Forretningsbetingelser District

10. Mai 2021

Danske Bank

Innhold

Innhold 2
Innledning 4
Del 1 – District – generelt 4
1. Moduler og tjenester 4
2. Transaksjoner 4
3. Registrerte konti 4
3.1. Konti i Danske Bank-konsernet 4
3.2. Konti, som håndteres via SWIFT 4
3.3. Konti i annen norsk bank 4
4. Ikke-registrerte konti 5
5. Betaling via sjekk 5
6. Ordre 5
6.1. Ordreavgivelse 5
6.2. Bindende ordre 5
6.3. Oppbevaring av ordre 5
7. Bruk av elektronisk kommunikasjon - eArkiv 5
7.1. Hvem har adgang til dokumentene 6
7.2. Oppbevaring 6
7.3. Stopp av levering av dokumenter i eArkiv 6
7.4. Opphør 6
8. Brukerfullmakt District 6
8.1. Tilgang via digitale kanaler 6
8.2. Administrasjonsrettigheter 6
8.3. Avtaleadministrasjon 7
8.4. Brukeradministrasjon 7
8.5. Avtaleinformasjon 7
8.6. Adgang og sperring 7
8.7. Beløpsgrense på konto 7
8.8. Kontoadgang 8
8.9. Transaksjonstyper 8
8.10. Fortrolige betalinger 8
8.11. Endring av Brukerfullmakt District 9
8.12. Tilbakekalling av brukerfullmakt til District 9
9. Andre fullmakter i District 9
9.1. Bestilling av basisprodukter 9
9.2. Fullmakter til bedriften fra andre selskaper (tredjemann) 9
9.3. Fullmakt til kjøp/salg av valuta og verdipapirer 10
9.4. Fullmakt til Trade Finance i District 10
9.5. Fullmakt for Collection Service – SEPA Direct Debit i District 10
10. Fullmaktstyper 10
10.1. Fullmaktstyper 10
10.2. Alene-fullmakt 10
10.3. To i fellesskap (A-fullmakt) 10
10.4. To i fellesskap (B- fullmakt) 11
10.5. To i fellesskap (C-fullmakt) 11
11. Kundesupport 11
Del 2 – District sikkerhetssystem 11
12. Tekniske forhold 11
12.1. Overførings- og adgangsforhold 11
12.2. Distribusjon, kontroll og oppbevaring av programmet 12

12.3. Datasikkerhet 12
12.4. eSafeID 12
12.5. BankID 13
12.6. e-Safekey 13
12.7. EDISec 13
12.8. OpenPGP Security 13
12.9. EDISec-nøkler og OpenPGP Security-sertifikater 14
13. Adgang 14
13.1. Tildeling av bruker-ID, midlertidig passord og kodebrikke 14
13.2. Oppbevaring av bruker-ID, personlig passord og kodebrikke 15
13.3. Sletting eller sperring av bedriftens eller brukerens tilgang til District 15
13.4. Bankens rett til å sperre bedriftens eller brukerens tilgang til District 15
14. Krypteringsforbud 16
Del 3 - Avtalerettslige forhold 16
15. Krav om bruk i næringsvirksomhet 16
16. Endring av District 16
17. Endring av service og support 16
18. Ansvar 16
18.1. Bedriftens ansvar 16
18.2. Bankens ansvar 17
19. Andre vilkår og betingelser 17
19.1. District avtalens oppbygning 17
19.2. Priser 18
19.3. Andre endringer av District avtalen 18
19.4. Overdragelse og bruk av underleverandører 18
20. Oppsigelse og mislighold 18
21. Lovvalg og verneting 18
22. Definisjoner og ordforklaringer 18

Innledning

District er Danske Banks internettbaserte selvbetjeningssystem som gir adgang til kontoinformasjon, betalinger og andre bankforretninger som din bedrift etterspør.

I forretningsbetingelsene for District finner du en beskrivelse av District.

Del 1 – beskriver mulighetene i District og hvordan systemet brukes.
Del 2 – beskriver de sikkerhetsmessige krav i forbindelse med bruk av District.
Del 3 – beskriver de avtalemessige forhold i forbindelse med etablering av District.

Del 1 – District – generelt

1. Moduler og tjenester

District består av separate moduler og tjenester.
I modulbeskrivelsen finnes en beskrivelse av de moduler og tjenester som er tilknyttet bedriftens avtale om District.

2. Transaksjoner

Med District kan bedriften blant annet foreta betalinger og forespørsler på saldo og bevegelser på konti som er registrert i District, via avtalen. Betalinger og forespørsler betegnes under ett som transaksjoner.

3. Registrerte konti

Konti skal registreres i District for at en bedrift kan foreta transaksjoner via District. Kontiene registreres via Avtale om District.

3.1. Konti i Danske Bank-konsernet

Med konti i Danske Bank-konsernet menes konti som er opprettet i Danske Bank og alle andre konsernforbundne selskaper av banken under denne avtale.

Følgende konti i Danske Bank-konsernet kan registreres i District

- Konti, som tilhører bedriften og er opprettet i bedriftens navn
- Konti, som tilhører andre bedrifter inkludert datterselskaper. Det forutsetter at disse selskap eller datterselskap har avgitt en fullmakt til bedriften som gir bedriften adgang til å disponere på deres vegne

Registrerte konti i Danske Bank –konsernet kan også håndteres via SWIFT MT101eller MT940, se beskrivelsen i avsnitt 3.2.

3.2. Konti, som håndteres via SWIFT

Konti som er opprettet i banker utenfor Danske Bank-konsernet samt konti i konsernet, hvor bedriften ønsker å foreta transaksjoner via SWIFT MT101 eller MT940, kan også registreres i District. Bedriften kan registrere både egne konti og andre selskaps konti. Bedriften eller andre selskap skal inngå en avtale med den bank hvor kontiene er opprettet om en betalingsanmodning via MT101 eller en avtale om Balance Reporting via MT940.

Andre selskaps konti kan kun registreres hvis de har gitt fullmakt til bedriften.

3.3. Konti i annen norsk bank

Konto som er opprettet i annen norsk bank utenfor Danske Bank-konsernet, hvor bedriften ønsker å foreta transaksjoner eller se saldo, kan også registreres i District. Bedriften kan registrere både egne og andre selskaps konti. Bedriften eller det andre selskap skal inngå en egen avtale med Danske Bank og den bank hvor kontoen er opprettet.

Andre selskaps konti kan kun registreres hvis de har gitt fullmakt til bedriften.

Danske Bank
Foretaksregisteret NO 977 074 010 MVA

Danske Bank A/S
Erhvervs- og Selskabsstyrelsen CVR-nr. 61 12 62 28

Holmens Kanal 2-12
DK-1092 København K – Danmark

4. Ikke-registrerte konti

Hvis konti, som tilhører bedriften og/eller andre selskaper, ikke er registrert i District, kan det kun foretas betalinger til disse konti. Det kan ikke forespørres på eller foretas betalinger fra ikke-registrerte konti.

