Vilkår for District

Gjelder fra 1. april 2025

Innhold

1 Innledning

Disse vilkårene er innlemmet i hver tilslutningsavtale som er inngått med en kunde, og sammen med vilkårene som gjelder for hver registrert konto (heretter omtalt som de «generelle vilkårene»), utgjør de avtalen mellom Danske Bank og kunden (heretter omtalt som «avtalen»). Med mindre annet er oppgitt, skal disse vilkårene ha forrang ved eventuell motstrid mellom disse vilkårene og de generelle vilkårene med hensyn til District.

District er en flerkanalsplattform med et fullverdig kundegrensesnitt, som kombinerer ulike Danske Bank-tjenester med utvalgte tredjepartstjenester for å danne et komplett og brukervennlig digitalt system for tilknyttede finansielle tjenester. District kan gi tilgang til kontoinformasjon, betalinger og en rekke andre banktjenester etter forespørsel fra deg.

Disse vilkårene er delt inn i følgende deler:

- Del 1 – beskriver alternativene som er tilgjengelige i District, og hvordan systemet skal brukes
- Del 2 – beskriver tredjeparters tilgangsrettigheter
- Del 3 – beskriver sikkerhetskravene ved bruk av District
- Del 4 – beskriver de avtalerettslige forholdene knyttet til bruken av District
- Del 5 – inneholder en liste over definerte begreper

I disse vilkårene gjelder følgende:
Der det i disse vilkårene henvises til «oss», «vi», «Danske Bank», «Banken» eller «Danske Bank-konsernet», gjelder henvisningen Danske Bank A/S og alle dets datterselskaper, filialer og enheter.

«Du», «din», «dine» eller «kunden» betyr kunden som har inngått en avtale med Danske Bank ved å signere en tilslutningsavtale.

Del 1 - District - Generell beskrivelse

1. Moduler og tjenester

District består av separate moduler og tjenester. Modulene du har valgt, er angitt i tilslutningsavtalen.

Hver gang du velger en ny modul, legges den til i tilslutningsavtalen, og du må da signere en oppdatert tilslutningsavtale. Se avsnitt 9 nedenfor for mer informasjon om valg av moduler.

District er tilgjengelig både på nett og som en app. App-versjonen, kalt District Mobile, gir deg tilgang til kjernefunksjonene i District.

Du godtar at ved å bruke en digital enhet (som en smarttelefon, et nettbrett eller en mobiltelefon som kan brukes til å få tilgang til internett eller laste ned appen) til å få tilgang til District Mobile, vil du kun ha tilgang til et begrenset utvalg av tjenester.

Når en bruker laster ned District Mobile, godtar du at disse vilkårene skal gjelde for din og brukerens bruk av District.

2. Innlogging i District

Løsningene som kan brukes til å logge på District, inkluderer Danske Banks eSafeID-sikkerhetsløsning med bruk av enten en eSafeID-kodebrikke (fysisk token) eller mobilautentiseringsappen Danske ID. Sektor-ID-er som BankID i Norge og Sverige samt MitID i Danmark støttes for ulike autentiseringsformål. Men der eSafeID og Danske ID er standardalternativene i alle markeder, kan sektorløsningene variere i henhold til det aktuelle landet for tilslutningsavtalen.

Mer informasjon om de tilgjengelige sikkerhetsløsningene i District er oppgitt under avsnitt 18.3 nedenfor.

Det kreves en bruker for å kunne legge inn alle elementene for den valgte sikkerhetsløsningen ved bruk av District. For District Mobile-appen kan biometrisk pålogging aktiveres når enheten/appen er aktivert.

Hvis brukeren ikke bruker District i en periode på fem minutter, kan vedkommende bli bedt om å legge inn enkelte elementer fra den valgte sikkerhetsløsningen på nytt for å fortsette å bruke District.

3. Transaksjoner

Via District er det mulig å utføre betalinger, kreve inn betalinger og se saldoer og transaksjoner i registrerte kontoer.

Den valgte sikkerhetsløsningen må brukes for å autorisere og samtykke til betalinger gjennom District. Når en bruker utfører en betaling via District, kan denne bli bedt om å legge inn ett eller flere elementer fra den valgte sikkerhetsløsningen på nytt. Mer informasjon om betalinger, autoriseringer og fullmakter er oppgitt under avsnitt 12 og 13 nedenfor.

Når du tar i bruk den valgte sikkerhetsløsningen, samtykker du til og autoriserer dermed alle tjenestene og aktivitetene som er tilgjengelige via District.

4. Registrerte kontoer

Du må ha registrerte kontoer i District før du kan utføre transaksjoner.

4.1. Registrerte kontoer i Danske Bank-konsernet

Følgende kontoer kan registreres i District:

- kontoer som innehas av deg og er åpnet i ditt navn i Danske Bank-konsernet
- kontoer som innehas av tredjeparter, forutsatt at den aktuelle tredjeparten har utstedt en tredjepartsfullmakt til deg, som gir deg tillatelse til å disponere på vegne av tredjeparten eller et datterselskap

Registrerte kontoer i Danske Bank-konsernet kan også administreres via SWIFT MT101 eller MT940/942, dersom dette er tilgjengelig i landet ditt (se beskrivelsen i avsnitt 4.2).

4.2. Registrerte kontoer i Danske Bank-konsernet

Kontoer i banker utenfor Danske Bank-konsernet som vi samarbeider med via SWIFT-nettverket, samt kontoer i Danske Bank-konsernet som du ønsker å bruke til transaksjoner via SWIFT MT101 eller SWIFT MT940, kan også registreres i District som en del av en

tilslutningsavtale. Du kan registrere både dine egne kontoer og tredjepartskontoer. Du og/eller tredjeparten må inngå en avtale med banken den aktuelle kontoen er i, med hensyn til betalingsanmodninger via SWIFT MT101 eller en avtale om saldorapportering via SWIFT MT940.

5. Uregistrerte kontoer

Hvis kontoer som innehas av deg og/eller en tredjepart, ikke er registrert i District, kan du kun utføre betalinger til disse kontoene. Det er ikke mulig å vise oppføringer for, eller utføre betalinger fra, kontoer som ikke er registrert i District.

6. Utenlandske sjekker

Du kan utføre betalinger ved å utstede en sjekk. Dersom du og/eller en tredjepart har en avtale om betalingsanmodninger via SWIFT MT101, kan sjekker også brukes til transaksjoner utenfor Danske Bank-konsernet, forutsatt at dette alternativet er inkludert i avtalen mellom deg og/eller den aktuelle tredjeparten og den eksterne banken. Utstedte sjekker betraktes som banksjekker, og beløpene belastes kontoen på datoen for utstedelsen. Bedriften kan få satt inn det pålydende beløpet for ikke-innløste sjekker på registrerte kontoer. Dersom pålydende på uinnløste sjekker skal krediteres din eller en tredjeparts konto, må du eller den aktuelle tredjeparten ha spesifikke avtalebetingelser om å holde Danske Bank-konsernet skadesløs dersom slike sjekker deretter innløses.

7. Elektroniske ordre

Når en bruker ber om å få gjennomført en transaksjon i District, for eksempel en betaling, kalles det en elektronisk ordre. En elektronisk ordre eller transaksjon utføres når en eller to brukere med riktig fullmaktstype (se avsnitt 12) har signert den elektroniske ordren digitalt. Når en bruker avgir en elektronisk ordre, og ordren er gjennomført, sender vi en elektronisk kvittering.

Fra det tidspunkt vi har kvittert for mottak av den elektroniske ordren, går risikoen for å utføre ordren i henhold til de mottatte opplysningene over til oss.

Dersom en betaling er autorisert på dine vegne, men det er oppgitt en uriktig unik identifikator for betalingsmottakeren, har vi intet ansvar dersom vi behandler betalingen i samsvar med den aktuelle unike identifikatoren. Vi vil imidlertid gjøre rimelige bestrebelser på å få tilbakeført de aktuelle midlene. Du samtykker i at vi kan belaste deg et gebyr for dette. Vi oppbevarer elektroniske ordre i minst syv år, og opptil ti år (avhengig av de generelle vilkårene som er gjeldende for deg). I denne perioden kan du og/eller tredjeparten belastningskontoen tilhører, bestille en papirutskrift av ordren mot betaling av bankens til enhver tid gjeldende sats for ekstraordinær bistand. Mer informasjon om gebyrer er oppgitt i avsnitt 25.2.

7.1. Avslag på utførelse av ordre

Dersom vi ikke godtar å skulle utføre en elektronisk ordre som er autorisert på dine vegne gjennom District, vil vi varsle deg om avslaget så raskt som mulig via District, per telefon, skriftlig, via sikker e-post, via faks eller på annen rimelig måte.

7.2. Bindende ordre

Ordre som er gjennomført i overensstemmelse med opplysningene i den elektroniske ordren, er bindende for deg. Danske Bank kan derfor ikke tilbakeføre betalinger, handler med valuta eller finansielle instrumenter eller andre transaksjoner, herunder utstedte sjekker, som er endelig utført i overensstemmelse med en elektronisk ordre.

7.3. Kansellering av ordre

Du kan endre eller kansellere elektroniske ordre i henhold til reglene og fristene som er oppgitt i de generelle vilkårene som gjelder for deg.

8. Automatisk registrering for mottak av dokumenter i eArkiv

Når du inngår en avtale, registreres du automatisk for å motta dokumenter elektronisk. Dokumentene arkiveres i eArkiv. Dokumenter du mottar i elektronisk form, har samme rettsvirkning som om dokumentene hadde blitt sendt som ordinær post. Tredjepartskontoer som er tilknyttet avtalen din, behandles som dine egne kontoer.

8.1. Dokumenter mottatt i elektronisk form
Du mottar alle dokumenter som sendes elektronisk av Danske Bank, i eArkiv. I særskilte tilfeller kan vi sende slike dokumenter i fysisk form som ordinær post.

Hvis du er kunde hos en eller flere av Danske Bank-konsernets enheter, og du mottar dokumenter digitalt fra disse enhetene, mottar du også de aktuelle dokumentene i eArkiv.

Kontoutdrag, lister over utførte og mottatte betalinger og diverse annet er eksempler på digitalt mottatte dokumenter. Vi legger regelmessig til dokumenttyper og øker antallet dokumenter du kan motta digitalt i eArkiv.

