risici reguleret af denne politik

Ved risiko på persondata menes den iboende risiko for, at sparekassen ikke efterlever databeskyttelseslovgivningen eller bliver udsat for databrud, der indebærer krænkelser af fysiske personers rettigheder eller frihedsrettigheder.

5. Sparekassens risikoprofil på persondataområdet

Det er sparekassens hensigt, via overholdelse af databeskyttelseslovgivningen at minimere risikoen for direkte eller indirekte tab som følge af overtrædelse af lovgivningen eller datasikkerhedsbrud.

Det vurderes, at sparekassen har begrænset den iboende risiko for, at sparekassen overtræder lovgivningen, herunder blive gjort ansvarlig for datasikkerhedsbrud.

6. Risikofaktorer

6.1 Medarbejdere

Identifikation og afgrænsning af risikofaktoren ved sparekassens medarbejdere:

Det er medarbejderne, der i det daglige behandler kundernes personoplysninger, og af samme grund er det af afgørende betydning, at medarbejderne behandler kundeoplysninger korrekt og med den nødvendige fortrolighed. Fejl eller forsømmelse begået af medarbejderne kan have store konsekvenser for persondatasikkerheden.

Medarbejdere udgør som følge heraf en væsentlig operationel risiko.

6.2 IT-systemer/IT-sikkerhed

Identifikation og afgrænsning af risikofaktoren ved sparekassens IT-systemer:
Sparekassens behandling af persondata er i dag elektronisk og foregår i sparekassens IT-systemer. Sparekassens IT-systemer indeholder således mange oplysninger om kunder, medarbejdere med videre, som ikke må komme til uvedkommendes kendskab.

Det kan have store konsekvenser for sparekassen, herunder påføre sparekassen et tab, hvis deres IT-systemer kompromitteres, og det er derfor også vurderingen, at IT-systemer/IT sikkerhed udgør en operationel risiko, som gennem risikobegrænsende tiltag skal minimeres.

6.3 Eksterne databehandlere

Identifikation og afgrænsning af risikofaktoren ved eksterne databehandlere:
Sparekassen lader i en række tilfælde eksterne parter foretage databehandling på sparekassens vegne. Det drejer sig blandt andet om sparekassens datacentral, Finans-Support ApS og databehandlere, der deltager i diverse sektorsamarbejder.

Det vurderes, at disse databehandlere udgør en operationel risiko, da eventuelle fejl eller forsømmelser fra deres side i forhold behandling af personoplysninger på vegne af sparekassen kan påføre sparekassen et tab.

6.4 Eksterne samarbejdspartnere

Identifikation og afgrænsning af risikofaktoren ved sparekassens eksterne samarbejdspartnere:
Sparekassen indgår i en række tilfælde samarbejder med eksterne parter, hvor der sker en udveksling af personoplysninger, herunder kundeoplysninger. Hvis disse personoplysninger kompromitteres som følge af fejl eller forsømmelse fra de eksterne samarbejdspartnere, kan dette påføre sparekassen et tab. Det vurderes, at de eksterne samarbejdspartnere som følge heraf udgør en operationel risiko.

6.5 Eksterne serviceleverandører

Identifikation og afgrænsning af risikofaktoren ved sparekassens eksterne samarbejdspartnere:
I det omfang sparekassen benytter eksterne serviceleverandører, som f.eks. rengøringspersonale eller eksterne konsulenter, der kan eller allerede har fået adgang til personoplysninger, som sparekassen er ansvarlig for, vil de udgøre en operationel risiko, da manglende fejl eller forsømmelse fra deres side, kan påføre sparekassen et tab.

6.6 Eventuelle yderligere risikofaktorer

Når sparekassen måtte blive opmærksom på yderligere risikofaktorer skal disse identificeres og beskrives.

7. Risikobegrænsende tiltag

På baggrund af risikovurderingen har sparekassen indført følgende tiltag for at sikre efterlevelse at databeskyttelseslovgivningen, herunder minimere risikoen for datasikkerhedsbrud:

7.1 Forretningsgange og procedurer:

Sparekassen har indført følgende forretningsgange:

- 4.4.1.8 Forretningsgang for arkivering
- 4.4.1.9 Forretningsgang for behandling af kundeoplysninger
- Forretningsgang for behandling af oplysninger om medarbejdere/HR-oplysninger

Sparekassen vil når behovet opstår derudover indføre producerer for:

- Efterlevelse af oplysningspligt
- Indsigtsanmodninger

- Anmodninger om berigtigelse eller sletning
- Anmodninger om begrænsning af behandling
- Indsigelsesanmodninger
- Anmodninger om dataportabilitet
- Anmodninger om ikke at være genstand for automatiske afgørelser
- Indhentelse og tilbagekaldelse af samtykke
- Udarbejdelse af fortegnelser
- Gennemførelse af konsekvensanalyse (DPIA)
- Anmeldelse af brud på persondatasikkerheden

7.2 Awareness

Sparekassen har iværksat tiltag med henblik på at sikre den fornødne awareness hos de enkelte medarbejdere bl.a. undervisning, herunder e-learning og afholdelse af informationsmøder.