5. Betaling via sjekk

Bedriften kan gjennomføre en utenlands betaling ved å skrive ut en sjekk. Sjekken kan skrives ut fra registrerte konti i Danske Bank-konsernet.

Hvis bedriften og/eller andre selskaper har en avtale om betalingsanmodning via MT101, kan det også skrives ut sjekk fra registrerte konti utenfor Danske Bank-konsernet hvis dette er medtatt i avtalen mellom bedriften og/eller de andre selskap og banker utenfor Danske Bank-konsernet.

Utstedte sjekker betraktes som banksjekker, og beløpene belastes på kontoen på datoen for utstedelsen.

Bedriften kan få satt sjekkens pålydende av ikke-innløste sjekker inn på registrerte konti. Skal sjekkens pålydende av de ikke-innløste sjekker krediteres bedriftens eller tredjemanns konti, skal bedriften eller tredjemann erklære, at banken holdes skadesløs, hvis sjekken etterfølgende innløses.

6. Ordre

Når bedriften eller bedriftens brukere ber om å få gjennomført en transaksjon i District, f.eks. en betaling, kalles det en elektronisk ordre.

6.1. Ordreavgivelse

Når en bruker på vegne av bedriften og/eller tredjemann avgir en elektronisk ordre, sender banken en elektronisk kvittering. Fra det tidspunkt banken har kvittert for ordren, går risikoen for å utføre ordren i henhold til de mottatte opplysninger over til banken.

6.2. Bindende ordre

Ordre som er gjennomført i overensstemmelse med opplysningene i den elektroniske ordren, er bindende for bedriften. Banken kan derfor ikke tilbakeføre betalinger, handler med valuta eller verdipapirer eller andre transaksjoner, herunder utstedte sjekker, som er endelig utført i overensstemmelse med ordren.

6.3. Oppbevaring av ordre

Banken oppbevarer elektroniske ordre i minst 10 år. I den periode kan den bedriften og/eller tredjemann, som belastningskontoen tilhører, bestille en papirutskrift av ordren mot betaling av bankens til enhver tid gjeldende sats for ekstraordinær bistand.

7. Bruk av elektronisk kommunikasjon - eArkiv

Banken har rett til å sende alle opplysninger og meldinger som elektroniske dokumenter til eArkiv i bedriftens District.

Bedriften vil bli informert i District hver gang en ny type dokument fra banken blir tilgjengelig elektronisk i eArkiv. Banken kan dog til enhver tid beslutte å sende et dokument som ordinær post. Banken vil så langt det er mulig varsle om dette i District.

Opplysninger og meldinger bedriften har mottatt elektronisk har samme rettsvirkning som om dokumentene blir sendt som ordinær post.

Hvis bedriften er kunde i et eller flere av Danske Bank konsernets andre selskaper og det sendes dokumenter elektronisk til bedriften fra disse, vil banken også ha rett til å sende dem elektronisk til District.

Danske Bank
Foretaksregisteret NO 977 074 010 MVA

Danske Bank A/S
Erhvervs- og Selskabsstyrelsen CVR-nr. 61 12 62 28

Holmens Kanal 2-12
DK-1092 København K - Danmark

7.1. Hvem har adgang til dokumentene

Den enkelte brukers rettigheter til konti, depoter, produkter og tjenester bestemmer hvilke dokumenter brukeren får adgang til å se i eArkiv. Brukere med forespørselsadgang til kontoen/kontiene har adgang til dokumentene i eArkiv knyttet til den aktuelle konto/konti.

7.2. Oppbevaring

Banken oppbevarer som minimum de elektroniske dokumentene i eArkiv i inneværende år pluss fem år. Bedriften skal være oppmerksom på at dokumentene vil bli slettet hvis bedriften fjerner en konto, skifter kundenummer eller avslutter District. Bedriften oppfordres i disse tilfellene til selv å lagre dokumentene.

Hvis bedriften har behov for å oppbevare dokumentene lengre enn det banken stiller til rådighet via District, må bedriften selv lagre dokumentene for egen oppbevaring.

7.3. Stopp av levering av dokumenter i eArkiv

Hvis bedriften ikke ønsker å motta dokumenter i eArkiv, må banken kontaktes. Banken kan etter avtale sende dokumentene som vanlig post. Banken kan i slike tilfeller pålegge gebyr.

7.4. Opphør

Hvis bedriftens District avtale slettes, bedriften får nytt organisasjonsnummer eller det fjernes konti fra bedriftens District-avtale vil muligheten til å motta og hente ut elektroniske dokumenter fra eArkiv også opphøre tilsvarende. Se pkt. 7.2 om oppbevaring m.v.

8. Brukerfullmakt District

Bedriften skal utstede en fullmakt til en bruker, før denne kan foreta transaksjoner i District på vegne av bedriften eller andre selskaper (tredjemann). Denne fullmakten opprettes på bankens fullmaktsblankett Brukerfullmakt District.
Hvis et annet selskap har underskrevet en fullmakt til bedriften, kan bedriften overføre denne fullmakt til en bruker. Det skjer ved hjelp av Brukerfullmakt District.

Bedriften skal før opprettelse av en brukerfullmakt til District informere bruker om at navn og fødselsnummer vil bli utlevert til banken og innhente brukers samtykke til dette.

Hvis bruker har behov for å foreta transaksjoner via kassen, skal bedriften underskrive blanketten Fullmakt disponering av konto og District/PC - Næringsforhold.

8.1. Tilgang via digitale kanaler

Brukeren får automatisk tilgang til District via forskjellige nettlesere og via Business Appene, men bedriften kan velge bort tilgang via Business Appene. Ved innlogging via en slik kanal vil brukeren kun ha de tilganger som er definert i Brukerfullmakten for District.

8.2. Administrasjonsrettigheter

Bedrifter som får tilknyttet administrasjonsmodul, skal ta stilling til om bruker skal tildeles administrasjonsrettigheter. Følgende administrasjonsrettigheter kan tildeles:

- Avtaleadministrasjon
- Brukeradministrasjon
- Avtaleinformasjon
- Adgang og sperring
- Beløpsgrense - konto

For brukere som tildeles Avtale- og/eller Brukeradministrasjonsrettigheter skal bedriften ta stilling til hvilken fullmakt

bruker skal ha til disse rettighetene.
Følgende fullmakter kan tildeles:

- Opprette/Innlegger
- Alene-fullmakt
- To i fellesskap (A-fullmakt).

Se beskrivelsen av våre fullmaktstyper i avsnitt 10.

