Fundamental Fondsmæglerselskab A/S

P-115 Politik for persondatabeskyttelse for kunder og ansatte

Opdateret juni 2025

Fundamental Fondsmæglerselskab A/S

P-115 Politik for persondatabeskyttelse for kunder og ansatte

Politik for persondatabeskyttelse for kunder og ansatte	Michael Bonde Kristensen (compliance konsulent) Marie-Louise Henricson, Sine Nielsen og René Spurré
Dato for denne version	Juni 2025
Dato for godkendelse af bestyrelsen	August 2025
Næste revision af politikken senest	August 2026

Lovgrundlag

Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter: ”Databeskyttelsesforordningen”). Politikken fastlægger de overordnede rammer for behandlingen af personoplysninger i Fundamental Fondsmæglerselskab A/S (herefter: Fundamental).

LBK nr. 289 af 08/03/2024 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter: ”Databeskyttelsesloven”).

Vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Indledning

Denne politik fastlægger de overordnede rammer for behandlingen af personoplysninger i Fundamental.

Fundamental behandler dagligt personoplysninger om både kunder, medarbejdere og ansøgere, da det er nødvendigt for at kunne levere investeringsservice til kunderne og som led i den daglige drift.

Det er derfor afgørende, at Fundamental i videst muligt omfang beskytter personoplysninger, og behandler disse oplysninger inden for databeskyttelseslovgivningens rammer.

Nærværende politik gælder for alle dele af selskabet, inklusive de processer, services og data, som er outsourcet til eller lagret hos eksterne leverandører.

I politikkens bilag 1 og 2 findes en gennemgang af selskabets behandling af persondata.

Definitioner

Brud på persondatasikkerhed: Et brud på persondatasikkerheden er en sikkerhedshændelse, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person (”den registrerede”).

Identificerbar person: En person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et CPR-nr., lokaliseringsdata, en online-identifikator eller et eller flere elementer, der er særlige for denne persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Personoplysninger inddeles i følgende kategorier:

Følsomme personoplysninger: Personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Oplysninger om strafbare forhold: Personoplysninger vedrørende straffe, domme eller lovovertrædelser.

Fortrolige personoplysninger: Personligt identifikationsnummer (CPR-nr.) givet til statsborgere og personer med opholdstilladelse i Danmark.

Almindelige (ikke-følsomme) personoplysninger: Personoplysninger, som ikke er omfattet af de ovenstående kategorier.

Roller og ansvar

Alle medarbejdere i Fundamental skal være bekendt med indholdet af politikken.

Bestyrelsen er forpligtet til at implementere de overordnede rammer i databeskyttelses-politikken og løbende sikre sig, at Fundamental efterlever rammerne i politikken. Bestyrelsen er desuden forpligtet til at sikre, at databeskyttelsespolitikken om nødvendigt bliver opdateret.

Direktionen har ansvaret for, at denne politik udbygges i en forretningsgang med instrukser til, hvordan persondata konkret håndteres i selskabet.

Den løbende drift i relation til sikring af databeskyttelsespolitikken sker i et samarbejde mellem ledelsen, compliance og den IT-ansvarlige.

Fundamental har ingen databeskyttelsesrådgiver (DPO) og er ikke forpligtet til at udpege én.

Fundamental som dataansvarlig

Som dataansvarlig afgør Fundamental, til hvilke formål og med hvilke hjælpemidler personoplysninger må behandles. Desuden sikrer Fundamental, at alle databehandlere, der benyttes, kan stille de fornødne sikkerhedsgarantier for behandling af personoplysninger. Desuden sikres det, at de er instrueret i, hvordan de må behandle personoplysninger på Fundamentals vegne samt, at der til enhver tid er indgået en databehandleraftale, der lever op til kravene i de gældende regler.

Principper for behandling af personoplysninger

Fundamental tilstræber at efterleve de grundlæggende principper for behandling af personoplysninger, og Fundamental sikrer sig altid hjemmel for behandling af oplysninger om kunder, medarbejdere og ansøgere.

Grundlæggende principper for Fundamentals behandling af personoplysninger

Fundamental følger de grundlæggende databeskyttelsesprincipper om:

- Lovlighed, rimelighed og gennemsigtighed – at oplysninger behandles på et lovligt og rimeligt grundlag, og at der skabes transparens omkring behandlingen af oplysninger.
- Formålsbegrænsning – at oplysninger indsamles til udtrykkeligt angivne formål, og må ikke viderebehandles til formål, som strider imod disse.
- Dataminimering – ikke at indsamle flere oplysninger end nødvendigt.
- Rigtighed – at sikre oplysningers rigtighed og løbende ajourføring.
- Opbevaringsbegrænsning – at oplysninger ikke opbevares længere tid end nødvendigt.
- Integritet og fortrolighed – at oplysninger beskyttes mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse.

