Betingelser for District

Gældende fra 1. juni 2020

DB0208DK 2020. 06

Indledning

District er en multikanalplatform med fuld kundeinterface som har til formål at aggregere alle Danske Bank services sammen med udvalgte tredjeparters services og herved skabe et komplet og brugervenligt digitalt økosystem af sammenhængende finansielle ydelser. District giver eksempelvis jeres virksomhed adgang til kontoinformationer, betalinger og mange andre finansielle ydelser.

I disse betingelser finder I en beskrivelse af District.

Del 1 – beskriver mulighederne i District, og hvordan systemet bruges.
Del 2 – beskriver de sikkerhedsmæssige krav i forbindelse med brug af District.
Del 3 – beskriver de aftalemæssige forhold i forbindelse med tilslutning til District.

Del 1 – District – generelt

1 Moduler og ydelser

District består af separate moduler og ydelser.

Modulbeskrivelsen indeholder en beskrivelse af de moduler og ydelser, der er i den valgte District version og/eller en beskrivelse af de separate moduler og ydelser.

2 Transaktioner

I District kan I blandt andet oprette opkrævninger, foretage betalinger og forespørgsler på saldi og se bevægelser på konti, der er tilmeldt District via Tilslutningsaftalen, oprette aftale indlån, oprette betalingskonti, foretage cash management og likviditetsstyring eller søge om og disponere over bevilgede lån. Lån er først til disposition, når banken har modtaget lånedokumentationen underskrevet af tegningsberettigede personer. Betalinger, opkrævninger, andre dispositioner og forespørgsler betegnes under ét som transaktioner.

3 Tilmeldte konti

Konti skal tilmeldes District, for at en virksomhed kan foretage transaktioner via District, jf. nedenfor.

3.1 Tilmeldte konti i Danske Bank-koncernen

Konti i Danske Bank-koncernen er konti, der er oprettet i Danske Bank og alle andre koncernforbundne selskaber og divisioner af banken under denne aftale.

Følgende konti i Danske Bank-koncernen kan tilmeldes District:

- Konti, der tilhører jeres virksomhed og er oprettet i virksomhedens navn
- Konti, der tilhører tredjemand herunder datterselskaber. Det forudsætter, at tredjemand eller datterselskabet har afgivet en tredjemandsfuldmagt til den virksomhed, der giver jer adgang til at disponere på tredjemands eller datterselskabets vegne.

Tilmeldte konti i Danske Bank-koncernen kan også håndteres via SWIFT MT101eller MT940/942, se beskrivelsen i pkt. 3.2.

3.2 Tilmeldte konti, der håndteres via SWIFT

Konti, der er oprettet i andre pengeinstitutter end Danske Bank-koncernen og konti i koncernen, hvor I ønsker at foretage transaktioner via SWIFT MT101 eller MT940/942, kan også tilmeldes District via Tilslutningsaftalen. I kan tilmelde både egne konti og tredjemandskonti. I eller tredjemand skal indgå en aftale med det pengeinstitut, hvor kontiene er oprettet, om Payment Instruction via MT101 eller en aftale om Balance Reporting via MT940, jf. pkt. 8.9.

4 Ikke-tilmeldte konti

Hvis konti, der tilhører jeres virksomhed og/eller tredjemand, ikke er tilmeldt District, kan der kun foretages betalinger til disse konti.

Der kan ikke forespørges på eller foretages betalinger fra konti, der ikke er tilmeldt.

5 Betaling via check

Virksomheden kan gennemføre en betaling ved at udskrive en check. Checken kan udskrives fra tilmeldte konti i Danske Bank-koncernen.

Hvis I og/eller tredjemand har en aftale om betalingsanmodning via MT101, kan der også udskrives check fra tilmeldte konti uden for Danske Bank-koncernen, hvis dette står i aftalen mellem virksomheden og/eller tredjemand og pengeinstituttet uden for Danske Bank-koncernen.

Udstedte checks betragtes som bankchecks, og beløbene hæves på kontoen på udstedelsesdatoen.

Virksomheden kan få sat beløbet på ikke-indløste checks ind på tilmeldte konti. Skal beløbet fra de ikke-indløste checks krediteres jeres eller tredjemands konti, skal I eller tredjemand erklære, at Danske Bank holdes skadesløs, hvis checken efterfølgende indløses.