Du kan velge å motta dokumentene via ordinær post mot et ekstra gebyr.

8.2. Tilgang til dokumenter i eArkiv
Rettighetene til den enkelte bruker bestemmer hvilke dokumenter brukeren får adgang til å se i eArkiv.

En bruker kan for eksempel alltid se sin egen brukerfullmakt.

Brukere som har tillatelse til å se oppføringer og saldoer eller til å administrere en konto, gis også adgang til å se dokumentene som er forbundet med den aktuelle kontoen i eArkiv.

Brukere kan gis en særskilt fullmakt til å få adgang til konfidensielle dokumenter og sammendrag i eArkiv.

8.3. Oppbevaring av dokumenter
Vi arkiverer elektroniske ordre og dokumenter i eArkiv i inneværende år som et minimum, pluss ytterligere oppbevaringstid i henhold til den aktuelle dokumenttypen. Vær oppmerksom på at dokumentene blir slettet hvis du fjerner en konto, skifter kundenummer eller bytter bank, eller dersom du av andre grunner ikke lenger har tilgang til District. I slike tilfeller oppfordres du til å ta en kopi og selv lagre dokumentene.

Dersom du har behov for å oppbevare dokumentene lengre enn perioden Danske Bank stiller til rådighet via District, bør du selv ta en kopi og lagre dokumentene for egen oppbevaring.

8.4. Oppsigelse
Dersom avtalen din opphører, eller du får nytt organisasjonsnummer eller fjerner kontoer, vil også muligheten til å motta og hente ut elektroniske dokumenter fra eArkiv opphøre. Se avsnitt 8.3 om oppbevaring av dokumenter.

9. Valg av moduler
Tilslutningsavtalen spesifiserer modulene du har valgt som en del av avtalen din med Danske Bank. Detaljene for hver modul er gitt i modulbeskrivelsene, som utgjør en del av den aktuelle tilslutningsavtalen.

10. Brukerfullmakter
Alle brukere som utfører transaksjoner på dine vegne, må ha fullmakt til å gjøre dette. Slike fullmakter opprettes via bankens skjema for brukerfullmakter, eller via administrasjonsmodulen i District.

Dersom du har tildelt administrasjonsmodulen til en bruker, må du også spesifisere administrasjonsrettighetene du ønsker å tildele den aktuelle brukeren. Brukerfullmakten spesifiserer hva disse administrasjonsrettighetene er. De ulike administrasjonsrettighetene som kan angis i brukerfullmakten, er oppført i avsnitt 10.1.

10.1. Administrasjonsrettigheter
Dersom administrasjonsmodulen er inkludert i avtalen din, må du aktivt velge administrasjonsrettighetene som skal innehas av brukeren som er utpekt som administrator. Ingen av administrasjonsrettighetene er tildelt som standard. Følgende er en ikke-uttømmende liste og en kort beskrivelse av administrasjonsrettighetene som kan gis (en fullstendig liste er tilgjengelig i District):

- avtaleadministrasjon
- brukeradministrasjon
- avtaleinformasjon
- adgang og sperring
- beløpsgrense – konto
- kortadministrasjon

Danske Bank kan fra tid til annen oppdatere og utvide de tilgjengelige typene administrasjonsrettigheter. Eventuelle nye eller ytterligere administrasjonsrettigheter vil være underlagt disse vilkårene. Du mottar separat varsel om slike eventuelle endringer via District eller på annen passende måte. Dersom en bruker er gitt administrasjonsrettigheter, skal alle henvisninger til deg i disse vilkårene tolkes tilsvarende. Dette innebærer at alt en avtaleadministrator gjør i tilknytning til vilkårene i brukerfullmakten, vil behandles som om handlingene var utført av deg. Dersom en tredjepart har signert en fullmakt i din favør, kan du delegere denne fullmakten til en bruker. Dette gjøres via brukerfullmakt-delen i District.

10.1.1. Brukerfullmakt

For brukere som tildeles rettigheten avtaleadministrator og/eller brukeradministrator, må du også bestemme fullmaktsnivået brukeren skal ha, dvs. om brukeren skal gis en av disse fullmaktene:

- alenefullmakt
- to i fellesskap (A-fullmakt)

De ulike fullmaktene er beskrevet i avsnitt 12. En bruker som har rettighetene avtaleadministrator og brukeradministrator, må ha samme godkjenningsrettigheter for begge rettighetene.

10.1.2. Avtaleadministrasjon

Dersom du tildeler rettigheten avtaleadministrasjon til en bruker, gir du brukeren adgang til å

- opprette, endre og slette brukeres avtaleadministrasjonsrettigheter
- opprette, endre og slette øvrige rettigheter knyttet til enkeltbrukere

En bruker med slike administrasjonsrettigheter kalles en avtaleadministrator. Du må avgjøre om en avtaleadministrator skal ha adgang til å gjøre endringer i sin egen bruker-ID. Dersom en avtaleadministrator ikke har adgang til å gjøre endringer i sin egen bruker-ID, kan vedkommende ikke tildele ovennevnte administrasjonsrettigheter til seg selv, og vil heller ikke kunne opprette og godkjenne elektroniske ordre. Denne innstillingen gjelder også for brukerens rettigheter som brukeradministrator.

Der det gis rettigheter knyttet til avtaleadministrasjon og brukeradministrasjon, må dette alltid signeres av dine signaturberettigede. Når en avtaleadministrator ber om at det opprettes en brukerfullmakt med avtaleadministrasjonsrettigheter, genereres et brukerfullmaktsskjema med signaturfelt, som blir tilgjengelig i eArkiv.

Brukerfullmaktsskjemaet kan åpnes av brukere med rettigheten «avtaleinformasjon». Brukerfullmaktsskjemaet må skrives ut, signeres og sendes til Danske Bank. Dersom omstendighetene tilsier det, kan banken velge å godta en elektronisk signatur.

Brukere med rettigheten avtaleadministrasjon skal også tildeles rettigheten brukeradministrasjon.

10.1.3. Brukeradministrasjon

Hvis du tildeler en bruker rettigheten brukeradministrasjon, gir du brukeren adgang til å gjøre følgende på dine vegne:

- opprette og endre brukere, samt gi brukere adgang til fullmakts- og transaksjonstyper, moduler og kontoer som er underlagt avtalen til enhver tid
- opprette og endre brukeres grunnopplysninger
- slette alt på en bruker, inkludert grunnopplysninger

En bruker med disse administrasjonsrettighetene kalles en brukeradministrator. Du må avgjøre om en brukeradministrator skal ha adgang til å gjøre endringer i sin egen bruker-ID. Dersom en brukeradministrator ikke har adgang til å gjøre endringer i sin egen bruker-ID, kan vedkommende ikke tildele ovennevnte rettigheter til seg selv, og vil heller ikke kunne opprette og godkjenne elektroniske ordre. Denne innstillingen gjelder også for brukerens rettigheter som avtaleadministrator.

Dersom banken oppretter en bruker med disse administrasjonsrettighetene, må brukerfullmaktsskjemaet skrives ut, signeres og sendes til Danske Bank. Dersom omstendighetene tilsier det, kan banken velge å godta en elektronisk signatur.

10.1.4. Avtaleinformasjon

Dersom en bruker gis rettigheten avtaleinformasjon, får brukeren tilgang – via en brukerliste – til å søke etter brukere som dekkes av tilslutningsavtalen, og til å se tilgangsrettighetene til hver bruker (herunder grunnopplysninger, moduler, administrasjonsrettigheter, tilgang til kontoer og tilgang til betalinger.

10.1.5. Adgang og sperring
Hvis du tildeler en bruker rettigheten adgang og sperring, gir du brukeren adgang til å gjøre følgende på dine vegne:

- bestille midlertidige PIN-koder (éngangspinkoder)
- bestille eSafeID-kodebrikker og fullføre aktivering av nye eSafeID-kodebrikker
- sperre og oppheve sperring av brukere

10.1.6. Beløpsgrense – konto
Hvis du tildeler en bruker rettigheten Beløpsgrense – konto, gir du brukeren adgang til å opprette, endre og slette beløpsgrenser på de kontoene som brukeren til enhver tid kan disponere iht. avtalen.

For brukere som tildeles rettigheten Beløpsgrense – konto, skal du ta stilling til hvilken fullmakt brukeren skal ha:

- alenefullmakt
- to i fellesskap (A-fullmakt)

Mer informasjon om kontofullmaktstyper er oppgitt i avsnitt 12.

10.1.7. Kortadministrasjon
Hvis du tildeler en bruker rettigheten kortadministrasjon, gir du vedkommende adgang til å gjøre følgende på dine vegne:

- sperre kort
- bestille nytt kort
- bestille PIN-kode for et kort, og bestille ny PIN-kode for et kort
- endre en kortgrense
- se kortinformasjon
- oppdatere informasjon om kortinnehaver

For å se transaksjoner på en registrert konto som er knyttet til et kort, må brukeren ha lesetilgang til den aktuelle kontoen.

Du, og i enkelte tilfeller også kortinnehaver, må inngå egen dokumentasjon med banken. I slike tilfeller kvitterer du for at du vil sørge for at kortinnehaver signerer de nødvendige dokumentene før kortet utstedes, og at du skal oversende de aktuelle dokumentene til banken på forespørsel.

10.1.8. Markets Online – Danske FX
En bruker som tildeles rettigheten Markets Online – Danske FX, er autorisert på dine vegne til å opprette, endre og slette ordre knyttet til handel med verdipapirer eller valuta via District eller via OneTrader-modulen. For at en bruker skal kunne handle med verdipapirer eller inngå valutakontrakter på dine vegne, må du gi skriftlig fullmakt for den aktuelle brukeren.

10.1.9. Varslingssenter
Rettigheten varslingssenter gir brukeren adgang til å gjøre følgende på dine vegne:

- opprette abonnement på varslinger for brukere
- lese mottatte varslinger
- administrere brukerinformasjon
- slette abonnementer på varslinger som er opprettet av brukere

Danske Bank kan kreve et gebyr for varslinger fra brukeren.

10.1.10. Trade Finance
En bruker som tildeles rettigheten trade finance, autoriseres på dine vegne til å opprette, endre eller slette saker knyttet til trade finance-instruksjoner som er gitt til banken under Garanti- og Trade Finance-modulen. De ulike fullmaktstypene er beskrevet under avsnitt 12 nedenfor.