8.3. Avtaleadministrasjon

Hvis bedriften tildeler bruker Avtaleadministrasjon, gir bedriften bruker adgang til å

- opprette, endre og slette brukers Avtaleadministrasjonsrettigheter
- opprette, endre og slette brukers Brukeradministrasjonsrettigheter – se avsnitt 8.3
- opprette og slette brukers Avtaleinformasjonsrettigheter – se avsnitt 8.4
- opprette og slette brukers rettigheter vedrørende adgang og sperring – se avsnitt 8.5
- Opprette, endre og slette brukers beløpsgrense på konto – se avsnitt 8.6

Avtaleadministrator kan tildele seg selv og andre brukere disse rettigheter.

Når en bruker med rettigheten Avtaleadministrasjon oppretter eller endrer en brukerfullmakt med Avtaleadministrasjonsrettigheter, blir det generert en Brukerfullmakt District for underskrift. Brukerfullmakten er tilgjengelig i eArkiv i District for brukere med rettigheten Avtaleinformasjon. Brukerfullmakten skal underskrives av bedriften og sendes til banken. I øvrige tilfeller godkjenner og underskriver bruker med sin digitale signatur.

Brukere med rettigheten Avtaleadministrasjon skal også være tildelt rettigheten Brukeradministrasjon.

8.4. Brukeradministrasjon

Hvis bedriften tildeler bruker Brukeradministrasjon, gir bedriften bruker adgang til

- opprette og endre brukere, samt gi brukere adgang til moduler, produkter og tjenester , konti, fullmakts- og transaksjonstyper
- opprette og slette brukernes tilgang til bestilling av basisprodukter - se punkt 9.1
- opprette og endre brukers grunnopplysninger
- slette alt på en bruker inkludert grunnopplysninger.

Brukeradministrator kan tildele seg selv og andre brukere disse rettigheter.

8.5. Avtaleinformasjon

Med rettigheten Avtaleinformasjon får bruker tilgang til avtalens brukere samt se brukeres individuelle adganger (herunder grunnopplysninger, moduler, administrasjonsrettigheter, adgang til konti og betalingsadganger).
Bruker får også tilgang til utvalgte dokumenter, som vises i District.

8.6. Adgang og sperring

Hvis bedriften tildeler bruker rettigheten Adgang og sperring, gir bedriften bruker adgang til

- å bestille midlertidig pinkode til brukere
- bestille kodebrikke og fullføre aktivering av ny kodebrikke
- sperre og oppheve sperring på brukere.

8.7. Beløpsgrense på konto

Hvis bedriften tildeler bruker rettigheten Beløpsgrense - konto, gir bedriften bruker adgang til

- opprette, endre og slette beløpsgrense på de konti som brukeren til enhver tid kan disponere på avtalen.

For brukere som tildeles Beløpsgrense på kont skal bedriften ta stilling til hvilken fullmakt bruker skal ha. Følgende fullmakter kan tildeles:

- Alene-fullmakt
- To i fellesskap (A-fullmakt)
- To i fellesskap (B-fullmakt)
- To i fellesskap (C-fullmakt)

Se beskrivelsen av våre fullmaktstyper i avsnitt 10.

8.8. Kontoadgang

Bedriften skal ta stilling til hvilke konti bruker skal kunne spørre på og/eller foreta betalinger fra. Hvis bedriften gir bruker rett til å foreta betalinger fra en konto, får bruker adgang til å foreta de transaksjonstyper, som bedriften gir bruker adgang til.

For hver konto bruker får adgang til, skal det tas stilling til hvilken fullmakt bruker skal ha. På kontonivå kan det tildeles følgende fullmakter:

- Alene-fullmakt
- To i fellesskap (A-fullmakt)
- To i fellesskap (B-fullmakt)
- To i fellesskap (C-fullmakt)

Se beskrivelsen av våre fullmaktstyper i avsnitt 10.

Vær oppmerksom på at den valgte fullmakt på kontonivå vil få anvendelse på alle District-avtaler som kontoen er tilknyttet.

8.9. Transaksjonstyper

Bedriften skal ta stilling til, hvilke av følgende transaksjonstyper bruker skal ha adgang til.

- Betalinger mellom konti registrert på District-avtalen i samme land innenfor Danske Bank-konsernet
- Betalingsanmodninger via SWIFT MT101
- Betalinger til konti som ikke er registrert på District-avtalen i eller utenfor Danske Bank-konsernet– herunder betaling via sjekk
- Overføring til utlandet til konti i eller utenfor Danske Bank-konsernet.

Bedriften skal også ta stilling til, om bruker skal kunne opprette og godkjenne eller kun opprette de valgte betalinger. Hvis bruker både skal kunne opprette og godkjenne betalinger, skal det også tas stilling til, hvilken fullmakt bruker skal ha til hver transaksjonstype. Følgende fullmakter kan tildeles på transaksjonsnivå:

- Opprette/Innlegger.
- Alene-fullmakt.
- To i fellesskap (A-fullmakt).

Se beskrivelsen av våre fullmaktstyper i pkt. 10.

Den valgte fullmakt brukes som utgangspunkt på alle betalinger innenfor den enkelte betalingstype. Har bedriften valgt en mer restriktiv fullmakt på kontonivå, kommer den til anvendelse, når det foretas betalinger til ikke registrert konti og ved overføring til utlandet. Vær oppmerksom på at det også betraktes som en begrensning, hvis bedriften har valgt ikke å tildele en fullmakt på kontonivå.

8.10. Fortrolige betalinger

Bedriften skal ta stilling til, om bruker skal kunne foreta fortrolige betalinger. Med fortrolige betalinger forstås betalinger som f.eks. lønninger, som kun skal sees, opprettes eller godkjennes av bruker med denne rett.

Bruker får adgang til å foreta fortrolige betalinger innenfor de transaksjonstyper, som bedriften har gitt bruker adgang til.

Vær oppmerksom på at det ikke skjelnes mellom fortrolige betalinger og ikke-fortrolige betalinger ved forespørsel på en konto.

8.11. Endring av Brukerfullmakt District

Ønsker bedriften å utvide eller innskrenke en brukers adgang i District, skal det utstedes en ny Brukerfullmakt District, som erstatter den tidligere brukerfullmakt til District. Hvis endringen vedrører brukers fullmaktsforhold på kontonivå skal bedriften og/eller tredjemann også underskrive en kontofullmakt.

Vær forøvrig oppmerksom på at en brukers fullmakt til District kan påvirkes hvis bedriften utsteder en fullmakt til disponering av konto (kontofullmakt).

8.12. Tilbakekalling av brukerfullmakt til District

Brukerfullmakt District gjelder inntil bedriften kaller den tilbake. Det kan bedriften gjøre skriftlig. Fullmakten kan også kalles tilbake pr. telefon, men tilbakekallingen skal alltid følges opp med en skriftlig bekreftelse umiddelbart etter. Brukers adgang til å handle på bedriftens vegne via District sperres etter den telefoniske henvendelsen.

Når banken har mottatt en tilbakekalling, bekrefter banken skriftlig at brukernummer og brukers nøkler er slettet i bankens systemer.