Hjemmel for behandling af kundeoplysninger.

Fundamental kan i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra b, c, e og f, behandle oplysninger om kunder, herunder navn, adresse, telefonnummer, e-mailadresse og andre almindelige oplysninger, der behandles som led i Fundamentals virke.

Fundamental indsamler desuden CPR-numre på kunder i forbindelse med kundeoprettelse og aftaleindgåelse. I forbindelse med aftaleindgåelsen indhentes kundens samtykke til indsamling af CPR-nummer.

Fundamental behandler som udgangspunkt ikke følsomme oplysninger om kunder, og i de yderst sjældne tilfælde, hvor der bliver registreret følsomme oplysninger, vil der blive indhentet samtykke.

Hjemmel for behandling af HR-data

Fundamental behandler oplysninger om ansøgere med hjemmel i databeskyttelses-forordningens artikel 6, stk. 1, litra b samt CPR-numre.

Fundamental behandler oplysninger om medarbejdere på baggrund af databeskyttelses-lovens § 12, stk. 1 og 2. I de tilfælde, hvor der f.eks. indhentes straffeattester eller lægejournaler, indhentes der samtykke fra medarbejderen.

Opmærksomhed og oplysning

Fundamental tilstræber at skabe opmærksomhed og oplysning omkring databeskyttelse og IT-sikkerhed, så medarbejderne er bekendt med ”dos and don’ts” inden for IT-sikkerhed, dette sker bl.a. ved Fundamentals politikker, intern kommunikation samt undervisning.

Håndtering af de registreredes rettigheder

Fundamental efterlever reglerne om de registreredes rettigheder. Hvis en registreret ønsker at gøre sine rettigheder gældende efter databeskyttelsesforordningen, besvarer

Fundamental sådanne anmodninger inden 30 dage, medmindre anmodningen er tilstrækkeligt kompleks og medfører en ressourcekrævende indsats, hvorefter besvarelsen vil blive sendt inden 90 dage.

Efter databeskyttelsesforordningen har de registrerede bl.a. følgende rettigheder:

- Ret til indsigt i sine oplysninger
- Ret til berigtigelse af ukorrekte oplysninger
- Retten til sletning ("retten til at blive glemt")
- Ret til begrænsning af behandlingen
- Ret til dataportabilitet
- Ret til at gøre indsigelse mod en behandling, herunder i relation til profilering

Ovenstående rettigheder er ikke absolutte. Fundamental forbeholder sig retten til f.eks. at undtage eller begrænse ovenstående rettigheder, hvis der er legitime interesser i lovgivningen herfor, herunder i relation til chikanøse og åbenlyst grundløse henvendelser.

Anvendelse af databehandlere

Fundamental anvender kun databehandlere, som kan stå inde for sikkerheden. Der indgås altid databehandleraftaler med databehandlere. Fundamental har en procedure for løbende kontrol med databehandlere.

Sletning

Fundamental tilstræber sig på i videst muligt omfang ikke at opbevare oplysninger i længere tid end nødvendigt.

Dette betyder, at Fundamental opbevarer oplysninger i følgende perioder:

- Jobansøgere, der har fået afslag på deres ansøgning: maksimalt 6 måneder, medmindre der indhentes samtykke til at opbevare ansøgningen i længere tid.

- Tidligere medarbejdere: Oplysninger om tidligere medarbejdere opbevares så længe, der er et sagligt behov herfor, dog maksimalt 5 år, eller evt. længere, hvis det er nødvendigt for opfyldelse af forpligtelser efter relevant lovgivning så som bogføringsloven eller i relation til potentielle arbejdsskadesager, refusionssager, retssager m.v.

- Oplysninger om tidligere kunder: Oplysninger om tidligere kunder opbevares så længe, der er et sagligt behov for det, dog maksimalt 5 år, eller evt. længere, hvis det er nødvendigt for opfyldelse af forpligtelser efter relevant lovgivning så som bogføringsloven og Hvidvaskloven.

Fundamental forsøger i videst mulige omfang at implementere automatiske sletteprocedurer og begrænse manuelle procedurer.