10.2. Sletting av inaktive brukere
Uavhengig av vilkårene i avsnitt 10.1 vil banken slette brukerens tilgang til District dersom brukeren ikke har logget inn på District i løpet av en periode på 15 måneder. Sletting av en bruker påvirker ikke eventuelle andre fullmakter som er innvilget den aktuelle brukeren.

10.3. Meldingssystem
Alle brukere kan sende meldinger til banken elektronisk via en sikker kryptert linje. Brukere kan kun se meldinger de selv sender og mottar i District. Elektroniske ordre kan ikke legges inn via meldingssystemet.

10.4. Kansellering av administrasjonsmodulen
Kontakt Danske Bank hvis du vil kansellere administrasjonsmodulen. Danske Bank kan belaste deg et årlig gebyr for videre administrasjon av avtalen.

Hvis administrasjonsmodulen kanselleres, vil beløpsgrensene som allerede er autorisert, fortsette å gjelde for denne avtalen. For eventuelle kontoer som er åpnet etter datoen for

kansellering av administrasjonsmodulen, vil beløpsgrenser ikke gjelde, men beløpsgrenser for enkeltbrukere vil fortsatt gjelde. Du må kontakte Danske Bank skriftlig hvis du vil endre eller kansellere autoriserte beløpsgrenser, og du ikke har tilgang til administrasjonsmodulen.

Etter kansellering av administrasjonsmodulen vil eventuelle brukere som er innvilget automatisk tilgang til fremtidige kontoer, ikke ha automatisk tilgang til eventuelle fremtidige kontoer som åpnes.

10.5. Endring av brukerfullmakt

Dersom du ønsker å utvide en brukers adgang i District, skal du utstede en ny brukerfullmakt for District i fysisk form, eller – der det er mulig – med din elektroniske signatur i District. Denne nye brukerfullmakten erstatter den forrige. Dersom endringen vedrører brukerens fullmaktsforhold på kontonivå, skal du og/eller den relevante tredjeparten også underskrive en kontofullmakt. Vær for øvrig oppmerksom på at fullmakten en bruker har til District kan påvirkes hvis du utsteder en fullmakt til disponering av konto.

10.6. Tilbakekalling av brukerfullmakter

Brukerfullmakter gjelder inntil du skriftlig kaller dem tilbake – enten fysisk, eller elektronisk med bruk av den valgte sikkerhetsløsningen. Hvis du sier opp avtalen, anser vi dette som en tilbakekalling av alle brukerfullmakter som er utstedt i henhold til avtalen.

Hvis du og/eller en tredjepart har gitt bruker en kontofullmakt, skal denne fullmakten kalles tilbake separat. Det er altså ikke tilstrekkelig at du kun tilbakekaller brukerfullmakten.

10.7. Adgang til kontoer

For hver bruker må du oppgi hvilke kontoer brukeren skal kunne se saldoer og oppføringer for, og/eller utføre betalinger fra. Hvis du gir en bruker fullmakt til å utføre betalinger fra en konto, gis brukeren adgang til transaksjonstypene du angir. For hver konto brukeren gis adgang til, må brukerens fullmaktstype oppgis. Se avsnitt 12 nedenfor for mer informasjon om fullmaktstyper.

10.8. Betalingsgrenser

Dersom administrasjonsmodulen er inkludert i avtalen, kan du administrere grensene for elektroniske ordre som opprettes og/eller godkjennes via District, enten på kontonivå som gjelder for alle brukere (kalt Beløpsgrense – konto) eller for enkeltbrukere (kalt Beløpsgrense – bruker).

Det er ditt ansvar å opprette beløpsgrenser i henhold til dine behov. Dersom en beløpsgrense – konto eller en beløpsgrense – bruker overskrides, kan ikke betalinger behandles før du har iverksatt passende tiltak. I unntakstilfeller kan banken, etter eget skjønn, godta å opprette en beløpsgrense på dine vegne i henhold til skriftlig instruks fra deg.

10.9. Transaksjonstyper

For hver bruker må du oppgi hvilke transaksjonstyper brukeren skal ha adgang til:

- betalinger mellom kontoer registrert under denne avtalen i samme land innenfor Danske Bank-konsernet
- betalingsanmodninger via SWIFT MT101
- euro-betalinger til registrerte kontoer og uregistrerte kontoer i samme land, innenfor Danske Bank-konsernet eller innenfor SEPA-området (Det felles betalingsområdet for euro)
- utenlandsbetalinger til registrerte kontoer og uregistrerte kontoer innenfor eller utenfor Danske Bank-konsernet

Videre må du oppgi om brukeren skal ha fullmakt til å opprette og godkjenne, eller bare til å opprette, de valgte betalingene. Dersom brukeren får fullmakt til å både opprette og godkjenne betalinger, skal det også oppgis hvilke fullmakter som er relevante for hver transaksjonstype. Følgende fullmakter er tilgjengelige på transaksjonsnivå:

- alenefullmakt
- to i fellesskap

Se beskrivelsen av våre ulike fullmaktstyper i avsnitt 12 nedenfor. Generelt anvendes den valgte fullmakten for alle betalinger innen hver betalingstype. Hvis du har valgt en mer restriktiv fullmakt på kontonivå, vil denne gjelde for betalinger til uregistrerte kontoer og utenlandsbetalinger. Vær oppmerksom på at hvis brukeren ikke er innvilget noen fullmakter på kontonivå, anses dette også som en restriksjon.

11. Valutakurser

Betalinger til registrerte kontoer og uregistrerte kontoer i den relevante jurisdiksjonen innenfor eller utenfor Danske Bank-konsernet kan behandles

- uten valutaveksling – dersom veksling ikke er nødvendig (for eksempel dersom betalingen utføres i samme valuta som denominasjonen for mottakerkontoen)
- til gjeldende referansekurs
- til spotkurs – en valutakurs basert på gjeldende markedskurs på det aktuelle tidspunktet, og på eller innenfor spreadene for kursene våre (tilgjengelig i District)
- til avtalt kurs – en kurs som avtales med banken på forhånd for den spesifikke betalingen (du må ha et avtalenummer for å bruke denne kursen)
- til terminkursen – en kurs som er avtalt med hensyn til en terminkontrakt avtalt mellom oss (du må ha et terminkontraktsnummer for å bruke denne kursen)

Innenlandsbetalinger fra én valuta til en annen mellom registrerte kontoer som behandles som en intern kontooverføring i District, behandles til gjeldende referansekurs.

12. Fullmaktstyper

Danske Bank opererer med følgende fullmaktstyper:

- alenefullmakt
- to i fellesskap (A-fullmakt)
- to i fellesskap (B-fullmakt)
- to i fellesskap (C-fullmakt)

Med disse fullmaktene kan du bestemme hvilke brukere som sammen eller alene må godkjenne en betaling eller en ordre.

Fullmaktene er beskrevet nedenfor.

12.1. Alenefullmakt

Når en ordre eller betaling opprettes eller endres av en bruker med denne fullmakten, anses den automatisk som godkjent av brukeren. Brukere med denne fullmakten kan også godkjenne ordre eller betalinger som er lagt inn av brukere med alle andre fullmaktstyper.

12.2. To i fellesskap (A-fullmakt)

Når en ordre eller betaling opprettes av en bruker med A-fullmakt, godkjennes den automatisk av denne brukeren (1. godkjennelse). Ordren eller betalingen krever ennå en godkjennelse (2. godkjennelse) av en bruker som har enten A-, B- eller C-fullmakt, eller alenefullmakt i overensstemmelse med avsnitt 12.1. Brukere med A-fullmakt er sideordnet, og godkjennelsesrekkefølgen er derfor underordnet.

12.3. To i fellesskap (B-fullmakt)

Når en ordre eller betaling opprettes av en bruker med B-fullmakt, er den automatisk godkjent av denne brukeren (1. godkjennelse).
Ordren eller betalingen skal deretter godkjennes (2. godkjennelse) av en bruker med enten A- eller C-fullmakt, eller av en bruker med alenefullmakt i overensstemmelse med avsnitt 12.1. To brukere med B-fullmakt kan ikke godkjenne en betaling i fellesskap.

12.4. To i fellesskap (C-fullmakt)

Når en ordre eller betaling opprettes av en bruker med C-fullmakt, er den automatisk godkjent av denne brukeren (1. godkjennelse). Ordren eller betalingen skal deretter godkjennes (2. godkjennelse) av en bruker med enten A- eller B-fullmakt, eller av en bruker med alenefullmakt i overensstemmelse med avsnitt 12.1. To brukere med C-fullmakt kan ikke godkjenne en betaling i fellesskap.

13. Øvrige fullmakter i District

13.1. Tredjepartsfullmakter som er gitt til deg

Hvis du ønsker å foreta transaksjoner på tredjepartskontoer i Danske Bank-konsernet, må den aktuelle tredjeparten signere skjemaet vårt for tredjepartsfullmakter. Hvis det skal være mulig å bruke SWIFT MT940 angående tredjepartskontoer utenfor Danske Bank-konsernet, må vi først få tilsendt en avtale om at Danske Bank-konsernet kan motta data om tredjepartens eksterne konto(er).

Hvis du skal utføre betalinger fra tredjepartens kontoer utenfor Danske Bank-konsernet via SWIFT MT101, må du først oversende oss en avtale som erklærer at du kan sende betalingsinstruksjoner til tredjepartens bank(er) via Danske Bank-konsernet. Banken registrerer tredjepartskontoene i District via tilslutningsavtalen din. Adgangen til SWIFT MT101 avhenger av tredjepartsbankene.

14. District Mobile

14.1. Tilgang og bruk

For å få tilgang til District via District Mobile må du ha fylt ut og signert en tilslutningsavtale, og brukeren må være tilordnet tilslutningsavtalen. Når en bruker laster ned District Mobile, godtar du at disse vilkårene er gjeldende med hensyn til din eller den aktuelle brukerens bruk av District via District Mobile. I tillegg er bruken av District Mobile underlagt vilkårene i lisensen den er lastet ned i henhold til fra Apple App Store eller Google Play-butikken.

District Mobile gir for eksempel tilgang til følgende innhold og tjenester:

- vise saldoer
- vise transaksjoner
- vise transaksjonshistorikk
- opprette og godkjenne betalinger
- administrasjon

Banken kan fra tid til annen oppdatere, utvide eller redusere tjenestene som tilbys via District Mobile.