6 Elektroniske ordrer

Når virksomheden eller virksomhedens brugere beder om at få gennemført en ordre eller transaktion i District, f.eks. en betaling, kaldes det en elektronisk ordre.

En ordre eller transaktioner vil bliver gennemført, når en eller to brugere med det rette autorisationsniveau (se afsnit 9 om fuldmagtstyper) har elektronisk underskrevet (digitalt signeret) ordren.

6.1 Tilbagekaldelse af en ordre

I kan tilbagekalde betalingsordrer til og med dagen før den bankdag, hvor ordren ønskes gennemført. Der gælder andre frister for tilbagekaldelse af andre ordrer.

Med hensyn til frister for ændring eller tilbagekaldelse for betalingsordrer (cut-off-tidsfrister) henviser vi til

- Regler for betalingstilladelse
- Priser og tidsfrister - Danmark
- Priser og vilkår for udenlandske betalinger samt betalinger i fremmed valuta i Danmark

6.2 Bindende ordrer
Ordrer, der er gennemført i overensstemmelse med oplysningerne i den elektroniske ordre, er bindende for virksomheden. Banken kan derfor ikke tilbageføre betalinger, handler med valuta eller værdipapirer eller andre transaktioner, herunder udstedte checks, der er endeligt udført i overensstemmelse med ordren.

Når ordren er gennemført, sender vi en elektronisk kvittering.

7 Automatisk tilmelding til modtagelse af dokumenter fra banken i eArkiv

Når I indgår en District-aftale, tilmeldes virksomheden automatisk elektronisk modtagelse af dokumenter fra banken. Dokumenterne bliver opbevaret i jeres eArkiv i District.

Jeres virksomhed modtager dokumenterne elektronisk fra banken med samme retsvirkning som almindelig post på papir.

Tredjemandskonti der tilknyttes District-aftalen behandles som egne konti.

7.1 Dokumenter, som modtages elektronisk
Jeres virksomhed vil modtage alle de dokumenter, som banken sender elektronisk, i eArkiv. Banken kan i særlige tilfælde sende disse dokumenter som almindelig post på papir.

Hvis jeres virksomhed er kunde i et eller flere af Danske Bank-koncernens andre selskaber, og I modtager dokumenter elektronisk fra disse, vil I også modtage dem i District.

Kontoudskrifter, ind- og udbetalingslister og diverse oversigter er eksempler på dokumenter, som I modtager elektronisk. Vi udvider løbende typerne og mængden af elektroniske dokumenter, som I modtager i eArkiv. Hver gang en ny type dokument bliver elektronisk tilgængeligt, får I besked i District, og ikke med post.

7.2 Hvem har adgang til dokumenterne i eArkiv?
Den enkelte brugers rettigheder bestemmer, hvilke dokumenter brugeren får adgang til at se. En bruger vil f.eks. altid kunne se sin egen Brugerfuldmagt i District. Herudover får en bruger med forespørgselsadgang/ dispositionsadgang til en konto adgang til at se de dokumenter, der vedrører den givne konto i eArkiv.

7.3 Opbevaring
Vi opbevarer som minimum de elektroniske ordrer og dokumenter i eArkiv løbende år plus syv år. I skal dog være opmærksomme på, at dokumenterne vil blive slettet, hvis I afmelder en konto eller skifter kundenummer, eller hvis jeres virksomhed skifter pengeinstitut eller af anden årsag ikke længere har District. I opfordres i disse tilfælde til selv at kopiere dokumenterne til egen opbevaring.

Hvis I har brug for at opbevare dokumenterne i en længere periode, end den banken stiller dem til rådighed via District, bør I selv kopiere dokumenterne til egen opbevaring.

7.4 Afmelding af eArkiv
I skal kontakte banken, hvis I ikke ønsker at modtage dokumenter i eArkiv. Vi kan efter aftale sende jer dokumenterne i papirformat mod betaling af et gebyr.

7.5 Ophør
I kan ikke længere modtage elektroniske dokumenter i eArkiv, hvis District-aftalen ophører, hvis I skifter kundenummer eller afmelder konti. Se pkt. 7.3 om opbevaring m.v.

