

POLITIK FOR PERSONDATASIKKERHED
FOR
SECURE SPECTRUM MIDTVEST ApS
(SELSKABET)

17. februar 2023

Version: nr. 1

1. Indledning

Nærværende politik er udarbejdet i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 - Persondataforordningen art. 6 stk. 1a-c, samt art. 13, Lov nr. 502 af 23/05/2018 Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven).

Politikken fastlægger de overordnede rammer for behandling af personoplysninger i Selskabet. Politikken finder anvendelse ved behandling af persondata tilhørende Selskabets kunder (potentielle, nuværende og tidligere), ansatte (tidligere og nuværende) og ansøgere.

2. Overordnet strategisk mål

Direktionens overordnede strategiske mål er at sikre en forståelse af, hvorfor og hvordan personoplysninger indsamles, beskyttes og anvendes, samt at gøre de ansatte bekendt med de forpligtelser som følger af lovgivningen.

3. Ansvar

Direktionen er forpligtet til at implementere de overordnede rammer i politikken, og løbende sikre sig at Selskabet efterlever rammerne i politikken. Direktionen skal yderligere sikre sig, at Selskabets ansatte gennem medarbejderinformationer, møder eller lignende gøres bekendt med Selskabets persondatapolitik.

4. Definitioner

Ansatte dækker over personer, der direkte er ansat i virksomheden.

Kunder dækker over privatpersoner, ejere af et selskab, herunder alle reelle ejere, tegningsberettigede, bestyrelsesmedlemmer og kontaktpersoner.

5. Risikovurdering af Selskabet

I forhold til Risikovurdering af Selskabet henvises til særskilt Risikovurdering som tillæg til denne politik.

6. Grundlæggende principper om behandling af persondata

Selskabet skal altid følge de grundlæggende principper om behandling af persondata:

- Lovlighed
- Formålsbegrænsning
- Dataminimering
- Rigtighed
- Opbevaringsbegrænsning
- Integritet og fortrolighed

7. Behandlingsgrundlag

Retsgrundlaget for behandlingen af kunder og tidligere kunders persondata følger af:

- Persondataforordningens art. 6 stk. 1, b – behandling er nødvendig af hensyn til opfyldelse af kontrakt.
- Persondataforordningens art. 6 stk. 1, c – behandlingen er nødvendig for at overholde en retlig forpligtelse. Her henvises der til politik for hvidvask og terrorfinansiering kapitel 3 om kundekendskab.

Retsgrundlaget for behandling af potentielle kunders persondata følger af:

- Persondataforordningens art. 6 stk. 1, a – afgivelse af samtykke til behandling af personoplysninger
- Persondataforordningens art. 6 stk. 1, f – forfølge en legitim interesse

8. Persondata

Selskabet behandler forskellige typer af persondata alt efter, om det er potentielle kunder, kunder eller samarbejdspartnere, herunder:

- Navn
- Kontaktoplysninger
- Adresse og cpr-nummer
- Konto-nr. og depot-nr.
- Økonomiske forhold, herunder formueforhold, investeringer og skatteforhold
- Oplysninger om kundens beskæftigelse
- Oplysninger om kundens familieforhold
- Kopi af pas, sundhedskort og kørekort
- Telefonsamtaler mellem kunden og dennes rådgiver, som Selskabet i henhold til anden lovgivning er pålagt at optage.

9. Persondataansvarlig

Den persondataansvarlige er selskabets direktør.

10. Fortegnelser

Selskabet fører fortegnelser over alle behandlingsaktiviteter, som Selskabet foretager.

Fortegnelserne laves i et Excelark, hvor behandlinger og deres hjemmel anføres, således at det altid kan dokumenteres, hvordan Selskabet behandler data, samt hvilken hjemmel Selskabet har til behandlingen.

Der laves forskellige fortegnelser alt efter hvilken slags persondata og formål med behandling, der er.

11. Sletningspligter

Personoplysninger skal slettes, når Selskabet ikke længere har brug for at behandle dem.

Tidspunktet for, hvornår personoplysningernes slettes afhænger af til hvilket formål personoplysningerne er indsamlet.

Slettepligt for de enkelte kategorier af indsamlede og behandlede data fremgår af fortegnelserne, se afsnit 10.