14.2. Sikkerhet

I tillegg til eventuelle andre forpliktelser eller øvrig ansvar du måtte ha i henhold til disse vilkårene, må du og hver enkelt bruker treffe alle rimelige tiltak for å ivareta konfidensialiteten til all informasjon som vises eller lagres på mobilenheten i forbindelse med bruk av District Mobile. Du alene er ansvarlig for sikkerheten til mobilenheten.

Du og hver av brukerne skal som et minimum treffe følgende tiltak for å beskytte kontoinformasjonen din:

- Sikre mobilenheten med en sikkerhetskode, endre den med jevne mellomrom, og hold tastaturet låst.
- Sørg for at du og hver av brukerne logger av fra alle District Mobile-økter med en gang du/brukeren er ferdig med å bruke de relevante tjenestene.
- Hold mobilenheten i din besittelse til enhver tid. Ikke la mobilenheten være uten tilsyn på steder der uautoriserte personer kan få tilgang til den.

15. Visning av data fra eksterne tjenesteleverandører

15.1. Innhenting av data fra eksterne tjenesteleverandører

En bruker kan innhente data fra et utvalg leverandører av finansielle og ikke-finansielle tjenester, og vise dem i enkelte av produktene og tjenestene i District, dersom brukeren har adgang til dataene via en personlig sikkerhetsløsning med den valgte tjenesteleverandøren («integrasjonsprosessen»). Dataene hentes til District ved hjelp av tjenesteleverandørens API. Tilgjengeligheten til dataene avhenger av brukerens tilgangsrettigheter hos tjenesteleverandøren og i District.

I noen tilfeller krever tilgang til data fra en tjenesteleverandør at ytterligere avtaler signeres, for eksempel District-tilslutningsavtalen dersom en modul er en forutsetning for å få tilgang til data i et produkt eller en tjeneste i District via integrasjonsprosessen. Ved avvik mellom disse vilkårene og eventuelle tilleggsavtaler/moduler som gir tilgang til data via integreringsprosessen i District, skal vilkårene for tilleggsavtalen/modulen ha forrang.

15.2. Integrering

Når en bruker ønsker å hente ut data fra en ekstern tjenesteleverandør første gang, omdirigerer District brukeren til den valgte tjenesteleverandøren. Tjenesteleverandøren ber brukeren om å identifisere seg med relevant personlig sikkerhetsinformasjon. Dette er nødvendig for å opprette forbindelsen mellom tjenesteleverandøren og District. Danske Bank har ikke tilgang til slik personlig sikkerhetsinformasjon.

Tjenesteleverandøren genererer imidlertid et token som unikt identifiserer brukeren, og sender dette til Danske Bank, som lagrer tokenet. Når brukeren bruker det aktuelle produktet eller den aktuelle tjenesten, sender Danske Bank tokenet til tjenesteleverandørens API, og tjenesteleverandøren returnerer dataene.

Dersom en bruker ikke lenger har slik gyldig personlig sikkerhetsinformasjon med den aktuelle tjenesteleverandøren, slettes tokenet, og det blir ikke lenger mulig for brukeren å få tilgang til dataene via District. Det samme gjelder dersom brukeren ikke lenger har tilgang til District eller det relevante produktet eller den relevante tjenesten i District. Brukeren kan også fjerne tilknytninger i dashbordet med oversikt over tilknytninger i District.

15.3. Kundens erklæring

Du forstår og godtar at

- all uthenting av data (inkludert personopplysninger) gjennom integrasjonsprosessen utføres på dine vegne
- det via integrasjonsprosessen er mulig å hente og vise data som ikke tilhører deg, og som dermed kan tilhøre en annen juridisk person eller fysisk person

Du erkjenner og påtar deg ansvaret for alle opplysninger som hentes ut fra en ekstern tjenesteleverandør via integrasjonsprosessen, og garanterer at

- du har alle juridiske rettigheter til å bruke dataene brukeren får adgang til gjennom integrasjonsprosessen, og som hentes ut og vises i et produkt eller en tjeneste i District
- data ikke hentes ut dersom eventuelle gjeldende tredjepartsavtaler forbyr slik bruk av data
- enhver bruker som bruker integrasjonsprosessen, har alle juridiske rettigheter til å gjøre dette, og er informert om og vil overholde disse vilkårene ved uthenting av data via de eksterne tjenesteleverandørene

15.4. Behandling av data

Data som hentes ut, lagres midlertidig i brukerens nettleserminne, og Danske Bank verken lagrer eller deler dataene eller behandler dem på noen annen måte enn til det formål å vise dataene til brukeren i sanntid.

Danske Bank behandler dataene kun når brukeren bruker produktene eller tjenestene i District som viser dataene fra tjenesteleverandøren.

15.5. Tjenesteleverandørens applikasjon

Danske Bank er ikke ansvarlig for innholdet i, riktigheten til eller tilgjengeligheten av dataene som hentes ut fra tjenesteleverandøren via integrasjonsprosessen, og kan ikke holdes ansvarlig for eventuelle skader eller tap (inkludert eventuelle indirekte tap eller følgetap) som måtte oppstå under eller i forbindelse med bruken av tjenesteleverandørens API-er samt integrasjonsprosessen.

15.6. Kundens ansvar

Du er ansvarlig for, og godtar å godtgjøre Danske Bank for ethvert ansvar og alle skader, tap, kostnader, juridiske kostnader, kostnader til profesjonelle tjenester samt øvrige utgifter som banken eventuelt måtte påføres, uansett om det er direkte, indirekte eller som en følgevirkning, i forbindelse med eller basert på enhver tvist, ethvert krav eller enhver rettssak fremmet mot Danske Bank av en tredjepart basert på eller i forbindelse med din bruk av produktene og tjenestene som henter ut data fra tjenesteleverandører, med mindre et slikt krav oppstår som følge av vesentlig mislighold med hensyn til integrasjonsprosessen, forsettlig mislighold eller bedrageri som banken er ansvarlig for.

16. Kundesupport

Banken gir deg kundesupport og service i form av

- brukeradministrasjon
- telefonstøtte
- internett-baserte støttefunksjoner
- kundesupport lokalt

Brukeradministrasjon kan omfatte etablering av tilslutningsavtaler, autorisasjoner og fullmakter, tilpasning av din og brukernes adgang til de enkelte deler av support og service, sletting og sperring av brukere, bestilling av éngangspinkoder og registrering av endrede fullmaktsforhold mv.

Telefonsupport kan omfatte opplæring, veiledning i bruk, hjelp til feilsøking og veiledning for tilpasninger, samt alternativt å sperre District. Telefonsupport i forbindelse med opplæring i og installasjon, oppsetting og feilsøking mv. av District skjer i samarbeid med IT-avdelingen din og på ditt ansvar.

Internettbaserte supportfunksjoner kan omfatte opplæring, veiledning i bruk, hjelp til feilsøking og veiledning for tilpasninger. Bruken av internettbaserte supportfunksjoner skjer i samarbeid med IT-avdelingen din og på ditt ansvar.

Support lokalt kan omfatte opplæring i bruken av District.

Feilsøking kan omfatte tilrettinger og/eller endringer av maskinenes oppsett og i IT-systemene dine, endringer i registreringsdatabaser, oppsett av rutere, brannmurer, proxyservere og interne sikkerhetssystemer samt generelle endringer av programvare- og maskinvarekonfigurasjoner. Konfigurasjon og support skjer i samarbeid med IT-avdelingen din og på ditt ansvar.

Del 2 - Tilgangsrettigheter for tredjepartsleverandører

17. Tredjepartsleverandører (TPL-er)

Via District kan du bruke tjenester fra tredjepartsleverandører (TPL-er) til å få adgang til kontoen din for å få kontoinformasjonstjenester, iverksette betalinger fra kontoen din og bekrefte forespørsler om midler.

Bruken av tjenester fra tredjepartsleverandører påvirker ikke gebyrene banken belaster deg for de respektive tjenestene.

TPL-er er uavhengige tjenesteleverandører. Hvis vi aktiverer en TPL-tjeneste for deg, gjør vi deg oppmerksom på dette på det aktuelle tidspunktet. TPL-tjenester kan brukes til å få tilgang til hver av kontoene dine som er tilgjengelige på nettet. Kontoen din er tilgjengelig på nettet med mindre de generelle vilkårene eller andre vilkår som gjelder for den aktuelle kontoen, tilsier noe annet.

Via District kan du få adgang til følgende typer tjenester som tilbys av TPL-er:

Kontoinformasjonstjenester
Disse tjenestene gjør det mulig for kontoinnehavere å konsolidere informasjon om ulike betalingskontoer de har hos én eller flere banker, og få en aggregert oversikt over sin finansielle stilling. Noen TPL-er kan også tilby flere tilknyttede tjenester, som verktøy for budsjettering og økonomisk planlegging.

Tjenester for betalingsinitiering
Med disse tjenestene kan kontoinnehaver utføre en rekke former for kredittoverføringer fra kontoen eller kontoene sine.

Utstedere av kortbaserte betalingsinstrumenter
Noen TPL-er kan utstede instrumenter for å utføre kortbaserte betalinger fra en konto. Slike TPL-er kan be oss om å bekrefte om beløpet som trengs til en betaling ved bruk av kortet de har utstedt, er tilgjengelig på kontoen din.

Hvis du bruker en TPL til å utføre en betaling fra kontoen din, må du bekrefte detaljene for betalingen, inkludert sorteringskode og kontonummer, eller – der det er relevant – BIC og IBAN til betalingsmottakeren samt betalingsbeløpet. Når du bekrefter disse opplysningene, behandler vi betalingen i henhold til det som er angitt i de generelle vilkårene eller øvrige vilkår som måtte gjelde for den aktuelle kontoen. Vær oppmerksom på at betalinger som initieres av en TPL, og som krever autorisering av mer enn én bruker (for eksempel dersom brukeren har en delt fullmakt for godkjenning av betalinger), først anses å ha blitt mottatt av oss når vi mottar den endelige autorisasjonen fra gjeldende bruker. Enhver betaling fra kontoen din ved hjelp av tjenester fra en TPL gjøres fra kontoen din som en kredittoverføring, også selv om kontoen er en vi har utstedt et kort for.