8 Brugerfuldmagt District

En bruger skal have fuldmagt fra virksomheden for at kunne foretage transaktioner i District på vegne af virksomheden eller tredjemand. Denne fuldmagt kan I oprette på bankens Brugerfuldmagt District.

Hvis tredjemand har underskrevet en fuldmagt til virksomheden, kan I videregive denne fuldmagt til jeres brugere. Det kan I gøre ved hjælp af Brugerfuldmagt District.

Inden I opretter en brugerfuldmagt til District, skal I have brugers samtykke til at kunne videregive brugers CPR-nr. til banken. Der er forslag til samtykkeerklæring i District.

Hvis bruger har brug for at foretage transaktioner via kassen, skal jeres virksomhed underskrive blanketten FULDMAGTSBLANKET - ERHVERV.

8.1 Brugerrettigheder
I skal tage stilling til, hvilke brugerrettigheder en bruger skal have adgang til:

- Betalinger mellem tilmeldte konti i samme land inden for Danske Bank-koncernen
- Betalingsanmodninger via SWIFT MT101
- Betalinger til ikke-tilmeldte konti i eller uden for Danske Bank-koncernen – herunder betalinger via indbetalingskort og udbetalinger via MobilePay Payout. Udbetalinger via MobilePay Payout forudsætter, at der er indgået en aftale med Danske Bank om MobilePay Payout.
- Grænseoverskridende betalinger på tværs af landegrænser til tilmeldte og ikke-tilmeldte konti i eller uden for Danske Bank-koncernen
- Oprette depoter, indlægge og udtage værdipapirer i depoter.
- Andre produkter og services.

I skal også tage stilling til, hvilken fuldmagt bruger skal tildeles pr. brugerrettighed. I kan vælge mellem følgende fuldmagter/rettigheder:

- Forespørge
- Oprette/indlægge
- Godkende to i forening
- Godkende alene

Den valgte fuldmagt bruges som udgangspunkt på alle betalinger inden for den enkelte transaktionstype. Har I valgt en mere restriktiv fuldmagt på kontoniveau (se beskrivelsen af kontoadgang i pkt. 8.2), bruges denne, når der foretages betalinger til ikke-tilmeldte konti og ved grænseoverskridende betalinger. Det betragtes også som en begrænsning, hvis I har valgt ikke at tildele en fuldmagt på kontoniveau, hvilket indebærer at bruger så kun kan forespørge på konti.

8.2 Kontoadgang
Hvis I giver bruger ret til at foretage betalinger til ikke-tilmeldte konti og grænseoverskridende betalinger, skal bruger have fuldmagt på kontoniveau.

For hver konto, bruger får adgang til på kontoniveau, skal der tages stilling til, hvilken fuldmagt bruger skal have

- Alene-fuldmagt
- To i forening (A-fuldmagt)
- To i forening (B-fuldmagt)
- To i forening (C-fuldmagt)

Se beskrivelsen af vores kontofuldmagtstyper i pkt. 9.
Den valgte fuldmagt på kontoniveau slår igennem på alle de District-aftaler, som kontoen er knyttet til.

8.3 Fortrolige betalinger
Jeres virksomhed skal tage stilling til, om bruger skal kunne foretage fortrolige betalinger.

Ved fortrolige betalinger forstås betalinger som f.eks. lønninger, der kun må kunne ses, oprettes eller godkendes af en bruger med denne ret.

Bruger får adgang til at foretage fortrolige betalinger inden for de transaktionstyper, som I har givet bruger adgang til.

Der skelnes ikke mellem fortrolige betalinger og ikke-fortrolige betalinger ved forespørgsel på en konto.

8.4 Administrationsrettigheder
Hvis District Administration er en del af jeres aftale, skal I tage stilling til, om bruger skal tildeles administrations-rettigheder i form af

- Aftaleadministration
- Brugeradministration
- Aftaleinformation
- Adgang og spærring
- Betalingsmaksimum - konto

Ved tildeling af Aftale- og/eller Brugeradministration, skal I tage stilling til, hvilken af følgende fuldmagter brugeren(erne) skal tildeles

- Oprette/indlægge
- Alene-fuldmagt
- To i forening

Tildeling af rettighederne Aftaleinformation og Adgang og spærring kan kun tildeles som Alene-fuldmagt.