Tredjelandsoverførsler

Fundamental overfører som udgangspunkt ikke personoplysninger til tredjelande uden for EU/EØS, og anvender kun databehandlere, som behandler personoplysninger inden for EU/EØS.

Hvis Fundamental i fremtiden måtte ønske at anvende databehandlere, som overfører personoplysninger til tredjelande uden for EU/EØS, sikres det, at der eksisterer et nødvendigt overførselsgrundlag i lovgivningen.

Sikkerhed

Fundamental har en række politikker, herunder en IT-sikkerhedspolitik med det formål at forhindre, at persondata hændeligt eller ulovligt bliver tilintetgjort, går tabt eller bliver ændret, mod uautoriseret videregivelse, og mod at uvedkommende får adgang eller kendskab til disse oplysninger.

Fundamental arbejder løbende med forbedring af IT-sikkerheden, herunder principperne om "Privacy by design and privacy by default" i forhold til beskyttelse af persondata i både nuværende og fremtidige systemer.

Herudover har Fundamental udarbejdet en procedure for håndtering af datasikkerhedsbrud.

Foretagelse af konsekvensanalyser

Ved initiering af nye behandlinger, som medfører en risiko for de registrerede, foretager Fundamental konsekvensanalyser og kontakter om nødvendigt Datatilsynet i forbindelse hermed.

Opdatering af politikken

Denne databeskyttelsespolitik kan til enhver tid opdateres på foranledning af bestyrelsen, dog minimum én gang årligt. Medarbejdere hos Fundamental notificeres om eventuelle opdateringer.

Godkendelse og underskrift

Denne politik for virksomhedens persondatabeskyttelse erstatter tidligere politik på området.

Godkendt på bestyrelsesmøde den 26. august 2025

Bilag 1 Behandlingsaktiviteter

Kunder

1. DATAANSVARLIG		
Selskabsnavn	Fundamental Fondsmæglerselskab A/S	
Adresse	Staktoften 3, 2950 Vedbæk	
Kontaktoplysninger til selskabet	mail@fundamental.dk - tlf. 39 90 37 00	
Evt. fælles dataansvarlig(e)	Michael Voss	
Evt. databeskyttelsesrådgiver (navn og kontaktoplysninger angives)	N/A	
2. KATEGORIER AF REGISTREREDE		
Kategorierne af registrerede	Nuværende og tidligere kunder	
3. FORMÅLENE MED BEHANDLINGEN		
Formålene med behandling af kundedata	MiFID tests, generel kommunikation til kunden, overholdelse af lovgivning om hvidvask, oplysninger til oprettelse af depot og konti	
4. KATEGORIER AF PERSONOOPLYSNINGER, SOM BEHANDLES		
Hvilke oplysninger om kunder (tidligere, nuværende og potentielle, jf. punkt 2) behandler selskabet? (Opdeles i oplysninger omfattet af persondataforordningens artikel 6 (almindelige oplysninger) og oplysninger omfattet af artikel 9 (følsomme oplysninger)).	Almindelige oplysninger (artikel 6 persondata-forordningen):	
	Identifikationsoplysninger:	Navn, adresse, telefonnummer, e-mailadresse, CPR-nummer/CVR-nummer for de kunder, der har givet samtykke
	Andre almindelige oplysninger:	
	Strafbare forhold:	Registreres ikke
	Særlige kategorier af oplysninger/følsomme oplysninger (artikel 9 i persondataforordningen):	
	Race eller etnisk oprindelse:	Registreres ikke
	Politisk, religiøs eller filosofisk overbevisning:	Registreres ikke. Registrering kan forekomme såfremt kunden er klassifi-