TPL-er kan levere tjenester på ulike måter. Noen TPL-er benytter seg av et API til å få tilgang til kontoen din, mens andre bruker en teknikk kalt «skjermskraping». Måten en TPL får tilgang til kontoen din på, er viktig, ettersom det påvirker på hvilken måte disse vilkårene gjelder for deg når du bruker TPL-ens tjenester.

Hvis en bruker samtykker til at en TPL får tilgang til en konto ved hjelp av et API, ber vi brukeren om å autentisere eventuelle TPL-forespørsler vi mottar, ved å skrive inn brukerens personlige sikkerhetsinformasjon på en sikker side tilhørende Danske Bank – som ikke er påloggingssiden i District. Ved å skrive inn sin personlige sikkerhetsinformasjon samtykker brukeren til at vi leverer informasjon til TPL-en og utfører en betaling de har initiert, eller svarer på en bekreftelse på en anmodning om midler, alt etter hva som er aktuelt. TPL-en kan kun se informasjonen brukeren din spesifikt gir autorisasjon til å se eller til å debitere den spesifikke betalingen som er autorisert av brukeren din.

Dersom brukeren samtykker til at en TPL får tilgang til kontoen ved hjelp av skjermskraping, samtykker brukeren til at vi gir informasjon eller utfører betalinger via den aktuelle TPL-en med brukerens personlige sikkerhetsinformasjon. En TPL som får tilgang til kontoen ved hjelp av skjermskraping, kan få tilgang til alle kontoene dine (både betalingskontoer og andre), samt all informasjonen brukerne dine kan få tilgang til i District, og kan utføre betalinger fra kontoen din på samme måte som brukerne dine kan. TPL-en kan be brukeren om å oppgi den personlige sikkerhetsinformasjonen på deres eget nettsted, eller omdirigere brukeren til påloggingssiden til District via bankens nettsted, og be om at informasjonen oppgis der.

Dersom TPL-en bruker skjermskrapingsteknikker, kan det hende at det ikke er klart for oss at det er tjenestene til en TPL som benyttes. I slike tilfeller må du oppgi informasjon om TPL-en på anmodning.

Brukeren vil kunne tilbakekalle TPL-tilgangen til kontoen din enten

- direkte via TPL-en ved å følge dennes prosedyrer
- i District under «Contact and help», eller

- ved å kontakte banken direkte

Du kan også kontakte banken for å få en fullstendig liste over hvilke TPL-er brukerne dine har autorisert til å få tilgang til kontoen(e) din(e). Vi kan kun tilby denne tjenesten dersom TPL-en bruker et API til å få tilgang til kontoen din. Brukeren kan tilbakekalle TPL-ens tilgang til kontoen din direkte via TPL-en ved hjelp av sine egne prosedyrer dersom TPL-en bruker skjermskrapingsteknikker til å få tilgang til kontoen din.

Hvis du gir oss beskjed om at du ønsker å tilbakekalle tilgangen en TPL har til kontoen din, vil vi etterkomme dette, men det utgjør ikke en tilbakekalling av samtykke til en betaling som allerede er debitert kontoen din, eller informasjon som allerede er gitt til en TPL som svar på en bekreftelse av forespørsel om midler eller kontoinformasjonstjenester.

Ellers vil vi bare tilbakekalle tilgangen en TPL har til kontoen din dersom tilgangen etter vår mening er uautorisert eller uredelig, eller hvis vi blir oppmerksomme på at den ikke lenger er autorisert eller regulert av en relevant myndighet.

Vi anbefaler at du kontrollerer at TPL-en er autorisert og regulert av den lokale reguleringsmyndigheten, eller – når det gjelder tilgang til kontoer i en filial av banken som befinner seg i EØS – en annen europeisk reguleringsmyndighet, før du benytter deg av TPL-ens tjenester. Dersom TPL-en er behørig autorisert og regulert i jurisdiksjonen for den aktuelle kontoen, plikter denne å sikre at ingen personlig sikkerhetsinformasjon gjøres tilgjengelig for uautoriserte personer, og at den bruker trygge og effektive kanaler for å levere tjenestene sine til deg.

En TPL skal ikke be om mer informasjon enn det som er absolutt nødvendig for å levere den spesifikke tjenesten.

Del 3 - Sikkerhetssystemet i District

18. - Tekniske forhold

18.1. Overføring og tilgang

For å kunne bruke District må du etablere en datakommunikasjonsforbindelse til oss. Du skal dekke utgiftene til denne forbindelsen og selv sørge for å anskaffe, installere og vedlikeholde det nødvendige IT-utstyret. Du skal dessuten sørge for å foreta nødvendige tilpasninger av IT-utstyret ditt – både for å kunne bruke forbindelsen, og for den fortsatte driften.

Du skal ikke benytte spesialprogramvare, som «overlay services» eller lignende programvare, når du bruker District.

Brukerne må betjene systemet direkte via brukergrensesnittet og programvaren som banken stiller til rådighet.

18.2. Distribusjon, kontroll og oppbevaring av programvare

Banken distribuerer programmene du trenger for å kunne bruke District. Disse kan for eksempel være aktuelle i forbindelse med filutveksling.

18.3. Datasikkerhet

18.3.1. Påloggingsløsninger

Sektor-ID-er (BankID i Norge og Sverige, og MitID i Danmark), eSafeID og Danske ID er autentiseringsløsningene som støttes i District. Påloggingsløsningene kan være gebyrbelagt.

18.3.2. Sektor-ID-er

For å bruke sektor-ID-er til å logge på District gjelder følgende:

- Det er en forutsetning at brukeren er registrert i Danske Banks systemer med personnummer eller et personlig ID-nummer.
- Det er en forutsetning at brukeren følger instruksene som gis av utstederen for å bestille og aktivere sikkerhetsløsningen.
- Sektor-ID-ene gjør det mulig for brukeren å logge på District og signere der uten å måtte innhente andre sikkerhetsløsninger/brikker fra banken.

18.3.3. eSafeID

eSafeID er bankens nettbaserte sikkerhetssystem for pålogging til District, og er tilgjengelig i alle land der District tilbys. eSafeID er en løsning for tofaktorautentisering som består av følgende elementer:

- en unik bruker-ID
- et passord
- Danske ID-appen for mobilautentisering

Som et alternativ til Danske ID kan brukeren få en eSafeID-kodebrikke som genererer sikkerhetskoder til engangsbruk. Når en bruker opprettes i District

med eSafeID-sikkerhetsløsningen, mottar brukeren påloggingsinformasjonen nevnt over. Banken kan kreve et gebyr for utstedelse av eSafeID-kodebrikker.

Éngangspinkoden er systemgenerert og skrives ut maskinelt uten at noen ser kombinasjonen. Hvis brevet med éngangspinkoden og/eller brevet med eSafeID-kodebrikken har vært åpnet eller er ødelagt, skal brukeren kontakte oss og bestille en ny éngangspinkode eller kodebrikke.

Av sikkerhetsmessige årsaker blir brevene med kodebrikke og éngangspinkode sendt hver for seg.
Hvis brukeren ikke har mottatt brevet med éngangspinkoden innen syv virkedager etter bestillingen, skal brukeren av sikkerhetsmessige årsaker kontakte banken for å annullere bestillingen og legge inn en ny.

Av sikkerhetsmessige årsaker må all påloggingsinformasjon aktiveres før første gangs bruk. Under aktivering må brukeren opprette et passord, og deretter makulere éngangspinkoden. Passordet må byttes regelmessig av brukeren.

Dersom brukeren har registrert et mobilnummer i District, kan brukeren velge å motta éngangspinkoden via tekstmelding. Hvis brukeren ikke har mottatt en tekstmelding med éngangspinkoden innen femten minutter etter bestilling, skal brukeren av sikkerhetsmessige årsaker kontakte banken for å annullere bestillingen og legge inn en ny. Når brukeren registrerer seg i District, må vedkommende opprette et passord og makulere éngangspinkoden.

Danske Bank er ikke ansvarlig for eventuelle feil eller tap forårsaket av at brukeren eller avtaleadministratoren ikke klarer å oppdatere brukerens mobilopplysninger i District.

18.4. Andre sikkerhetsløsninger

OpenPGP og EDIsec er bankens sikkerhetssystemer for kunder som vil utveksle informasjon elektronisk med banken direkte fra deres egne forretningssystemer.

OpenPGP og EDIsec er basert på et passord og bruker permanente krypteringsnøkler som er lagret i virksomhetens IT-miljø.

Bruk av de ovennevnte sikkerhetssystemene sikrer at data kan krypteres før de overføres til Danske Bank, og at dataene ikke endres under overføringen.

Avsenderens identitet blir også alltid bekreftet, og alle finansielt bindende transaksjoner signeres digitalt.

18.4.1. EDIsec

EDIsec er en sikkerhetsløsning som brukes til å beskytte data ved direkte dataoverføringer mellom deg og banken via en kommunikasjonskanal som er opprettet mellom deg og banken.

Når det skal opprettes en bruker via EDIsec-sikkerhetssystemet, tildeler banken en personlig bruker-ID til brukeren, men ikke et midlertidig passord. Gyldigheten til kundens offentlige EDIsec-nøkkel sikres gjennom at brukeren må generere et fingeravtrykk av nøkkelen og utveksle dette med banken i henhold til retningslinjene i «EDIsec Implementation Guide».

18.4.2. OpenPGP

OpenPGP er en sikkerhetsløsning som brukes til å beskytte data ved direkte dataoverføringer mellom deg og banken via en kommunikasjonskanal som er opprettet mellom deg og banken.

Når det skal opprettes en bruker via OpenPGP-sikkerhetssystemet, tildeler banken en personlig bruker-ID og et midlertidig passord til brukeren. Du må generere dine egne OpenPGP-krypteringsnøkler og sende dem til banken sammen med engangspassordet i samsvar med instruksjonene som er beskrevet i «OpenPGP Security Implementation Guide» fra banken.

Dersom et sertifikat er utstedt av en tredjepartsutsteder, anser banken brukeren som sertifikateieren, og dermed som ansvarlig for at sertifikatet til enhver tid er gyldig. Banken bruker kun den offentlige kryptografiske koden som finnes i sertifikatet.