8.4.1 Aftaleadministration
Hvis I tildeler en bruger Aftaleadministration, bemyndiger I (under den valgte fuldmagt, jf. ovenfor) brugeren til på jeres virksomheds vegne at

- anmode om tildeling og ændring af rettigheden Aftaleadministration til brugere
- slette brugeres Aftaleadministrationsrettigheder
- oprette, rette og slette brugeres Brugeradministrations-rettigheder – se pkt. 8.4.2
- oprette og slette brugeres Aftaleinformations-rettigheder – se pkt. 8.4.3
- oprette og slette brugeres rettigheder i forbindelse med Adgang og spærring – se pkt. 8.4.4
- oprette, rette og slette brugeres ret til at fastsætte betalingsmaksima – konto – se pkt. 8.4.5.

En bruger med disse rettigheder kaldes aftaleadministrator.

I skal tage stilling til, om aftaleadministrator må kunne foretage ændringer under sit eget bruger-id eller ej. Hvis aftale-adminitrator begrænses under sit eget bruger-id, vil aftaleadministrator ikke kunne tildele sig selv ovennævnte rettigheder. Aftaleadministrator vil heller ikke kunne oprette og godkende betalingsordrer. Valget gælder også for brugerens rettigheder som brugeradministrator.

Tildeling af Aftaleadministration skal altid underskrives af de tegningsberettigede i virksomheden. Når en bruger med rettigheden Aftaleadministration har bedt om at få oprettet eller rettet en brugerfuldmagt med Aftaleadministrationsrettigheder, bliver der derfor genereret en Brugerfuldmagt District med underskriftfelt, som er tilgængelig i Districts eArkiv. Bruger-fuldmagten er tilgængelig for brugere med rettigheden Aftalein-formation. Brugerfuldmagten skal underskrives og sendes til banken. I øvrige tilfælde godkender og underskriver bruger med sin digitale signatur.

Brugere med rettigheden Aftaleadministration skal også være tildelt rettigheden Brugeradministration.

8.4.2 Brugeradministration
Hvis I tildeler en bruger Brugeradministration, giver I brugeren bemyndigelse til på jeres vegne at

- oprette og rette jeres brugere, herunder at give brugere adgang til de fuldmagts- og transaktions-typer, moduler og konti, der til enhver tid er på aftalen

- oprette og rette en brugers stamoplysninger
- slette alt på en bruger, herunder stamoplysninger.

En bruger med disse rettigheder kaldes brugeradministrator. I skal tage stilling til, om brugeradministrator må kunne foretage ændringer under sit eget bruger-id eller ej. Hvis brugeradministrator begrænses under sit eget bruger-id, vil brugeradministrator ikke kunne tildele sig selv ovennævnte rettigheder. Brugeradministrator vil heller ikke kunne oprette og godkende betalingsordrer. Valget gælder også for brugerens rettigheder som aftaleadministrator.

8.4.3 Aftaleinformation
Hvis I tildeler bruger rettigheden Aftaleinformation, får bruger – via en brugeroversigt – adgang til at søge på aftalens brugere og se brugeres individuelle adgange (herunder stamoplysninger, moduler, administrationsrettigheder, adgange til konti og betalingsadgange).

Bruger får adgang til brugeroversigten og udvalgte dokumenter, der vises i District.

8.4.4 Adgang og spærring
Hvis I tildeler bruger rettigheden Adgang og spærring, bemyndiger I bruger til på jeres virksomheds vegne at
- bestille midlertidigt kodeord til brugere
- bestille nøgleviser og fuldende aktivering af ny nøgleviser
- spærre og ophæve spærring på brugere.

8.4.5 Betalingsmaksimum - konto
Hvis I tildeler bruger rettigheden Betalingsmaksimum - konto, bemyndiger I bruger til på jeres virksomheds vegne at

- oprette, rette og slette betalingsmaksima på de konti, som brugeren til enhver tid kan disponere over på aftalen.