		ceret som en politisk eksponeret person (PEP).
	Fagforeningsmæssigt tilhørsforhold:	Registreres ikke
	Helbredsoplysninger, herunder genetiske data:	Registreres ikke
	Biometrisk data med henblik på identifikation:	Registreres ikke
	Seksuelle forhold eller seksuel orientering:	Registreres ikke
5. KATEGORIER AF MODTAGERE AF OPLYSNINGERNE M.V.		
Hvilke kategorier af modtagere er eller vil personoplysningerne om kunder hos Fundamental blive videregivet til, herunder eventuelle modtagere i tredjelande eller internationale organisationer.	Kundeoplysninger videregives kun til Ringkjøbing Landbobank udelukkende med henblik på oprettelse af depot og konti, og efter aftale med den pågældende kunde	
6. OVERFØRSEL AF PERSONOPLYSNINGER TIL TREJDELANDE ELLER INTERNATIONALE ORGANISATION		
Sker der eventuelt overførsel af personoplysningerne til et land uden for EU/EØS eller en international organisation? (Eksempelvis data-behandlere placeret i tredjeland, eller databehandleres brug af under-databehandlere i tredjelande. Angiv land/organisation og modtager, hvis der sker overførsel).	Nej	
Hvis der sker overførelse, angives overførselsgrundlaget, idet det dog kun er et lovkrav, hvis overførslen baseres på persondataforordningens artikel 49, stk. 1, andet afsnit (overførselsgrundlag kunne herudover være f.eks. et sikkert tredjeland, Privacy Shield eller Kommissionens standardkontrakter)		
7. SLETNING AF DATA		
Hvis det er muligt, angives de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger.	Kundeoplysninger opbevares så længe, der er et sagligt behov herfor. Dette betyder bl.a., at identitetsoplysninger anonymiseres efter 5 år. Data opbevares i øvrigt kun så længe, det er nødvendigt af hensyn til at opfylde Fundamentals forpligtelser, og/eller for opfyldelse af relevant lovgivning, herunder særligt bogføringslovens regler om opbevaring af bogføringsmateriale i 5 år plus indeværende regnskabsår.	

	Følsomme personoplysninger opbevares så længe, det er relevant og nødvendigt af hensyn til den enkelte kundes eller medarbejders sikkerhed. Oplysninger om eventuelle lovovertrædelser slettes efter oplysningerne er videregivet til relevante myndigheder, medmindre oplysningerne er af betydning for Fundamentals virksomhed.
8. GENEREL BESKRIVELSE AF DE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER	
Hvis det er muligt, angives eller vedlægges en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i persondataforordningens artikel 32, stk. 1, dvs. foranstaltninger, der skal sikre behandlingssikkerheden.	Fundamental har en it-sikkerhedspolitik med henblik på at forhindre, at kundedata hændeligt eller ulovligt bliver tilintetgjort, går tabt eller bliver ændret, mod uautoriseret videregivelse, og mod at uvedkommende får adgang eller kendskab til disse oplysninger.

HR-data

1. DATAANSVARLIG		
Selskabsnavn	Fundamental Fondsmæglerselskab A/S	
Adresse	Staktoften 3, 2950 Vedbæk	
Kontaktoplysninger til selskabet	mail@fundamental.dk - tlf. 39 90 37 00	
Selskabets ansvarlige for persondatabeskyttelse (navn og kontaktoplysninger angives)	Sine Nielsen sn@fundamental.dk Tlf.: 39 90 37 00	
Evt. fælles dataansvarlig(e)	N/A	
Evt. databeskyttelsesrådgiver (navn og kontaktoplysninger angives)	N/A	
2. KATEGORIER AF REGISTRERede		
Kategorierne af registrerede	Nuværende og tidligere medarbejdere, ansøgere til stillinger i Fundamental og pårørende til ansatte medarbejdere.	
3 FORMÅLENE MED BEHANDLINGEN		
Formålene med behandling af HR-data	Personaleadministration, dvs.: Administration af personoplysninger om nuværende og tidligere ansatte samt ansøgere hos virksomheden i forbindelse med ansættelse, arbejdsforløb og afskedigelse eller ophør af ansættelse, herunder ved lønkørsel, ferieadministration, administration af forsikringer, pensionsordninger og personale-goder, medarbejderudvikling og generel personalepleje. Administrationen sker på grundlag af gældende lovgivning og andre centralt fastsatte regler samt overenskomster og aftaler, der indgås mellem arbejdsmarkedets parter samt lokalt og individuelt indgåede aftaler om løn- og ansættelsesvilkår samt eventuelle individuelt indhentede samtykker fra medarbejderne.	
4. KATEGORIER AF PERSONOPLYSNINGER, SOM BEHANDLES		
Hvilke oplysninger om medarbejdere og ansøgere behandler selskabet? (Opdeles i oplysninger omfattet af persondata-forordningens artikel 6 (almindelige oplysninger) og oplysninger omfattet af artikel 9 (følsomme oplysninger)).	Almindelige oplysninger (artikel 6 persondata-forordningen):	
	Identifikationsoplysninger:	Navn, adresse, telefonnummer, e-mailadresse og CPR-nummer.
	Andre almindelige oplysninger vedrørende	Stilling/titel, tjenestested, lønforhold,