Hvis bedriften sier opp District avtalen, ser banken det som en tilbakekalling av alle de brukerfullmakter som er utstedt i henhold til avtalen.

Hvis bedriften og/eller en tredjemann har gitt bruker en kontofullmakt, skal denne fullmakt kalles tilbake særskilt. Det er altså ikke tilstrekkelig at bedriften bare kaller brukerfullmakten til District tilbake.

9. Andre fullmakter i District

9.1. Bestilling av basisprodukter

Med District Administrasjon har du tilgang til Bestilling av basisprodukter slik at du kan inngå avtaler om basisprodukter i District.
Hvis du tildeler en bruker fullmakt til Bestilling av basisprodukter autoriserer du brukeren til å inngå bindene avtaler - på vegne av selskapet – om produkter tilgjengelig til enhver tid i Bestilling av basisprodukter i District.

9.2. Fullmakter til bedriften fra andre selskaper (tredjemann)

Hvis bedriften skal foreta transaksjoner på andre selskapers konti i Danske Bank-konsernet, skal selskapet undertegne bankens tredjemannsfullmakt.

Hvis det skal kunne forespørres på andre selskapers konti plassert utenfor Danske Bank-konsernet, skal banken motta tilfredsstillende dokumentasjon på at bedriften, via Danske Bank-konsernet, skal motta opplysninger om dette selskapets konti fra selskapets bank(er).

Hvis bedriften skal kunne gjennomføre betalinger fra andre selskapers konti utenfor Danske Bank-konsernet, skal banken motta tilfredsstillende dokumentasjon på at bedriften via Danske Bank –konsernet kan sende instruksjoner om betalinger til dette selskapets bank(er).

Banken registrerer andre selskapers konti til District via bedriftens Avtale om District.

9.3. Fullmakt til kjøp/salg av valuta og verdipapirer

Hvis en bruker skal ha adgang til informasjon, skal kunne se posisjoner over forretninger samt kjøp og salg av valuta på spot og termin, norske og utenlandske aksjer, obligasjoner og investeringsbeviser, skal bruker ha adgang til en eller flere av Markets Online-modulene. Adgang til kjøp og salg av valuta på spot og termin samt kjøp og salg av aksjer, obligasjoner og investeringsbeviser krever at bedriften utsteder fullmakten Valutaforretninger og/eller fullmakten Fondsforretninger til bruker. Fullmaktene gir alene bruker fullmakt til å inngå transaksjoner på bedriftens vegne via Markets Online.

Alle forretninger vedrørende kjøp og salg av valuta på spot og termin er underlagt betingelser i Derivatavtalen, som er inngått mellom bedriften og banken.

I Brukerfullmakt District angis hvilke konti og depoter bruker skal kunne forespørre på og handle over.

9.4. Fullmakt til Trade Finance i District

Hvis en bruker skal utstede remburser, inkasso og/eller garantier, skal bedriften tildele bruker Trade Finance modulen og underskrive avtalen Tilslutning/endring til Trade Finance modulen i District. Bedriften må ta stilling til om bruker skal ha adgang til

- remburser (eksport og/eller import)
- inkasso (eksport og/eller import)
- garantier.

Bedriften skal forøvrig ta stilling til om bruker skal kunne

- opprette og forespørre
- opprette og godkjenne to i fellesskap (A-fullmakt) eller
- opprette og godkjenne alene (Alene-fullmakt).

9.5. Fullmakt for Collection Service – SEPA Direct Debit i District

Hvis en kunde skal lage en SEPA Direct Debit-oppkreving, må virksomheten melde inn brukeren i Collection Service – SEPA Direct Debit-modulet. Brukeren vil da få tilgang til følgende:

- Oppkrevinger
- Refusjoner
- Tilbakekallelser

Dette gjelder for eurokonti knyttet til District.

10. Fullmaktstyper

10.1. Fullmaktstyper

I banken finnes følgende fullmaktstyper i District:

- Alene-fullmakt
- To i fellesskap (A-fullmakt)
- To i fellesskap (B- fullmakt)
- To i fellesskap (C- fullmakt)

Med disse fullmakter kan bedriften bestemme hvilke brukere som sammen eller alene må godkjenne en betaling eller en ordre. Fullmaktene beskrives i de følgende avsnitt.

10.2. Alene-fullmakt

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

10.3. To i fellesskap (A-fullmakt)

Når en ordre eller betaling opprettes av en bruker med A-fullmakt, er den automatisk godkjent av denne (1. godkjennelse).

Ordren eller betalingen krever ennå en godkjennelse (2. godkjennelse) av en bruker med enten Alene-, A-, B- eller C-fullmakt
Brukere med A-fullmakt er sideordnet, og godkjennelsesrekkefølgen er derfor underordnet.

10.4. To i fellesskap (B- fullmakt)

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

10.5. To i fellesskap (C-fullmakt)

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

11. Kundesupport

Banken stiller support og service til rådighet for bedriften. Support og service omfatter

- brukeradministrasjon
- support hos bedriften
- telefonsupport
- internettbaserte supportfunksjoner.

Brukeradministrasjon kan omfatte etablering av District avtale og fullmakter, tilpasning av bedriftens og brukeres adgang til de enkelte deler av support og service, sletting og sperring av brukere, bestilling av engangspinkoder og registrering av endrede fullmaktsforhold m.v.

Support hos bedriften kan omfatte oppsetting og undervisning i bruken av District og feilsøking i relasjon til District. Feilsøking kan medføre tilrettinger og/eller endringer av maskinenes oppsettinger og i bedriftens it-systemer, herunder endringer i registreringsdatabaser, oppsetting av rutere, firewalls, proxyservere, interne sikkerhetssystemer samt endringer av oppsetting av software og hardware forøvrig. Oppsetting og feilsøking skjer i samarbeid med bedriftens it-avdeling og på bedriftens ansvar.

Telefonsupport kan omfatte undervisning, veiledning i bruk, hjelp til feilfinning og veiledning for tilpasninger. Telefonsupport i forbindelse med installasjon, oppsetting, undervisning og feilfinning m.v. av District skjer i samarbeide med bedriftens it-avdeling og på bedriftens ansvar.

Internettbaserte supportfunksjoner kan omfatte undervisning, veiledning i bruk, hjelp til feilfinning samt veiledning for tilpasninger. Bruken av internettbaserte supportfunksjoner skjer i samarbeide med bedriftens it-avdeling og på bedriftens ansvar.

Del 2 – District sikkerhetssystem

12. Tekniske forhold

12.1. Overførings- og adgangsforhold

For å benytte District skal bedriften etablere en datakommunikasjonsforbindelse til banken. Bedriften skal etablere og dekke utgiftene til forbindelsen og selv sørge for å anskaffe, installere, sette opp og vedlikeholde det nødvendige IT-utstyret.