Du er ansvarlig for å gå til anskaffelse av og vedlikeholde egnet OpenPGP-programvare (egeneid eller anskaffet fra tredjepart) som kan håndtere OpenPGP-sikkerhet. Det betyr at programvaren for eksempel må kunne håndtere OpenPGP-koder og ha muligheten til kryptering og signering.

18.4.3. EDIsec-koder og OpenPGP-koder (nøkler)

For EDIsec og OpenPGP er du ansvarlig for å bruke gyldige krypteringsnøkler og sikre datakommunikasjonen med banken. Mer spesifikt må du sørge for at:

- Banken har et gyldig sett av krypteringsnøklene dine. Når krypteringsnøklene dine nærmer seg utløp, må du selv

fornye de offentlige krypteringsnøklene og utveksle dem med banken.
- Du må benytte en gyldig versjon av Danske Banks krypteringsnøkler til å sikre datakommunikasjonen med banken. Når bankens offentlige krypteringsnøkler nærmer seg utløp, må du påse at du selv oppdaterer systemet ditt med en ny versjon av bankens krypteringsnøkler, som gjøres tilgjengelig av banken.
- Hvis nøklene dine blir kompromittert, må du kontakte banken for å sperre dem.

Når Danske Bank mottar din offentlige EDISec-kode eller ditt offentlige OpenPGP-sertifikat, vil disse lagres sikkert i Danske Banks systemer, og vil ikke deles med parter utenfor Danske Bank.

Det er Danske Banks ansvar å sørge for at en gyldig versjon av bankens offentlige EDIsec-kode og offentlige OpenPGP-sertifikat alltid er tilgjengelig for deg.

18.5. EDIsec-koder og OpenPGP-koder (nøkler)
Du må iverksette effektive sikkerhetsprosedyrer for å forhindre uautorisert bruk av District, herunder uautorisert tilgang til krypteringsnøkler og eSafeID-kodebrikker.

Følgende regler gjelder for bruk av eSafeID og Danske ID:
- Det er kun brukeren som kan bruke bruker-ID-en, passordet, eSafeID-kodebrikken og den aktiverte instansen av Danske ID-appen.
- Bruker-ID-en, passordet, eSafeID-kodebrikken og den aktiverte Danske ID-appen er strengt personlige, og må ikke deles med noen tredjepart.
- Bruker-ID-en, passordet, eSafeID-kodebrikken og den aktiverte Danske ID-appen kan kun brukes til kommunikasjon med banken.
- Passordet må ikke skrives ned og oppbevares sammen med eSafeID-kodebrikken eller en mobil som har en aktiv Danske ID-app installert.
- Banken anbefaler at brukeren lagrer hemmelige koder i kryptert maskinvare så langt det er mulig.
- Brukeren må alltid bruke den nyeste versjonen av Danske ID-appen.

Brukeren må velge et passord som er så vanskelig som mulig å gjette – for eksempel ved å bruke en kombinasjon av store og små bokstaver, tall og symboler. Brukeren må sørge for at andre brukere ikke får kjennskap til passordet, og må lagre det på en hensiktsmessig og sikker måte. Mer informasjon om sikkerhetsanbefalinger er tilgjengelig under Sikkerhet-menyen i District og på Danske Bank-konsernets nettsider.

18.6. District Mobile - sikkerhet
Du og hver av brukerne må treffe alle rimelige tiltak for å ivareta konfidensialiteten til all informasjon som vises og lagres på mobilenheten din/deres i forbindelse med din bruk av District Mobile. Du og hver enkelt bruker er eneansvarlige for sikkerheten til mobilenheten.

Du og hver bruker bør som et minimum treffe følgende tiltak for å beskytte kontoinformasjonen din:

- Angi en PIN-kode for enheten og endre den med jevne mellomrom, eller bruk en alternativ sikkerhetsfunksjon, som fingeravtrykk.
- Hold tastaturet låst når enheten ikke er i bruk.
- Sørg for at brukeren logger av fra alle District Mobile-økter med en gang brukeren er ferdig med å bruke de relevante tjenestene.
- Sørg for at mobilenheten er i brukerens besittelse til enhver tid, og ikke la enheten være uten tilsyn der personer som ikke er autorisert til å bruke den, kan få tilgang til den.

18.7. Sletting eller sperring av tilgang
Du må varsle Danske Bank hvis du vil at banken skal fjerne en brukers tilgang til District. Du må umiddelbart kontakte banken for å sperre brukertilgangen dersom

- det er mistanke om uautorisert bruk av et passord, en krypteringsnøkkel eller en eSafeID-kodebrikke
- en tredjepart har fått tilgang til et passord, en krypteringsnøkkel, en eSafeID-kodebrikke eller en enhet med en aktiv forekomst av Danske ID

Det er mulig å be om sperring eller kansellering via District eller ved å kontakte banken. Dersom henvendelsen skjer per telefon, må meldingen senere bekreftes skriftlig. Vær oppmerksom på at brukeren sperres i mellomperioden.

Du er ansvarlig for alle transaksjoner utført av brukere før banken blir bedt om å sperre eller blokkere brukeren. Du er også ansvarlig for alle fremtidige transaksjoner som tidligere er bestilt av en slettet/sperret bruker i perioden frem til banken varsles om at transaksjonene må slettes, og bekrefter om dette er mulig.

18.8. Bankens rett til å sperre din eller en brukers tilgang
Brukere kan også sperres av banken. Vi forbeholder oss retten til å sperre din eller en brukers tilgang til District av objektivt begrunnede årsaker knyttet til sikkerheten til District, eller hvis vi registrerer forsøk på misbruk. Hvis tilgangen sperres, blir du varslet umiddelbart per telefon, skriftlig, per e-post, per faks eller på annen rimelig måte etter vårt valg, og vi fjerner sperringen av tilgangen til District dersom årsakene til sperringen opphører.

Banken forbeholder seg også retten til å sperre tilgangen din til District hvis ditt utstyr, programvare eller grensesnitt skader, forstyrrer eller på annen måte er til hinder for banken eller bankens IT-infrastruktur. Hvis tilgangen sperres, varsles du så snart som mulig.

Kontakt banken hvis du vil søke om opphevelse av sperringen. Når sperringen er opphevet, kan det sendes en éngangspinkode per tekstmelding til brukeren dersom brukeren har registrert et mobilnummer.

Du må iverksette alle rimelige tiltak for å forhindre uautorisert bruk av District-tjenesten og uautorisert tilgang til brukerens krypteringsnøkler, passord, eSafeID-kodebrikker og enheter med aktive instanser av Danske ID.

18.9. Krypteringsforbud
Nasjonal lovgivning i det landet der District benyttes, kan inneholde et generelt forbud mot eller begrensninger for kryptering. Det er derfor viktig å kjenne til landets lovgivning.

Del 4. - Avtalerettslige forhold

19. - Krav om bruk i næringsvirksomhet

District skal kun brukes til næringsvirksomhet. Informasjonen som gjøres tilgjengelig for deg, inkludert prisinformasjon, er utelukkende til eget bruk.

20. - Endringer i District

Vi kan til enhver tid utvide omfanget av District uten forhåndsvarsel, men ikke innskrenke omfanget eller innholdet i District med mindre enn én måneds forhåndsvarsel. Vi gir skriftlig informasjon om endringer via District eller på annen hensiktsmessig måte.

21. - Endringer i service og support

Banken kan til enhver tid endre omfanget av og innholdet i service og support med minst én måneds varsel. Varselet kan sendes skriftlig gjennom District eller på annen måte.

Vi vil informere om eventuelle endringer som krever at du må tilpasse utstyret ditt for å opprettholde forbindelsen og tilgangen, ved skriftlig varsel minst én måned i forveien via District eller på annen passende måte.

Vi kan når som helst og uten varsel endre vårt eget utstyr, grunnleggende programvare og relaterte prosedyrer for å optimalisere drift og servicenivåer.

Brukerne må betjene systemet direkte via brukergrensesnittet og programvaren som banken stiller til rådighet.

22. - Endringer i disse vilkårene

Vi kan endre disse vilkårene etter varsel til deg. Vi varsler deg én måned i forveien eller på annen måte som angitt i de generelle vilkårene som gjelder for deg. Varsel og informasjon om endringene gis via District eller på annen hensiktsmessig måte.

De nye vilkårene vil gjelde for deg med mindre du har varslet oss om at du ikke ønsker å være bundet av de nye vilkårene. Vi anser da avtalen som oppsagt på tidspunktet da de nye vilkårene trer i kraft. I noen tilfeller, når endringene er i din favør, trer de nye vilkårene i kraft umiddelbart.

23. - Ansvar

23.1. Ditt ansvar
Din bruk av District skjer på eget ansvar og egen risiko. Du bærer blant annet risikoen for:

- forsendelse av opplysninger til banken og risikoen for at en overføring blir tilintetgjort, skadet, forsinket eller berørt av feil og mangler ved overføringen, blant annet ved

gjennomstillingssentralers behandling eller bearbeidelse av datamateriale
- at opplysninger kommer til tredjeparters kjennskap som følge av feil eller uberettiget inntrengen på dataoverføringsforbindelsen
- feil bruk eller misbruk av District fra brukerens side
- alle operasjoner og transaksjoner som utføres ved hjelp av din eller en brukers krypteringsnøkkel
- å sikre at brukerne holder passordene sine sikre, slik at ingen tredjepart får kjennskap til dem
- å ivareta datasikkerheten i forbindelse med lagring av krypteringsnøkler i IT-miljøet ditt for å forhindre uautorisert tilgang
- uautorisert bruk av District
- at data som overføres til District, er korrekte og overførbare for den tiltenkte bruken

Du kan ikke holde banken ansvarlig for eventuelle konsekvenser som følge av noe av det ovenstående, og du kan heller ikke fremme krav mot banken for feil eller mangler som springer ut av dine egne forhold, herunder manglende overholdelse av sikkerhets- og kontrollprosedyrer.
Det er også ditt ansvar å:

- sikre at brukeren/brukerne er kjent med disse vilkårene og de ulike modulene, og at hver bruker overholder disse og følger instruksjonene i hjelpetekstene som vises på skjermen
- sørge for at du er kjent med innholdet i eArkiv, og har satt opp relevante varslinger i eArkiv
- kontrollere at innholdet i brukerfullmakter alltid er i overensstemmelse med autorisasjonene som er gitt brukeren av deg og eventuelle tredjeparter
- påse at innholdet i brukerfullmakten er i samsvar med dine ønsker og kravene til virksomheten din i alle øvrige henseender
- sørge for at innholdet i brukerfullmakten er i samsvar med brukerens ønsker
- varsle oss per telefon eller via kontaktpersonen din dersom passord, digitale signaturer eller krypteringsnøkler som er relatert til din adgang til District, har blitt misbrukt eller brukt på uautorisert måte. Du skal bekrefte varslingen ved skriftlig henvendelse til banken eller kontaktpersonen din innen syv dager.