Ved tildeling af Betalingsmaksimum - konto, skal I tage stilling til, hvilken af følgende fuldmagter bruger skal tildeles

- Alene-fuldmagt
- To i forening (A-fuldmagt)
- To i forening (B-fuldmagt)
- To i forening (C-fuldmagt)

Se beskrivelsen af vores kontofuldmagtstyper i pkt. 9

8.5 Meddelelsessystemet
Alle brugere får adgang til at sende elektroniske meddelelser til banken via en sikker kommunikationsforbindelse. Det er kun muligt for den enkelte bruger at se sine egne sendte og modtagne meddelelser i District. Der kan ikke afgives ordre via meddelelsessystemet.

8.6 Ændring af Brugerfuldmagt District
Hvis I ønsker at udvide eller indskrænke en brugers adgang i District, skal der underskrives en ny Brugerfuldmagt District, der erstatter den tidligere brugerfuldmagt. Hvis ændringen vedrører brugers fuldmagtsforhold på kontoniveau, skal I underskrive en kontofuldmagt og tredjemand skal underskrive en ny tredjemandsfuldmagt.

Hvis ændringerne foretages via District Administration af aftalens aftale- og/eller brugeradministrator, godkendes disse ændringer via digital signatur.

Hvis ændringen samtidig omfatter rettigheder til aftale-administration, skal der underskrives en brugerfuldmagt i henhold til virksomhedens tegningsregler, se punkt 8.4.1.

En brugers fuldmagt til District kan påvirkes, hvis virksomheden udsteder en FULDMAGTSBLANKET - ERHVERV

8.7 Tilbagekaldelse af brugerfuldmagt til District
Brugerfuldmagt District gælder, indtil I kalder den tilbage. Det kan I gøre skriftligt, ved henvendelse i filialen eller med elektronisk signatur, hvor dette er muligt. Fuldmagten kan også kaldes tilbage pr. telefon, men tilbagekaldelsen skal altid følges op med en skriftlig bekræftelse umiddelbart efter. Brugers adgang til at handle på jeres virksomheds vegne via District spærres efter den telefoniske henvendelse.

Når Danske Bank har modtaget en tilbagekaldelse, bekræfter vi skriftligt, at bruger-id og brugers nøgleviser er slettet i vores systemer.

Hvis I opsiger den fulde tilslutningsaftale til District, ser vi det som en tilbagekaldelse af alle de brugerfuldmagter, som er udstedt til aftalen.

Hvis I og/eller en tredjemand har givet bruger en kontofuldmagt, skal denne fuldmagt kaldes tilbage særskilt. Det er altså ikke tilstrækkeligt, at I blot kalder brugerfuldmagten til District tilbage.

8.8 Disposition over tredjemandskonti i District
Hvis I skal foretage transaktioner på tredjemands konti eller oprette/disponere over tredjemands værdipapirer på depoter i Danske Bank-koncernen, skal tredjemand underskrive bankens tredjemandsfuldmagt.

I skal indgå en særlig aftale med Danske Bank, hvis I skal kunne forespørge på tredjemands konti, der er placeret uden for Danske Bank-koncernen, idet dette skal gøres via SWIFT ved brug af MT940. Tredjemand skal også indgå en aftale med den kontoførende bank om, at Danske Bank-koncernen må modtage oplysninger om tredjemands konti i tredjemands pengeinstitut(ter).

I skal indgå aftale med Danske Bank, hvis I skal kunne gennemføre betalinger fra tredjemands konti uden for Danske Bank-koncernen. Tredjemand skal også indgå en aftale med den kontoførende bank om, at Danske Bank-koncernen må sende instruktioner om betalinger til tredjemands pengeinstitut(ter).

Tredjemand skal underskrive bankens tredjemandsfuldmagt, hvis I skal kunne oprette depot og/eller indlægge/udtage værdipapirer på depotet for tredjemand.

Banken tilmelder tredjemands konti til District via jeres Tilslutningsaftale.

8.9 Fuldmagt til køb/salg af valuta og værdipapirer
For at kunne få adgang til at se positioner over forretninger samt køb og salg af valuta på spot og termin, danske og udenlandske aktier, obligationer og investeringsbeviser skal bruger have adgang til et eller flere af Markets Online-modulerne. Adgang til køb og salg af valuta på spot og termin samt køb og salg af aktier, obligationer og investeringsbeviser kræver i øvrigt, at I udsteder fuldmagten Valutaforretninger og/eller fuldmagten Fondsforretninger til bruger. Fuldmagterne giver alene bruger fuldmagt til at indgå transaktioner på jeres virksomheds vegne via Markets Online.
For alle forretninger vedrørende køb og salg af valuta på spot og termin gælder betingelser i den rammeaftale om netting og slutafregning af forretninger, som er indgået mellem jeres virksomhed og banken.