Bedriften skal dessuten sørge for de nødvendige tilpasninger av bedriftens IT-

utstyr – både for å bruke forbindelsen og for den fortsatte drift.

Det skal ikke benyttes spesiell programvare, som f.eks "overlay services" eller lignende former for programvare når District brukes. Systemet skal betjenes direkte av brukere via det brukergrensesnittet og de programmene banken stiller til rådighet.

12.2. Distribusjon, kontroll og oppbevaring av programmet

Banken distribuerer de programmene som skal brukes for å installere District. Disse kan lastes ned fra internett.
Når programmene lastes ned fra internett, skal det kontrolleres at programleveransen er elektronisk signert av banken.

Dersom programmene ikke er elektronisk signert av banken, kan det være fordi programmene er endret, eller ikke er opprinnelig fra banken. Underskriften kan verifiseres ved å kontrollere "egenskaper" på den eller de nedlastede programfilene. Dersom det oppdages at den elektroniske signaturen ikke tilhører banken, skal dere ikke installere programvaren.

Banken kan til enhver tid uten varsel endre bankens eget materiale, basisprogrammer og dertil hørende prosedyrer for å sikre best mulige driftsforhold og servicenivå. Banken informerer om endringer som medfører at bedriften må tilpasse sitt utstyr for å opprettholde forbindelsen og adgangen, med en måneds varsel. Det skjer skriftlig gjennom District eller på annen måte.

12.3. Datasikkerhet

BankID, eSafeID, e-Safekey, EDISec og OpenPGP Security er de generelle sikkerhetssystemene i District.
BankID og esafeID er sikkerhetsløsninger for webbasert innlogging og signering i District.

e-Safekey, EDIsec og OpenPGP Security er bankens sikkerhetssystemer til de kundene som ønsker å utveksle opplysninger elektronisk med banken direkte gjennom deres egne forretningssystemer.

e-Safekey, EDIsec og OpenPGP Security er bygget opp rundt et passord som benytter permanente nøkkelfiler som lagres i bedriftens IT-miljø.
Bruk av disse sikkerhetssystemene sikrer at data er kryptert og/eller elektronisk signert før de sendes til og fra Danske Bank og ikke er endret under forsendelse. I tillegg vil avsenders digitale signatur alltid kontrolleres, og alle finansielt forpliktende transaksjoner være utstyrt med en digital signatur.

12.4. eSafeID

eSafeID er bankens webbaserte sikkerhetssystem som benyttes til å logge på District. eSafeID er bygget opp rundt to faktorer – noe man vet og noe man har: et personlig passord og en såkalt kodebrikke som genererer koder. Kodene som man får fra kodebrikken kan kun brukes én gang og lagres midlertidig i browser-sesjonen i det tidsrommet brukeren er logget på District.

Når en person skal opprettes som bruker i District med e-SafeID-sikkerhetssystemet, får brukeren en individuelt tildelt bruker-id, en engangskode og en kodebrikke.
Brukeren skal aktivere kodebrikken og opprette en personlig kode før eSafeID-sikkerhetssystem kan benyttes for å få tilgang til District.

Aktivering av kodebrikken krever to faktorer hvor engangskoden utgjør den ene faktoren. Har brukeren registrert mobilnummer ved opprettelse kan en

aktiveringskode sendes og utgjøre den andre faktoren. Brukeren kan også aktivere kodebrikken ved bruk av BankID. Alternativt kan administrator på avtalen fullføre aktivering av bruker.

Aktive brukere som mottar en ny kodebrikke skal aktivere kodebrikken før den kan benyttes. Aktivering skjer som beskrevet over.

12.5. BankID

Bruk av BankID forutsetter at bruker har norsk fødselsnummer (11 siffer) eller d-nummer og har en BankID utstedt av den banken brukeren er privatkunde i.
BankID gjør det mulig for brukeren å logge inn og signere uten bruk av annen sikkerhetsløsning.
BankID er standard sikkerhetsløsning for brukere med norsk fødsels og personnummer.
For BankID er følgende innloggings- og signeringsmuligheter tilgjengelig:

- BankID

Ved innlogging med BankID tilbys brukeren med tilgang til flere District avtaler muligheten for etter innlogging å velge hvilken avtale den vil arbeide på og veksle mellom avtaler uten ny innlogging.

12.6. e-Safekey

e-Safekey er en sikkerhetskomponent som benyttes i Danske Banks Business API-løsning. Når en bruker skal opprettes i District med e-Safekey-sikkerhetssystemet får brukeren en individuelt tildelt bruker-id og et midlertidig passord. Det midlertidige passordet brukes som førstegangsidentifikasjon under opprettelsen i sikkerhetssystemet.

12.7. EDISec

EDISec er et sikkerhetssystem brukt ved integrering mot Danske Banks systemer via datakommunikasjonsforbindelser. Når en bruker skal opprettes for datakommunikasjon med EDISec-sikkerhetssystemet får brukeren en individuelt tildelt bruker-id uten et midlertidig passord. Gyldighetstiden for kundens offentlige EDIsec-nøkkel sikres gjennom å generere et fingeravtrykk av nøkkelen og utveksle dette med Danske Bank i henhold til EDISec Implementation Guide.

12.8. OpenPGP Security

OpenPGP Security er et sikkerhetssystem brukt ved integrering mot Danske Banks systemer via datakommunikasjonsforbindelser. Når en bruker skal opprettes for datakommunikasjon med OpenPGP Security-sikkerhetssystemet får brukeren en individuelt tildelt bruker-id og et midlertidig passord. Kunden genererer et OpenPGP Security-sertifikat som inneholder sikkerhetsnøklene. Sertfikatet sendes til Danske Bank sammen med det midlertidige passordet i henhold til OpenPGP Security Implementation Guide.

Hvis et OpenPGP Security offentlig sertifikat utstedes av en tredjepart på vegne av kunden, vil Danske Bank anse kunden som innehaver av nøkkelen og således også ansvarlig for gyldigheten og forvaltningen av sertifikatet. Danske Bank benytter den offentlige kryptografiske nøkkel som er i sertifikatet.

Det er kundens ansvar å gå til anskaffelse av, samt vedlikeholde, programvare for OpenPGP Security, uavhengig av om det er kundens eget eller om det er anskaffet gjennom en tredjepart. Blant funksjonaliteten systemet må støtte er

håndtering av sertifikater samt muligheten for kryptering og signering.

12.9. EDISec-nøkler og OpenPGP Security-sertifikater

For både EDISec og OpenPGP Security er kunden selv ansvarlig for å sikre at det til enhver tid benyttes gyldige nøkler til å sikre datakommunikasjonen. Mer spesifikt må kunden sørge for at:

- Danske Bank har et gyldig sett av kundens offentlige nøkler. Når kundens offentlige nøkler nærmer seg utløp, må kunden selv fornye egne offentlige nøkler og deretter utveksle disse med Danske Bank.
- Kunden benytter et gyldig sett av Danske Banks offentlige nøkler for sikring av datakommunikasjonen. Når bankens offentlige nøkler nærmer seg utløp, må kunden selv oppdatere eget system med de nye offentlige nøklene som tilgjengeliggjøres av banken. Hvis kundens nøkler har blitt kompromittert eller skadet, må de ugyldiggjøres ved å kontakte banken.