I henhold til gjeldende lover kan du ikke fremme noen krav til oss med hensyn til eventuelle feil eller mangler som skyldes forhold på din kant, herunder manglende overholdelse av dine egne sikkerhets- og kontrollprosedyrer.

Hvis du har Danske Direkte Forening-kundepakken, gjelder ikke reglene over ved eventuell tredjeparts uautoriserte bruk av District. Følgelig er ditt ansvar ved eventuell uautorisert bruk av en tredjepart regulert av kontoavtalens de generelle vilkår.

23.2. Vårt ansvar

Vi er erstatningsansvarlige dersom vi på grunn av feil eller forsømmelser oppfyller avtalte forpliktelser for sent eller på mangelfull måte.

Vi er imidlertid ikke erstatningsansvarlige for feil eller mangler som skyldes:

- feil eller mangler i tredjepartsprogramvare som er en del av District-sikkerhetssystemet
- brukeres avsløring av éngangspinkoden og/eller passordet
- endringer i sikkerhetssystemet (som ikke er utført av oss)
- sikkerhetssystemets integrasjon med andre systemer eller programvare som ikke er levert av oss
- endringer i tjenester, informasjon og data som leveres av tredjeparter i sikkerhetssystemet ditt (som ikke er implementert av banken)
- ditt sikkerhetssystems integrasjon med andre systemer eller programvare som ikke er levert av banken

På områder hvor det gjelder et strengere ansvar, er vi forøvrig ikke ansvarlige for tap som skyldes:

- lovgivning eller myndighetsvedtak
- IT-systemfeil/nedetid eller ødeleggelse av data i disse systemene som følge av hendelsene som er oppført nedenfor, uansett om det er vi eller en ekstern leverandør som står for driften av systemene
- svikt i bankens strømforsyning eller telekommunikasjon
- lovpålagte intervensjoner
- forvaltningsvedtak, naturkatastrofer, krig, opprør, pandemi, indre uroligheter, sabotasje, terrorisme eller hærverk (herunder datavirus og hacking), streik, lockout, boikotter eller blokader; uansett om konflikten er rettet mot eller iverksatt av banken selv eller vår organisasjon, og uansett konfliktens årsak.
  Det gjelder også når konflikten bare rammer deler av vår organisasjon.
- alle andre omstendigheter som er utenfor bankens kontroll
- bankens ansvarsfrihet gjelder ikke hvis: vi burde ha forutsett forholdene som er årsak til tapet, da avtalen ble

inngått, eller burde ha forhindret eller avhjulpet årsaken til tapet
- lovgivningen under alle omstendigheter gjør banken ansvarlig for det forhold som er årsak til tapet

I samsvar med alminnelige gjeldende ansvarsregler er vi ansvarlige kun for direkte tap som kan tilskrives feil gjort av oss. Ut over dette er vårt ansvar begrenset til å avhjelpe manglene.

Ytterligere krav kan ikke gjøres gjeldende mot oss, heller ikke ansvar for indirekte skader eller følgeskader.

24. - Bruk av opplysninger

24.1. Bruk av kundens opplysninger
Det er nødvendig for Danske Bank å behandle opplysningene dine for å kunne levere de finansielle løsningene og produktene du har valgt via District, for å kunne utvikle nye produkter og tjenester til kundene våre i District, samt i henhold til loven.

Danske Bank og du er hver for dere behandlingsansvarlige slik dette er definert i personvernforordningen. Det følger av dette at dersom du deler eller ber banken om å dele opplysninger med tredjeparter, er slik deling av opplysninger ditt ansvar.

24.2. Bruk av en brukers opplysninger
Alle brukere må dele visse personopplysninger med oss for å kunne få tilgang til og bruke tjenestene våre på en sikker måte. Av sikkerhetsmessige årsaker loggfører vi brukernes tilgang til og bruk av District. Når vi vet mer om brukerne våre, kan vi også tilby produkter og tjenester på best mulig måte.

Vær oppmerksom på at navn og andre identifikatorer om brukerne kan vises til andre brukere.

24.3. Bruk av en brukers opplysninger
Dersom en tredjepart har gitt deg fullmakt til å disponere tredjepartens kontoer og bruke andre tjenester på tredjepartens vegne i District, vil vi dele opplysninger med brukere på grunnlag av en signert tredjepartsfullmakt.

Vær oppmerksom på at navn og andre identifikatorer om tredjeparten kan vises til alle brukere som har adgang til District-avtalen.

24.4. Erklæring
Når du gir oss personopplysninger, herunder nasjonale personlige ID-er for en bruker, kvitterer du for at du har rett til å utlevere slike personopplysninger til oss.

I tillegg bekrefter du at du tidligere har sørget for at brukeren er informert om hvor vedkommende kan finne informasjon om vår behandling av personopplysninger.

På bankens anmodning, eller dersom offentlige myndigheter etterspør relevant informasjon, må du gi banken slik dokumentasjon som med rimelighet kan kreves for at banken skal kunne vise at det foreligger et hensiktsmessig og gyldig rettslig grunnlag for bankens behandling av personopplysninger i henhold til det ovenstående.

24.5. Mer informasjon
Du kan lese mer om personopplysningene vi registrerer, hvordan vi bruker dem samt den registrertes rettigheter i den gjeldende personvernerklæringen som er tilgjengelig på det lokale nettstedet. Personvernerklæringen inneholder også kontaktinformasjon i tilfelle du har spørsmål.

25. - Øvrige vilkår

25.1. Avtalens oppbygging
Avtalen består av følgende:

- tilslutningsavtalen
- modulbeskrivelsen
- brukerfullmakt(er)
- disse vilkårene
- de generelle vilkårene og/eller andre vilkår som kan gjelde for banktjenestene som brukes via District

Ved å signere tilslutningsavtalen kvitterer du samtidig for at du har lest og akseptert alle deler av avtalen, herunder disse vilkårene, som er en del av avtalen.

Nye bruksvilkår for tjenester som tilbys via District, herunder brukervilkår for tjenester som tilbys av utvalgte tredjeparter, kan legges til med jevne mellomrom, avhengig av din bruk av tjenestene.

Med mindre annet er avtalt: Hvis du begynner å bruke en tjeneste som tilbys via District, anses de tilhørende

tjenestevilkårene å være akseptert, og eventuelle endringer i separate brukervilkår skal anses å være akseptert ved fortsatt bruk.

Disse vilkårene samt øvrige vilkår kan ses og lastes ned fra bankens nettsider.

25.2. Priser

Du må betale abonnementsavgifter og andre gebyrer for District i henhold til den til enhver tid gjeldende prislisten for Danske Bank-enheten i landet tilslutningsavtalen er inngått i, eller på annen måte etter avtale mellom deg og banken.

Banken kan endre priser og gebyrer for District med én måneds varsel. Endringer i priser og gebyrer varsles skriftlig via eArkiv i District, eller på en annen hensiktsmessig måte.

Banken har rett til å:

- samle opp og belaste gebyrer mer enn én måned etter at transaksjonen de angjelder, ble behandlet
- kreve et gebyr for å levere utfyllende opplysninger eller informasjon med hyppigere intervaller enn det som ble avtalt da avtalen ble inngått
- kreve et gebyr for administrasjon av avtalen dersom administratormodulen kanselleres på din anmodning
- kreve et gebyr for betalinger du utfører fra en konto, og for å gi deg informasjon om utførte betalinger

25.3. Overdragelse, overføring og tredjeparter

Avtalen er inngått av banken på vegne av Danske Bank-konsernet. Det innebærer at enhver enhet i Danske Bank-konsernet er berettiget til å oppfylle og håndheve avtalen. Det innebærer også at banken på ethvert tidspunkt kan overdra sine rettigheter og plikter i henhold til avtalen til en annen enhet i Danske Bank-konsernet.

Banken kan overdra sine rettigheter i henhold til avtalen til underleverandører. Slik bruk av underleverandører påvirker ikke bankens ansvar i henhold til avtalen.

25.4. Oppsigelse og mislighold

Du kan si opp avtalen til enhver tid ved skriftlig varsel til oss.

Forespørsler og avtaler som er gitt eller inngått før oppsigelsen, vil bli gjennomført. Betalt abonnementsavgift og eventuelle forhåndsbetalte gebyrer refunderes ikke.

Vi kan si opp Avtalen skriftlig når som helst med minst to måneders varsel.

Vi kan imidlertid si opp avtalen uten varsel dersom du misligholder avtalen. Det foreligger mislighold blant annet hvis bedriften unnlater å betale i henhold til avtalen, stanser sine betalinger eller kommer under konkurs eller insolvensbehandling.

25.5. Lovvalg og verneting

Disse vilkårene samt avtalen er underlagt og skal tolkes i samsvar med lovene i landet der den aktuelle Danske Bank-konsernenheten avtalen er inngått med, er registrert.

Hvis du har registrert deg for en modul hvis formål utelukkende er å bli benyttet i utlandet, aksepterer du – i samme omfang som banken – å være underlagt de rettsregler og sedvaner som gjelder i det land der du opererer, samt eventuelle spesifikke vilkår knyttet til det spesifikke landet og bruken av modulen i det landet.

25.6. Varsler og kommunikasjon

Varsler og annen kommunikasjon mellom deg og banken med hensyn til avtalen skal skje skriftlig, med mindre

- annet er avtalt mellom deg og banken
- banken bestemmer noe annet. Dette kan for eksempel gjelde i tilfeller der banken har behov for å kontakte deg raskt.

Varsler og annen kommunikasjon fra banken leveres i eArkiv i District.

Banken leverer ikke varsler eller annen kommunikasjon på noe varig medium, og disse vil bli gitt på annen hensiktsmessig måte.