8.10 Fuldmagt til Trade Finance i District
Hvis en bruger skal kunne udstede remburser, inkassationer og/eller garantier, skal I melde bruger til Trade Finance modulet og underskrive aftalen Tilslutning/ændring til Trade Finance modulet i District. I tager herved stilling til, om bruger skal have adgang til

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

I skal også tage stilling til, om bruger skal kunne

- oprette og forespørge
- oprette og godkende to i forening eller
- oprette og godkende alene.

8.11 Fuldmagt til Collection Service - SEPA Direct Debit i District
Hvis en bruger skal kunne danne SEPA Direct Debit opkrævninger, skal virksomheden tilmelde bruger til Collection Service – SEPA Direct Debit-modulet.
Derefter får bruger adgang til:

- opkrævninger
- refusioner
- tilbagekaldelser

på euro-konti tilknyttet District.

9 Fuldmagtstyper

I Danske Bank findes følgende fuldmagtstyper

- Alene-fuldmagt
- To i forening (A-fuldmagt)
- To i forening (B-fuldmagt)
- To i forening (C-fuldmagt).

Med disse fuldmagter kan I bestemme, hvilke brugere der sammen eller alene må godkende en betaling eller en ordre. Fuldmagterne beskrives i de følgende afsnit.

9.1 Alene-fuldmagt
Når en ordre eller betaling oprettes eller ændres af en bruger med denne fuldmagt, betragtes den automatisk som godkendt af brugeren. Brugere med denne fuldmagt kan også godkende ordrer eller betalinger, der er lagt ind af brugere med alle andre fuldmagtstyper.

9.2 To i forening
Når en betalingsordre eller en betaling oprettes af en bruger med to i forening fuldmagt kræves endnu en godkendelse (2. godkendelse) af en bruger med samme fuldmagtstype.

9.3 To i forening (A-fuldmagt)
Når en ordre eller betaling oprettes af en bruger med A-fuldmagt, er den automatisk godkendt af denne (1. godkendelse). Ordren eller betalingen kræver endnu en godkendelse (2. godkendelse) af en bruger med enten Alene-, A-, B- eller C-fuld¬magt. Brugere med A-fuldmagt er sideord-nede, og godkendelsesrækkefølgen er derfor underordnet.

9.4 To i forening (B- fuldmagt)
Når en ordre eller betaling oprettes af en bruger med B- fuldmagt, er den automatisk godkendt af denne (1. godkendelse). Ordren eller betalingen skal herefter godkendes (2. godkendelse) af en bruger med enten Alene-, A- eller C-fuldmagt. To brugere med B-fuldmagt kan ikke godkende en betaling sammen.

9.5 To i forening (C-fuldmagt)
Når en ordre eller betaling oprettes af en bruger med C-fuldmagt, er den automatisk godkendt af denne (1. godkendelse). Ordren eller betalingen skal herefter godkendes (2. godkendelse) af en bruger med enten Alene-, A- eller B-fuldmagt. To brugere med C-fuldmagt kan ikke godkende en betaling sammen.

10 Kundesupport

Danske Bank stiller support og service til rådighed for jeres virksomhed i form af

- brugeradministration
- telefonsupport, herunder spærretjeneste i District
- internetbaserede supportfunktioner
- on-site support.

Brugeradministration kan omfatte oprettelse af tilslutningsaftale og fuldmagter, tilretning af virksomhedens og brugeres adgang til de enkelte dele af support og service, sletning og spærring af brugere, bestilling af engangspinkoder og registrering af ændrede fuldmagtsforhold m.v.

Telefonsupport kan omfatte undervisning, vejledning i brug, hjælp til fejlfinding og vejledning for tilretninger og mulighed for at spærre District. Telefonsupport i forbindelse med installation, opsætning, undervisning og fejlfinding m.v. af District sker i samarbejde med virksomhedens it-afdeling og på virksomhedens ansvar.