Når Danske Bank mottar kundens offentlige EDISec-nøkkel eller offentlige OpenPGP Security-sertifikater vil nøklene/sertifikatene lagres sikkert i Danske Banks systemer, og vil ikke deles med parter utenfor Danske Bank.

Det er Danske Banks ansvar å sørge for at et gyldig sett av bankens offentlige EDISec-nøkkel eller OpenPGP Security-sertfikater alltid er tilgjengelig for kunden.

13. Adgang

13.1. Tildeling av bruker-ID, midlertidig passord og kodebrikke

Når en person skal opprettes som bruker i District med e-SafeID sikkerhetssystemet, får brukeren en individuelt bruker-id, en engangskode og en kodebrikke. Engangskoden brukes som førstegangsidentifikasjon under opprettelsen sammen med kodebrikken.

Når en bruker opprettes med e-EDIsec eller OpenPGP Security får brukeren tildelt en individuelt bruker-id. Ved OpenPGP tildeles også en engangskode..

Engangskoden konstrueres og skrives ut maskinelt, uten at noen får kjennskap til koden. Hvis brevet med engangskoden og/eller brevet med kodebrikken har vært åpent eller er ødelagt, skal brukeren kontakte banken og bestille en ny engangskode og/eller en ny kodebrikke. Av sikkerhetsmessige årsaker blir brevene med kodebrikke og midlertidig passord sendt adskilt.

Hvis brukeren ikke har mottatt brevet med engangskoden innen syv hverdager etter bestillingen, skal brukeren av sikkerhetsmessige årsaker, kontakte banken for å annullere den og bestille en ny..

Hvis brukeren har registrert sitt mobilnummer i District, kan brukeren motta det midlertidige passordet i en tekstmelding. Hvis brukeren ikke mottar meldingen med det midlertidige passordet innen 15 minutter etter at det er bestilt, må brukeren av sikkerhetshensyn kontakte Danske Bank for å avbryte prosessen og bestille et nytt. Ved opprettelsen velger brukeren sitt eget, personlige passord. Passordet skal endres regelmessig som er

kundens ansvar. Etterfølgende skal engangskoden makuleres av bruker. Danske Bank er ikke ansvarlig for eventuelle feil eller tap forårsaket av brukerens eller administratorens feil ved oppdatering av brukerens mobiltelefonopplysninger i District.

13.2. Oppbevaring av bruker-ID, personlig passord og kodebrikke

Bedriften skal implementere sikkerhetsprosedyrer som forhindrer uautorisert bruk av District og uautorisert tilgang til brukerens nøkkelfiler og kodebrikke.

Følgende regler gjelder for bruk av eSafe-ID, eSafekey, EDIsec og OpenPGP Security.

- Bruker-id, passord og kodebrikke skal kun anvendes av bruker.
- Passord, kodebrikke og nøkler er strengt personlige og må ikke deles med tredjepart/personer.
- Passord og sikkerhetskoder skal kun benyttes ved kommunikasjon med banken (OpenPGP kan også benyttes i andre sammenhenger)
- Man skal ikke skrive passordet ned.
- Danske Bank anbefaler at å oppbevare hemmelige nøkler i krypto hardware.

Se også anbefalinger om sikkerhet som er nevnt i menypunktet Sikkerhet i District på Danske Bank sin hjemmeside og i andre veiledninger.

13.3. Sletting eller sperring av bedriftens eller brukerens tilgang til District

Kunden skal gi banken beskjed dersom det er ønskelig at banken skal slette bedriftens eller brukerens tilgang til District. Kunden eller brukeren skal straks kontakte banken for å få sperret en brukers tilgang dersom:

- Det er mistanke om misbruk av det personlige passordet, bedriftens/brukerens nøkkelfil eller kodebrikke
- Andre har fått kjennskap til det personlige passordet, personlig nøkkelfil eller er i besittelse av kodebrikken.
- For BankID som sikkerhetsløsning må brukerens ID sperres/avsluttes da brukeren kan logge på g signere uten at særskilt sikkerhetsløsning er mottatt fra banken.

Melding om sperring eller opphevelse av sperring kan gis via District, telefon eller via bankens filialer. Hvis meldingen gis via telefon skal meldingen etterfølgende bekreftes skriftlig. Brukeren vil bli sperret i den mellomliggende perioden.

Kunden er ansvarlig for alle transaksjoner som gjennomføres av brukeren inntil banken har fått beskjed om å slette eller sperre en bruker. Kunden er også ansvarlig for alle fremtidige transaksjoner som tidligere er opprettet av en slettet/sperret bruker, inntil banken får beskjed om at transaksjonene skal slettes.

En bruker med Administrasjonsrettigheter kan både slette og sperre en brukers tilgang til District. jfr. pkt. 8.3 og 8.4

13.4. Bankens rett til å sperre bedriftens eller brukerens tilgang til District

Banken kan sperre bedriftens eller brukerens tilgang til District ved konstante forsøk på misbruk. Banken forbeholder seg videre retten til å sperre bedriftens tilgang til District hvis bedriftens utstyr, software eller interface skades, forstyrrer eller på annen måte er til hinder for banken eller bankens IT-infrastruktur. Hvis banken

sperrer tilgang blir bedriften varslet snarest mulig.

14. Krypteringsforbud

Lokal, nasjonal lovgivning i det landet District benyttes, kan inneholde et generelt forbud mot, eller begrensninger mot kryptering. Det er derfor viktig å kjenne landets lovgivning.

Del 3 - Avtalerettslige forhold

15. Krav om bruk i næringsvirksomhet

District skal brukes i næringsvirksomhet. Den informasjon som stilles til bedriftens disposisjon, herunder kursopplysninger, er kun til bedriftens egen bruk. Det er ikke tillatt å gi opplysningene videre til andre, med mindre banken har gitt skriftlig tillatelse.

16. Endring av District

District gir adgang til de produkter og tjenester som banken til enhver tid tilbyr.

Banken kan til enhver tid utvide eller innskrenke omfanget av District. Banken kan utvide omfanget og/eller innhold uten varsel. Når banken tilføyer nye produkter og tjenester krever ikke dette ny underskrift fra kunden, hvis endringen er til fordel for kunden og ikke innebærer vesentlige økte omkostninger for kunden. Hvis tjenestens omfang og/eller innhold begrenses, vil dette varsles 30 dager på forhånd.

Banken informerer skriftlig om endringer i District gjennom District eller på annen måte. Bedriften anses å ha akseptert endringene i District hvis bedriften ikke varsler banken skriftlig om det motsatte og sier opp District avtalen før iverksettelsen.