	ansættelsesforholdet til brug for administration:	arbejdstid, pensionsforhold, skatteoplysninger, bankoplysninger, oplysninger af relevans for lønindeholdelse, personalepapirer, CV, uddannelse, sygefravær. Væsentlige sociale problemer (som arbejdsskader, fleksjob, ansættelse på særlige vilkår, (f.eks. ved handicap), tests, referencer opbevares alene efter aftale med den pågældende medarbejder og kun så længe ansættelsesforholdet er i kraft, dog maks 5 år efter ansættelses-forholdets ophør og så længe, det er nødvendigt for opfyldelse af relevant lovgivning jf. pkt. 6.7
	Strafbare forhold:1	Der indhentes straffeattester fra medarbejderne hvert 3. år. Disse makuleres straks efter ansættelses-forholdets ophør.
	Særlige kategorier af oplysninger/følsomme oplysninger (artikel 9 i persondataforordningen):	
	Race eller etnisk oprindelse:	Registreres ikke
	Politisk, religiøs eller filosofisk overbevisning:	Registreres ikke
	Fagforeningsmæssigt tilhørsforhold:	Registreres ikke
	Helbredsoplysninger, herunder genetiske data:	Registreres ikke

[1] Oplysninger om strafbare forhold forventes at blive særreguleret ved databeskyttelseslovens § 8. Oplysninger om strafbare forhold anses ikke som en følsom oplysning, da den ikke er nævnt i persondataforordningens artikel 9, der udtømmende oplister, hvilke oplysninger der er følsomme (også benævnt særlige kategorier af oplysninger).

	Biometrisk data med henblik på identifikation:	Registreres ikke
	Seksuelle forhold eller seksuel orientering:	Registreres ikke
5 KATEGORIER AF MODTAGERE AF OPLYSNINGERNE M.V.		
Hvilke kategorier af modtagere er eller vil personoplysningerne (HR-data) blive videregivet til, herunder eventuelle modtagere i tredjelande eller internationale organisationer.	Der videregives oplysninger til Prosys, DataLøn, banker, SKAT, ATP, pensionskasser, forsikringsselskaber, og faglige organisationer, Arbejdsskadestyrelsen, Barselsfonden, revisorer og relevante myndigheder. Derudover videregives oplysningerne til andre, hvor det er i overensstemmelse med rettigheder og forpligtelser efter lovgivningen i øvrigt eller det er nødvendigt for at varetage interesser i forbindelse med en konkret tvist m.v. Herudover kan der overføres oplysninger til eksterne databehandlere, som Fundamental har indgået databehandleraftaler med.	
6. OVERFØRSEL AF PERSONOPLYSNINGER TIL TREJDELANDE ELLER INTERNATIONALE ORGANISATION		
Sker der eventuelt overførsel af personoplysningerne til et land uden for EU/EØS eller en international organisation? (Eksempelvis databehandlere placeret i tredjeland, eller databehandleres brug af underdata-behandlere i tredjelande. Angiv land/organisation og modtager, hvis der sker overførsel).	Nej	
Hvis der sker overførelse, angives overførselsgrundlaget, idet det dog kun er et lovkrav, hvis overførslen baseres på persondataforordningens artikel 49, stk. 1, andet afsnit (overførselsgrundlag kunne herudover f.eks. være et sikkert tredjeland, Privacy Shield eller Kommissionens standardkontrakter)	N/A	
7. SLETNING AF DATA		
Hvis det er muligt, angives de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger.	Oplysninger om ansøgere slettes senest 6 måneder efter afslag. Oplysninger om medarbejdere, herunder om medarbejderes pårørende, opbevares så længe der er et sagligt behov herfor, dog maksimalt 5 år efter ansættelsesforholdets ophør eller, hvis det er nødvendigt for opfyldelse af forpligtelser eller relevant lovgivning så som bogføringsloven.	

8. GENEREL BESKRIVELSE AF DE TEKNISKE OG ORGANISATORISKE SIKKERHEDS-FORANSTALTNINGER	
Hvis det er muligt, angives eller vedlægges en generel beskrivelse af de tekniske og organisatoriske sikkerheds-foranstaltninger omhandlet i persondata-forordningens artikel 32, stk. 1, dvs. foranstaltninger, der skal sikre behandlingssikkerheden.	Fundamental har en it-sikkerhedspolitik med henblik på at forhindre, at persondata hændeligt eller ulovligt bliver tilintetgjort, går tabt eller bliver ændret, mod uautoriseret videregivelse, og mod at uvedkommende får adgang eller kendskab til disse oplysninger.