Internetbaserede supportfunktioner kan omfatte undervisning, vejledning i brug, hjælp til fejlfinding og vejledning i tilretninger. Brugen af internetbaserede support-funktioner sker i samarbejde med jeres it-afdeling og på jeres virksomheds ansvar.

On-site support kan omfatte opsætning af og undervisning i brugen af District og fejlsøgning. Fejlsøgning kan medføre tilretninger og/eller ændringer af computernes opsætninger og jeres it-systemer, ændringer i registrerings-databaser, opsætningen af routere, firewalls, proxyservere, interne sikkerhedssystemer og ændringer af opsætningen af software og hardware i øvrigt. Opsætning og fejlsøgning sker i samarbejde med jeres it-afdeling og på jeres virksomheds ansvar.

Del 2 – District sikkerhedssystem

11 Tekniske forhold

11.1 Transmissions- og adgangsforhold

I skal etablere en datakommunikationsforbindelse til Danske Bank for at kunne bruge District. I betaler selv alle udgifter i den forbindelse, og I skal selv sørge for at anskaffe, installere, opsætte og vedligeholde det nødvendige IT-udstyr. I skal også sørge for de nødvendige tilpasninger af jeres IT-udstyr – både for at kunne bruge forbindelsen og for den fortsatte drift.

I må ikke anvende særlig software, som f.eks. "overlay services" eller lignende former for software, når I bruger District-systemet. Systemet skal betjenes direkte af brugere via den brugergrænseflade og de programmer, banken stiller til rådighed.

11.2 Distribution, kontrol og opbevaring af software

Banken distribuerer de programmer som skal bruges for at anvende District, hvilket eksempelvis kan være relevant i forbindelse med filudveksling. Disse hentes via internettet.

Når I downloader programmer fra internettet, skal I eller en bruger kontrollere, at programleverancen er elektronisk underskrevet (digitalt signeret) af banken.

Hvis programmerne ikke er elektronisk underskrevet (digitalt signeret) af banken, kan det muligvis være, fordi programmerne er ændrede eller ikke stammer fra Danske Bank. Underskriften kan efterfølgende verificeres ved at kontrollere "egenskaber" på den eller de downloadede programfiler. Hvis I opdager, at den elektroniske underskrift ikke er Danske Banks, må I ikke installere det downloadede program.

11.3 Datasikkerhed

eSafeID, e-Safekey, OpenPGP og EDIsec er de generelle sikkerhedssystemer i District.

e-Safekey, OpenPGP og EDIsec er bankens sikkerheds-systemer til de kunder, der ønsker at udveksle oplysninger elektronisk med banken direkte gennem deres egne forret-ningssystemer. e-Safekey, OpenPGP og EDIsec er bygget op omkring et kodeord, og der anvendes permanente nøglefiler, som lagres i virksomhedens IT-miljø.

Brugen af ovennævnte sikkerhedssystemer sikrer, at data kan krypteres inden afsendelse til banken og ikke ændres under overførslen.

Desuden bliver afsenderen altid identificeret og alle økonomisk forpligtende transaktioner forsynes med en elektronisk underskrift.

11.3.1 eSafeID

eSafeID er bankens webbaserede sikkerhedssystem, der anvendes til at logge på District. eSafeID er bygget op omkring to faktorer, noget man ved, og noget man har: Et personligt kodeord og en såkaldt nøgleviser. Nøgler fra nøgleviseren kan kun anvendes en gang. Disse to faktorer anvendes til at autentificere personen, hvorefter der genereres sessioner og kundespecifikke nøgler, som gemmes i browsersessionen i det tidsrum, brugeren er logget på District.

Når en person skal oprettes som bruger i District med eSafeID sikkerhedssystemet, får bruger et individuelt bruger-id, et midlertidigt kodeord og en nøgleviser. Bruger skal aktivere nøgleviseren og oprette et personligt kodeord før eSafeID sikkerhedssystemet kan benyttes til at skabe adgang til District.

Aktiveringen af nøgleviser kræver to faktorer, hvoraf kodeordet/det midlertidige kodeord kan udgøre den ene del.
Hvis bruger har registreret mobiltelefonnummer ved oprettelse, kan en aktiveringskode tilsendes og udgøre den anden faktor. Er bruger oprettet med CPR-nummer understøttes NemID til aktivering. Alternativt kan administrator på aftalen fuldende aktivering for en bruger uden de ovennævnte muligheder.