17. Endring av service og support

Banken kan til enhver tid endre omfang og innhold av service og support med en måneds varsel. Varsel kan sendes skriftlig, gjennom District eller på annen måte. Prisen for de aktuelle deler av service og support står i prislisten.

18. Ansvar

18.1. Bedriftens ansvar

Bruken av District skjer på bedriftens eget ansvar og egen risiko.

Bedriften bærer eksempelvis - men ikke begrenset til – risikoen for:

- forsendelse av opplysninger til banken og risikoen for at en forsendelse tilintetgjøres, kommer bort, skades, forsinkes, eller det oppstår feil og mangler i forsendelsen, blant annet ved gjennomstillingssentralers behandling eller bearbeidelse av datamateriale
- at opplysninger kommer til tredjemanns kjennskap som følge av feil eller uberettiget inntrengen på dataoverføringsforbindelsen
- misbruk i District.

Bedriften kan ikke gjøre banken ansvarlig for eventuelle følgeskader av dette.

Det er bedriftens ansvar å

- kontrollere at innholdet av brukerfullmaktene alltid stemmer overens med de fullmakter som bedriften og en eventuell tredjemann har gitt til bruker.
- kontrollere at innholdet av brukerfullmakten for øvrig stemmer overens med bedriftens ønsker.

Det er dessuten bedriftens ansvar, at bruker(e) kjenner forretningsbetingelsene for District, og at hver bruker overholder dem, herunder følger anvisningene i de

hjelpetekster som fremgår på skjermbildene.

Bedriften er ansvarlig for

- alle disposisjoner og transaksjoner som foretas med bedriftens egen nøkkel eller av brukernes nøkler
- at bruker sikrer at deres personlige kode oppbevares forsvarlig og ikke kommer til tredjemanns kunnskap
- å sikre datasikkerheten i forbindelse med lagring av brukers nøkler i bedriftens edb-miljø, så uautorisert adgang til nøklene forhindres
- brukernes eventuelle feilaktige bruk eller misbruk av District.

Bedriften kan ikke gjøre innsigelser gjeldende mot banken, hva angår feil og mangler som skyldes bedriftens egne forhold, herunder manglende overholdelse av sikkerhets- og kontrollprosedyrer.

18.2. Bankens ansvar

Banken er erstatningsansvarlig hvis den på grunn av feil eller forsømmelser oppfyller avtalte forpliktelser for sent eller mangelfullt.

Banken er dog ikke erstatningsansvarlig for feil og mangler som skyldes

- feil og mangler i tredjemanns software som er en del av District sikkerhetssystemet
- en brukers avsløring av engangspinkoden og/eller personlig kode
- endringer av sikkerhetssystemet (som ikke er gjennomført av banken)
- sikkerhetssystemets integrasjon med andre systemer eller software som ikke er levert av banken.

På de områder hvor det gjelder et strengere ansvar, er banken forøvrig ikke ansvarlig for tap, som skyldes

- nedbrudd i eller manglende adgang til it-systemer eller beskadigelse av data i disse systemer som kan henføres til nedennevnte begivenheter, uansett om det er banken selv eller en ekstern leverandør som står for driften av systemene
- svikt i bankens strømforsyning eller telekommunikasjon, lovinngrep eller forvaltningsakter, naturkatastrofer, krig, opprør, borgerlige uroligheter, sabotasje, terror eller hærverk (herunder computervirus og -hacking)
- streik, lockout, boikott eller blokade, uansett om konflikten er rettet mot eller iverksatt av banken selv eller dens organisasjon og uansett konfliktens årsak. Det gjelder også når konflikten bare rammer deler av banken
- andre omstendigheter som er utenfor bankens kontroll.

Bankens ansvarsfrihet gjelder ikke hvis

- banken burde ha forutsett det forhold som er årsak til tapet da avtalen ble inngått eller burde ha unngått eller overvunnet årsaken til tapet
- lovgivningen under alle omstendigheter gjør banken ansvarlig for det forhold som er årsak til tapet.

Banken er i overensstemmelse med alminnelige gjeldende ansvarsregler ansvarlig for direkte tap som kan henføres til feil i banken. Bankens ansvar er utover dette begrenset til å avhjelpe manglene. Ytterligere ansvar kan ikke gjøres gjeldende, heller ikke ansvar for indirekte følger eller avledede skadevirkninger.

19. Andre vilkår og betingelser

19.1. District avtalens oppbygning

En District avtale består av:

- Avtale om District
- Brukerfullmakt(er) District

- Modulbeskrivelse District
- Forretningsbetingelser District
- Generelle vilkår for innskudd og betalingsoppdrag - næringsforhold
- Priser for District
- Brukerveiledningen "Kom godt i gang" på District hjemmesiden og hjelpetekster på skjermbildene.

I tillegg gjelder også de betingelser og regelsett, som fremgår av de enkelte modulavtaler.

Når bedriften underskriver District avtalen, kvitterer bedriften samtidig for å ha lest og akseptert ovennevnte betingelser og regelsett, som er en del av avtalen.

Forretningsbetingelser District og andre gjeldende forretningsbetingelser kan ses og lastes ned fra www.danske-bank.no/betingelser.

19.2. Priser

Banken kan til enhver tid endre priser etter forutgående varsel. Det kan skje skriftlig gjennom District eller på annen måte. Banken belaster diverse avgifter og gebyrer på den konto eller de konti, banken har fått opplyst som gebyrkonto.

19.3. Andre endringer av District avtalen

Banken kan endre District avtalen til skade for bedriften en måned etter at banken har sendt skriftlig varsel til bedriften i District eller på annen måte om endringen. Bedriften anses for å ha akseptert endringen hvis ikke bedriften varsler banken skriftlig om det motsatte og sier opp District avtalen før iverksettelsesdatoen.

19.4. Overdragelse og bruk av underleverandører

Avtalen om District er inngått av banken på vegne av Danske Bank-konsernet. Det innebærer at ethvert medlem av Danske Bank-konsernet er berettiget til å oppfylle og håndheve avtalen. Det betyr også, at banken på ethvert tidspunkt kan overdra sine rettigheter og plikter til et annet medlem av Danske Bank-konsernet.

Banken har rett til å benytte underleverandører. Bruk av underleverandører påvirker ikke bankens ansvar i henhold til avtalen om District

20. Oppsigelse og mislighold

Bedriften kan si opp District avtalen uten varsel. Oppsigelse skal gis skriftlig. Ordre og avtaler, som er inngått før oppsigelsen vil bli gjennomført. Betalt abonnementsavgift refunderes ikke.
Banken kan si opp District avtalen skriftlig med en måneds varsel.
Banken kan dog si opp avtalen uten varsel, hvis bedriften misligholder avtalen, herunder også forretningsbetingelsene for District. Det foreligger mislighold blant annet hvis bedriften unnlater å betale i henhold til avtalen, stanser sine betalinger, kommer under konkurs eller annen insolvensbehandling, innleder akkord eller utsettes for utlegg eller arrest.