12. Håndtering af ustruktureret materiale

Struktureret materiale er defineret som materiale i systemer.

Ustruktureret materiale er defineret som alt materiale, der ikke er struktureret.

12.1 E-mails

I e-mails mellem ikke krypterede e-mailadresser skal vedhæftninger begrænses. I stedet for skal der alle steder, hvor det er muligt, linkes til materiale, som indeholder persondata.

Al persondata, som har karakter af følsomme eller fortrolige personoplysninger, som Selskabet sender og modtager, både fra og til kunder, potentielle medarbejdere samt eksisterende medarbejdere, må ikke sendes og modtages pr. e-mail, se afsnit 12.4.

Sker det, at der modtages en e-mail, som indeholder følsomme eller fortrolige personoplysninger, skal afsender informeres om, at e-mailen slettes samt guides til, hvordan afsendelsen i stedet kan finde sted.

12.2 Kundemapper

Alle kundeoplysninger er i en elektronisk kundemappe, der indeholdende persondata. Kundemapperne er, som alle elektroniske mapper, rettighedsbegrænset.

For følsom og/eller fortrolig data i kundemappen er rettighedsafgrænsningen yderligere skærpet, ligesom der, hvor det er vurderet relevant, er sket anonymisering af den følsomme eller fortrolige data.

Både de rådgivningsansvarlige og administrationen har ligeledes adgange til fysiske kundemapper, som opbevares i aflåste skabe med begrænset adgang.

12.3 Dokumenter

Alle dokumenter, der indeholder persondata, herunder aftaleforhold, skal være gemt ned på Selskabets drev, og tilgangen skal være rettighedsbegrænset.

Dokumenter i fysisk form skal være låst inde i skabe med begrænset adgang, og makuleres, når de ikke længere har et formål.

Andre fysiske dokumenter, som ikke direkte indeholder persondata, men som kan indeholde persondata, skal inden medarbejderen forlader arbejdspladsen være låst inde i medarbejderens skab eller skuffe. Når medarbejderen forlader arbejdspladsen, må der ikke ligge nogen form for dokumenter synligt på medarbejderens skrivebord.

12.4 Kommunikation omkring følsomme eller fortrolige data

Alle dokumenter, der indeholder følsom eller fortrolig persondata, herunder aftalegrundlag, skal fremsendes og modtages via selskabets system for sikker kommunikation.

12.5 Øvrig kommunikation

Der opfordres til, at alle dokumenter, der indeholder persondata af almindelig karakter, fremsendes og modtages via E-signatur.

12.6 Information til registrerede

Selskabet har, som led i at informere de registrerede, udarbejdet en persondatapolitik omhandlede kunders persondata, som er lagt tilgængelig for alle potentielle og eksisterende kunder på Selskabets hjemmeside.

13. Den registreredes rettigheder

13.1 Ret til indsigt

Den registrerede, herunder potentielle kunder, eksisterende kunder eller ansatte i Selskabet har ret til at få indsigt i de oplysninger, som Selskabet har registeret om personen, hvor disse oplysninger stammer fra, og hvad Selskabet anvender oplysningerne til.

Den registrerede har ligeledes ret til at få oplyst, hvem der modtager oplysninger om den registrerede, såfremt disse oplysninger videregives.

13.2 Ret til berigtigelse

Den registrerede har ret til at få urigtige oplysninger rettet.

13.3 Ret til sletning

Den registrerede har som udgangspunkt ret til at få slettet de oplysninger, som Selskabet har om den registrerede.

Dette er dog betinget af, hvorvidt Selskabet fortsat, i henhold til anden lovgivning, er forpligtet til at opbevare disse oplysninger.

Slettepligten fremgår af fortegnelserne, jf. afsnit 10.

Kan en sletning ikke imødekommes, skal den registrerede have besked herom.

13.4 Ret til dataportabilitet

Den registrerede har i visse tilfælde ret til at få de personoplysninger, som den registrerede selv har givet til Selskabet, overført fra én dataansvarlig til en anden dataansvarlig.

13.5 Ret til indsigelse

Den registrerede har ret til at gøre indsigelse mod behandling af sine personoplysninger. Såfremt Selskabet får en sådan indsigelse, skal Selskabet tage stilling til, hvorvidt indsigelsen kan imødekommes eller ej.