Del 5 - Definisjoner og ordforklaringer

Alle begreper som er brukt i disse vilkårene, har betydningen som er definert nedenfor.

I disse vilkårene gjelder følgende:

Tilslutningsavtalen:
betyr avtalen mellom deg og oss om bruk av District og modulene som gjøres tilgjengelige for deg.

Landet for tilslutningsavtalen:
betyr landet der du har inngått tilslutningsavtalen.

Kontoinformasjonstjenester:
betyr tjenester av typen som er beskrevet i avsnitt 17.

Administrasjonsrettigheter (eller rettigheter):
betyr rettighetene som er gitt til en bruker i henhold til det som er angitt i avsnitt 10.1. En fullstendig liste er tilgjengelig i District.

Avtalen:
betyr den fullstendige avtalen med hensyn til District, som beskrevet nærmere i innledningen til disse vilkårene.

Avtaleadministrator:
betyr en bruker som er tildelt brukeradministrasjonsrettigheter, som beskrevet i avsnitt 10.1.1.

API:
står for «Application Programme Interface», og er et grensesnitt som gir direkte tilgang til data og funksjonalitet i et datasystem.

Autorisasjon/fullmakt:
betyr enhver brukerfullmakt, kontofullmakt eller en av de andre fullmaktsformene i District.

Bankdager:
har den betydningen som er gitt i de generelle vilkårene.

Kort:
betyr bedriftskortet (debet eller kreditt) som er utstedt av banken og tilgjengelig i det aktuelle landet.

Kortbaserte betalinger:
betyr betalinger fra kontoen din gjort med et kort utstedt av en tredjepartsleverandør. Slike betalinger inkluderer ikke betalinger gjort med kort som vi har utstedt til deg.

Kortinnehaver:
betyr, for hvert kort, personen et kort er utstedt til.

Utenlandsbetalinger:
betyr betalinger som krysser en landegrense – også om betalingen er i samme valuta, f.eks. euro. Lokale regler kan gjelde for betalinger utført i utlandet. Dette gjelder betalinger mellom både registrerte kontoer og uregistrerte kontoer.

Betalinger regnes ikke som utenlandsbetalinger hvis de gjøres mellom to kontoer i samme land i ett av landene der Danske Bank-konsernet er representert. Betalinger som behandles via SWIFT, faller heller ikke inn under denne kategorien.

Kunden:
betyr bankens kunde som har inngått en avtale med Danske Bank ved å signere en tilslutningsavtale.

Danske Bank A/S og banken:
betyr Danske Bank A/S, Bernstorffsgade 40, DK-1577 København V, Danmark, CVR-nr. 61126228.

Danske Bank-konsernet:
betyr Danske Bank A/S samt alle dets datterselskaper, filialer og enheter.

Danske ID:
betyr mobilautentiseringsapplikasjonen som er utviklet av Danske Bank, og som kan lastes ned fra både Apple App Store og Google Play-butikken.

Elektroniske ordre:
betyr en forespørsel fra deg eller en bruker om en transaksjon eller andre handlinger.

Elektronisk signatur:
betyr en elektronisk signatur som genereres av en bruker ved hjelp av deres bruker-ID, passord og Sector ID/eSafeID-kode.

District:
betyr en flerkanalsplattform med et fullverdig kundegrensesnitt, som skal kombinere alle bankens tjenester med utvalgte tredjepartstjenester for å danne et komplett og brukervennlig digitalt system for tilknyttede finansielle tjenester.

District Mobile:
betyr bankens mobilbankapp for bedrifter, som er tilgjengelig fra Apple App Store eller Google Play-butikken (eller andre distributører av programvareapplikasjoner som fra tid til annen kan tilby mobilbankapplikasjoner for bankvirksomhet), og som gjør det mulig med elektronisk overføring og mottak av informasjon og betalinger (inkludert informasjon vedrørende en registrert konto).

Innenlandsbetalinger:
betyr en betaling til en mottaker som er hjemmehørende i et marked der Danske Bank-konsernet driver virksomhet, og som avsenderkontoen er registrert i.

eArkiv:
betyr den elektroniske arkivtjenesten som er tilgjengelig via District.

Krypteringsnøkkel:
betyr elektroniske filer som brukes i sikkerhetssystemene e-Safekey, OpenPGP og EDIsec som et nøkkelpar: en privat nøkkel for å opprette en digital signatur, og en offentlig nøkkel for å bekrefte den digitale signaturen og kryptere data fra banken til kunden eller brukeren.

eSafeID:
betyr en nettbasert sikkerhetsløsning, nærmere beskrevet i avsnitt 18.3.3.

eSafeID-kode:
betyr en engangskode som genereres med eSafeID-kodebrikken, som brukes sammen med bruker-ID og passord for å logge på og bruke District.

eSafeID-kodebrikke:
betyr en kodebrikke som kommer i ulike formater. Et fellestrekk er at de viser en sikkerhetskode som skal brukes ved pålogging i District ved hjelp av sikkerhetssystemet eSafeID.

Gebyrkonto:
betyr kontoen(e) spesifisert av deg som kontoen(e) der banken har rett til å belaste District-gebyrer (modul- og servicegebyrer), transaksjonsgebyrer og andre gebyrer i henhold til tilslutningsavtalen.

Referansekurs:
betyr det som er angitt i vilkårene for de enkelte kontoene.

Modul:
betyr et sett eller delsett av funksjoner i District.

Modulbeskrivelsen:
betyr punktlistebeskrivelsen av funksjonaliteten til de enkelte modulene som er registrert under tilslutningsavtalen.

Oppsigelsestid:
betyr oppsigelsestiden som er angitt i de generelle vilkårene, og denne kan variere.

Passord:
betyr, når du registrerer deg for District, passordet som en bruker oppretter for å erstatte éngangspinkoden.

Betalingskonto:
betyr en konto som brukes til gjennomføring av betalingstransaksjoner.

Tjenester for betalingsinitiering:
betyr tjenester av typen som er beskrevet i avsnitt 17.

Registrert konto:
betyr enhver konto som er registrert i District i henhold til avtalen.

Skjermskraping:
betyr et datamaskinbasert program som kopierer data fra brukerens datamaskin, som informasjonen i District, og oversetter den slik at informasjonen kan vises til brukeren i et annet format.

Sektor-ID-er:
betyr de ulike påloggingsløsningene som er beskrevet i avsnitt 18.

Tjenesteleverandør:
betyr en tredjepartsleverandør som beskrevet i avsnitt 17, eller en annen aktør i tjenesteleverandørens rolle.

SWIFT MT101:
betyr en forespørsel om en betalingsoverføring sendt via SWIFT-nettverket.

SWIFT MT940:
betyr et elektronisk kontoutdrag mottatt via SWIFT-nettverket.

Éngangspinkode (midlertidig PIN):
betyr et personlig identifikasjonsnummer som utstedes og sendes av banken til en bruker. Nummeret består av fire eller åtte siffer og brukes av brukeren til å registrere seg i District.

Transaksjoner:
er fellesbetegnelsen på tjenestene og funksjonene i District, som beskrevet i avsnitt 3.

Tredjepart:
betyr en person som ikke er kunden eller kundens datterselskap eller tilknyttede selskap, som har signert en tredjepartsfullmakt.

Tredjepartsfullmakt:
betyr et dokument signert av tredjeparten, som autoriserer fullmaktshaveren til å disponere tredjepartens kontoer og bruke andre tjenester på vegne av tredjeparten i District.

Du:
betyr deg som kunde.

Bruker:
betyr en person som er autorisert av deg til å disponere på dine vegne via District.

Brukeradministrator:
betyr en bruker som er tildelt brukeradministrasjonsrettigheter, som beskrevet i avsnitt 10.1.2.

Brukerfullmakt:
betyr din autorisasjon av en bruker, med spesifisering av tjenestene, kontoene, autorisasjonene og/eller rettighetene den enkelte brukeren har adgang til.

Bruker-ID:
et nummer på seks siffer som tildeles en bruker for å identifisere brukeren, og er oppført i brukerfullmakten.

DANMARK
Danske Bank A/S er lisensiert av og driver virksomhet under tilsyn av
det danske Finanstilsynet, Strandgade 29
DK-1401 København K Tel. +45 3355 8282
www.finanstilsynet.dk.
Det danske finanstilsynet har registrert Danske Banks lisens under FSA-nr. 3000.

IRLAND
Danske Bank A/S (som opererer under navnet Danske Bank) er godkjent av det danske Finanstilsynet og er regulert av den irske sentralbanken mht. regler om god forretningsskikk.
www.danskebank.ie

FINLAND
Bankens virksomhet overvåkes også av det finske finanstilsynet,
Snellmaninkatu 6,
Postboks 103,
FI-00101 Helsinki, Finland.

Bankens aktiviteter overvåkes også med hensyn til forbrukerspørsmål av
det finske forbrukerombudet (www.kkv.fi),
Finnish Competition and Consumer Authority,
Pb. 5,
FI-00531 Helsinki
Finland,
tlf. +358 (0)29 505 3000 (sentralbord).

NORGE
Virksomheten til Danske Bank i Norge overvåkes av Finanstilsynet,
Revierstredet 3,
0151 OSLO
Postboks 1187 Sentrum
0107 OSLO
Norge

SVERIGE
Danske Bank A/S, Danmark, filialen i Sverige, er autorisert av det danske finanstilsynet og overvåkes også av det svenske finanstilsynet.

STORBRITANNIA
Autorisert og regulert av det danske finanstilsynet. Autorisert av Prudential Regulation Authority. Underlagt regulering av Financial Conduct Authority og begrenset regulering av Prudential Regulation Authority. Mer informasjon om omfanget av Prudential Regulation Authoritys regulering av oss er tilgjengelig fra oss på forespørsel.

Registrert filial i England og Wales, selskapsnr. FC011846, filial nr. BR000080. Danske Bank A/S, et aksjeselskap stiftet i Danmark, CVR-nr. 61 12 62 28, København.

POLEN
Bankens virksomhet overvåkes av:
Komisja Nadzoru Finansowego (det polske finanstilsynet) med registrert virksomhetsadresse på 20, Piękna str., 00-549 Warszawa,
med hensyn til alle forhold nevnt i de relevante bestemmelsene i den polske bankloven; samt det danske finanstilsynet med forretningsadresse Strandgade 29, DK-1401 København K.