7.3 Medarbejderkompetencer

Medarbejderne skal besidde en faglighed, som sætter den enkelte medarbejder i stand til på kvalificeret vis at håndtere sparekassens persondatarisiko inden for deres faglige områder. Kvalifikationerne afspejler indholdet af jobfunktioner og kan hidrøre fra uddannelse, særligt branchekendskab og erhvervserfaring i øvrigt.

7.4 Databehandleraftaler og outsourcing

Ved brug af databehandlere (en fysisk eller juridisk person, der behandler oplysninger på sparekassens vegne) vil der blive udarbejdet en databehandlingsaftale, som fastsætter genstanden og varigheden af behandlingen, behandlingens karakter og formål, typer af personoplysninger og kategorierne af de registrerede, samt parternes rettigheder og forpligtelser.

7.5 Fortrolighedserklæring

Samarbejds- og servicepartnere vil efter en konkret vurdering blive bedt om at underskrive en fortrolighedserklæring.

7.6 Udpegning af Databeskyttelsesrådgiver (DPO)/ Forankring af ansvar

Det vurderes ikke pt. nødvendigt at udpege en DPO, idet forankringen af ansvar sker ved at udnævne den complianceansvarlige som ansvarlig for sparekassens databeskyttelse.

7.7 Databeskyttelse gennem design og standardindstillinger

Sparekassen vil i overensstemmelse med databeskyttelseslovgivningen både i forbindelse med anskaffelses- og udviklingsfasen af IT-systemer – og på tidspunktet for selve behandlingen gennemføre passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper og opfyldelse af kravene i databeskyttelsesforordningen og beskytte de registreredes rettigheder. Dette sker typisk i regi af datacentralen.

7.8 Eventuelle yderligere risikobegrænsende tiltag

Hvis sparekassen måtte blive opmærksom på yderligere risikobegrænsende tiltag skal disse beskrives og implementeres.

8. Organisatorisk ansvarsfordeling

Bestyrelsen og direktionen er ansvarlig for overholdelse af politik for behandling af personoplysninger.

8.1 Bestyrelsen

Bestyrelsen har i fællesskab med direktionen det overordnede ansvar for, at databeskyttelseslovgivningen efterleves. Bestyrelsen har mere konkret ansvar for følgende opgaver:

- Vedtagelse af en overordnet persondatapolitik
- Efter oplæg fra direktionen tage stilling til, om sparekassen skal udpege en DPO
    - I givet fald godkende rammerne for DPO'ens funktion
    - Godkende eventuel indstilling fra direktionen om afskedigelse af DPO'en

8.2 Direktionen

Direktion har i fællesskab med bestyrelsen det overordnede ansvar for, at databeskyttelseslovgivningen efterleves. Direktionen har mere konkret ansvar for følgende opgaver:

- Sikring af, at de fornødne ressourcer er til rådighed, således at databeskyttelseslovgivningen kan efterleves i hele organisationen
- Bidrage til fælles forståelse af vigtigheden af at overholde gældende databeskyttelseslovgivning
- Udstede instruks til en eventuel DPO, hvis direktøren ikke selv er DPO.
- Inddrage en eventuel DPO'en tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger i sparekassen
- Forelægge indstilling om eventuel afskedigelse af DPO'en for bestyrelsen til endelig godkendelse

8.3 DPO'ens ansvar

- DPO'ens ansvar kan være særskilt beskrevet i en instruks udstedt af direktionen

8.4 HR's ansvar

HR og den lønansvarlige har følgende konkrete opgaver:

- Udarbejdelse og vedligeholde procedurer for at sikre, at medarbejdernes HR-oplysninger behandles lovligt

8.5 Medarbejderes ansvar

Medarbejdere har følgende konkrete forpligtelser:

- Efterlevelse af politikker, forretningsgange og øvrige procedurer inden for deres arbejdsområde, der vedrører behandling af personoplysninger
- Deltage i eventuelle informations- og undervisningsaktiviteter
- Have generel opmærksomhed på beskyttelse af personoplysninger i forbindelse med ansættelsen i sparekassen
- Ved mistanke om datasikkerhedsbrud underrette nærmeste leder om denne mistanke

9. Kontroller og rapportering

Ved mistanke om datasikkerhedsbrud skal bestyrelsen underrettes senest på næstkommende bestyrelsesmøde.