21. Lovvalg og verneting

Tvister eller krav og alle forhold forøvrig mellom kunden og banken oppstått i forbindelse med eller som har tilknytning til disse forretningsvilkår, skal løses etter norsk rett med Trondheim tingrett som verneting.

Hvis bedriften benytter en modul, hvis formål utelukkende er å bli benyttet i utlandet, aksepterer bedriften – i samme omfang som banken – å være underlagt de rettsregler og sedvaner som gjelder i det land hvor bedriften opererer.

22. Definisjoner og ordforklaringer

Danske Bank
Foretaksregisteret NO 977 074 010 MVA

Danske Bank A/S
Erhvervs- og Selskabsstyrelsen CVR-nr. 61 12 62 28

Holmens Kanal 2-12
DK-1092 København K – Danmark

- **Avtale om District**: Avtale om bruk av District mellom bedriften og banken.
- **Bankdager:** Lørdag, søn- og helligdag samt grunnlovsdag og julaften, er ikke bankdager i Norge.
- **Basis produkter:** er enkle produkter. Modulen består av de produkter som til enhver tid er tilgjengelig i District. (Tilbudet vil kunne endres over tid).
- **Betalinger mellom registrerte konti:** Betalinger mellom registrert konti i samme land innenfor Danske Bank-konsernet.
- **Bruker:** En bruker er en person (f.eks. en medarbeider), som er bemyndiget av bedriften til å disponere på bedriftens vegne via District. Ved direkte integrasjon mellom bedriftens og bankens edb-system, kan en bruker dessuten være en computer eller et system hos bedriften.
- **Bruker-id:** Nummer på seks posisjoner som tildeles den enkelte bruker av District. Kan inneholde både tall og store bokstaver. Bruker-id står i brukerfullmakten.
- **Brukerfullmakt:** Bedriftens fullmakt til bruker som spesifiserer hvilke tjenester, konti, fullmakter og rettigheter den enkelte bruker har adgang til.
- **Business Online** er den tidligere betegnelsen for Danske Banks internetbaserte betalings- og informasjonssystem for bedrifter. En henvisning til Business Online er derfor det samme som en henvisning til District.
- **District**: Internettbasert betalings- og informasjonssystem.
- **Dataleveranse:** Overførsel av data mellom bedriften og banken. En dataleveranse kan f.eks. inneholde betalingsinstruksjoner.
- **Digital signatur:** Elektronisk underskrift som benyttes ved forpliktende transaksjoner, f.eks. betalinger og ved oppkobling til banken.
- **Nøkkel**: nøkler skal brukes i sammenheng med bruker-ID og personlig passord, når det logges på District med eSafeID sikkerhetssystemet. Nøkkelen kan kun brukes én gang.
- **EDISec:** Sikkerhetsløsning som benyttes ved integrasjon mot Danske Banks systemer via datakommunikasjonskanaler.
- **Engangskode:** Kode som utstedes og sendes av banken til bedriftens bruker(e). Koden består av fire eller åtte tegn og benyttes av bedriftens bruker(e) til sikkerhetsopprettelse i District/Business PC.
- **eSafeID:** Webbasert sikkerhetsløsning som benyttes til å logge på District. eSafeID er en 2-faktor sikkerhetsløsning som består av henholdsvis noe brukeren vet (personlig passord) og noe brukeren har (kodebrikke)
- **e-Safekey:** Sikkerhetsløsning som benyttes ved integrasjonsløsninger til oppkobling mot District.
- **Fortrolige betalinger:** Med fortrolige betalinger forstås betalinger (f.eks. lønninger) som bare skal ses eller behandles av brukere med særlige rettigheter. Betalinger som er markert som fortrolige vil bare kunne behandles av brukere som har denne rettighet.
- **Fullmakt:** Enten brukerfullmakten til District, Fullmakt – bedrift, District kontofullmakt eller en av bankens andre fullmaktsblanketter til District.
- **Fullmaktshaver:** En eller flere tilknyttede bedrifter og/eller fysiske personer som er tildelt en fullmakt.
- **Grunndata:** Fornavn, evt. mellomnavn, etternavn, brukernavn, kundenr, fødselsnr og tilknyttet næringsadresse.

- **Kodebrikke:** Kodebrikker er personlige og finnes i ulike varianter. Felles for dem er at de kan vise en nøkkel som skal brukes når man skal logge på District.
- **Kundesupport:** Hjelpefunksjon i Danske Bank, som via telefonen yter teknisk support eller support til District-brukere.
- **Modulavtale:** Avtale som inneholder bestemmelser om den enkelte modul, f.eks. Trade Finance, Collection Service m.fl.
- **Modulbeskrivelse:** Beskrivelse i punktform av funksjonene i de enkelte moduler som er registrert på avtalen.
- **Nøkkelfiler:** Elektroniske nøkkelfiler benyttes i sikkerhetssystemene e-Safekey og EDIsec. Hver bruker danner en nøkkelfil (som inneholder et nøkkelpar) – en privat nøkkel, som brukes til å danne digitale signaturer, og en offentlig nøkkel, som brukes til å bekrefte den digitale signaturen og kryptere data fra banken til kunden. Hver bruker har sin hemmelige nøkkelfil, slik at bruker kan danne unike, personlige digitale signaturer. Adgangen til å benytte nøkkelfilen er beskyttet av brukers personlige passord. Nøkkelfilen oppbevares i virksomhetens IT-system
- **OpenPGP Security:** Sikkerhetsløsning som benyttes ved integrasjon mot Danske Banks systemer via datakommunikasjonskanaler.
- **Ordre:** Elektronisk, skriftlig eller muntlig ordre til banken om å gjennomføre endringer, transaksjoner m.m.
- **Overføring til utlandet:** En betaling som passerer en landegrense – også om betalingen er i samme valuta, f.eks. euro. Det gjelder både betalinger mellom registrert konti og til ikke registrert konti. Betalingen regnes ikke som overføring til utlandet hvis den skjer mellom to konti i samme land i de land Danske Bank-konsernet er representert.
- **Personlig passord:** Kode som beskytter brukers hemmelige nøkkel, som brukes til å danne digitale signaturer (elektroniske underskrifter). Koden skal være på minimum 4 tegn og skal bestå av minimum et tall.
- **Sikkerhetsopprettelse:** Den opprettelsesprosedyre bruker gjennomgår før District kan tas i bruk.
- **Transaksjoner:** Betalinger, betalingsanmodninger og forespørsler i District

Danske Bank
Foretaksregisteret NO 977 074 010 MVA

Danske Bank A/S
Erhvervs- og Selskabsstyrelsen CVR-nr. 61 12 62 28

Holmens Kanal 2-12
DK-1092 København K – Danmark