Den registrerede kan til enhver tid gøre indsigelse mod anvendelse af sine oplysninger til direkte markedsføring. En sådan indsigelse skal imødekommes, og Selskabet skal sørge for, at den registrerede ikke modtager materiale, som kan karakteriseres som direkte markedsføring.

13.6 Ret til begrænsning

Såfremt den registrerede har gjort indsigelse mod behandlingen af sine personoplysninger, kan den registrerede kræve, at behandling af disse oplysninger begrænses til opbevaring, indtil det kan fastslås, hvad der skal ske med oplysningerne.

14. Videregivelse af persondata

Selskabet videregiver persondata på baggrund af en retlig forpligtelse til opfyldelse af kontrakten mellem Selskabet og kunden, eller hvor Selskabet har indgået særskilt samtykke om videregivelsen. Nedenstående er eksempler på, hvem Selskabet kan videregive persondata til:

- Banker
- SKAT
- NSK
- Secure Spectrum Fondsmæglerselskab A/S
- Secure Spectrum Administration ApS
- Alternative Equity Partners A/S
- Investeringsfonde, hvor Selskabet faciliterer investeringer for kunden

I en række tilfælde kan Selskabet videregive medarbejderens oplysninger til relevante modtagere, f.eks.:

- SKAT
- Arbejdsmarkedets Tillægspension (ATP)
- ACF (Arbejdsgivernes Centrale Ferieregister), Arbejdsmarkedets Feriefond og Feriekonto
- Danmarks Statistik
- NemKonto
- Banker (fuldmagtsforhold)
- Pensionsinstitut (medarbejderordning)
- Arbejdsskadestyrelsen (anmeldelser om arbejdsskader)
- Arbejdsgivernes Uddannelsesbidrag (AUB)
- Kommuner (dagpengerefusion)
- Virk.dk
- Indkomstregistret
- DA-Barsel og/eller Barsel.dk
- Selskabets eksterne revision
- Finanstilsynet
- Plesner Advokatpartnerselskab (Whistleblowerordning)

I tilfælde af videregivelse vil det ske inden for rammerne af gældende lovgivning.

15. Databehandleraftaler

Såfremt Selskabet videregiver persondata som Selskabet er dataansvarlig for til et andet selskab, på baggrund af en aftale om behandling af persondata, skal der indgås en Databehandleraftale.

En databehandleraftale skal altid leve op til de krav, Selskabet har sat for databehandleraftaler. Kravene afspejler de krav, der er sat i denne politik til behandling af personoplysninger. Hvis det ikke er tilfældet, skal der laves en individuel vurdering af om afvigelsen kan accepteres. Vurderingen skal altid gemmes sammen med databehandleraftalen.

16. Intern uddannelse og awareness

Direktionen og eventuelle ansatte skal løbende holde sig ajour inden for reglerne om behandling af persondata. Direktionen og eventuelle ansatte skal minimum én gang om året modtage undervisning, f.eks. e-learning om persondataretten.

17. Anmeldelse ved sikkerhedsbrud

Mistanke om sikkerhedsbrud eller reelle sikkerhedsbrud skal omgående indberettes til den Persondataansvarlige. Den Persondataansvarlige skal på baggrund af henvendelsen træffe beslutning om, hvorvidt mistanke om sikkerhedsbrud eller det reelle sikkerhedsbrud, er af en karakter, der medfører, at det skal anmeldes til Datatilsynet.

Sikkerhedsbrud, eller mistanke om sikkerhedsbrud, som det vurderes skal anmeldes, skal anmeldes til Datatilsynet inden for 72 timer efter, at Selskabet er blevet bekendt med samme.

Det skal i samme omgang vurderes, om der skal ske underretning til den/de registrerede, som kan være berørt af mistanken om sikkerhedsbrud eller har været berørt af det reelle sikkerhedsbrud.

18. Opdatering af politikken

Direktionen skal mindst én gang årligt, i overensstemmelse med årsplanen, vurdere og eventuelt opdatere nærværende politik.

Godkendt af direktionen i Secure Spectrum MidtVest ApS, den 17. februar 2023.