Brugere der allerede er oprettet og som modtager en ny nøgleviser skal aktivere den nye nøgleviser inden den kan anvendes. Aktivering sker som beskrevet ovenfor.

11.3.2 e-Safekey

e-Safekey er sikkerhedssystemet i Danske Banks Business API løsning. Når en person skal oprettes som bruger i District med e-Safekey sikkerhedssystemet, får brugeren et individuelt bruger-id og et midlertidigt kodeord. Det midlertidige kodeord bruges som førstegangsidentifikation under oprettelsen.

11.3.3 EDIsec
EDIsec er en sikkerhedsløsning der benyttes til at sikre data ved direkte datatransmission mellem kunden og banken i en kommunikationskanal, der er etableret mellem kunden og banken.

Når en bruger skal oprettes med EDIsec sikkerhedsløsningen tildeler Danske Bank brugeren et individuelt bruger-id, men ikke et midlertidigt kodeord. Validiteten af kundens offentlige EDIsec nøgle bekræftes af det fingerprint som kunden skal lave af nøglen, og som udveksles med Danske Bank ifølge de retningslinjer, der er beskrevet i EDIsec implementerings-guiden.

11.3.4 OpenPGP
OpenPGP er en sikkerhedsløsning der benyttes til at sikre data ved direkte datatransmission mellem kunden og banken i en kommunikationskanal, der er etableret mellem kunden og banken.

Når en bruger skal oprettes med OpenPGP sikkerheds-løsningen tildeler Danske Bank brugeren et individuelt bruger-id og midlertidigt kodeord. Kunden skal danne sine egne OpenPGP nøgler og sende dem til banken sammen med det midlertidige kodeord ifølge de instruktioner, der er beskrevet i OpenPGP Security Implementation Guide fra Danske Bank.

Hvis et certifikat er udstedt af en tredjepartsudsteder betragter Danske bank brugeren som ejer af certifikatet og dermed som ansvarlig for certifikatets validitet og for vedligeholdelsen heraf. Danske Bank anvender alene den offentlige kryptografiske nøgle der er i certifikatet.

Det er kundens eget ansvar at anskaffe og benytte dertil egnet OpenPGP software (egen eller fra tredjepart), der kan håndtere OpenPGP sikkerhed. Herunder skal softwaren bl.a. kunne håndtere OpenPGP nøgler og signering/kryptering af filer.

11.3.5 EDIsec nøgler og OpenPGP nøgler
For EDIsec og OpenPGP er det kundens ansvar at benytte valide nøgler og sikre datakommunikationen til banken. Specifikt gælder at:

- Danske Bank skal have valide udgaver af kundens nøgler. Når kundens egne nøgler er ved at udløbe, skal kunden sikre, at kundens offentlige nøgler udveksles med banken
- Kunden skal benytte valide udgaver af Danske Banks nøgler til at sikre datakommunikationen til banken. Når bankens offentlige nøgler er ved at udløbe skal kunden sørge for at opdatere sit system med en ny udgave af bankens nøgler, om banken vil stille til rådighed
- Hvis kundens nøgler bliver kompromitteret, skal kunden henvende sig til banken for at få nøglerne blokeret.

Når Danske Bank modtager en kundes offentlige EDIsec nøgle eller offentlige OpenPGP certifikat vil disse blive opbevaret i Danske Banks IT-infrastruktur og vil ikke blive udvekslet med parter uden for banken.

Det er bankens ansvar til enhver tid at sikre, at valide udgaver af bankens offentlige EDIsec nøgle og offentlige OpenPGP certifikat er tilgængelig for kunden.

12 Tildeling af bruger-id, midlertidigt kodeord og nøgleviser

Når en person skal oprettes som bruger i District med eSafeID sikkerhedsløsningen, får brugeren et individuelt bruger-id, et midlertidigt kodeord og en nøgleviser. Det midlertidige kodeord bruges som førstegangsidentifikation under oprettelsen sammen med nøgleviseren.

Når en bruger oprettes med EDIsec eller OpenPGP sikker-hedsløsningen tildeles brugeren et bruger-id af banken. Ved OpenPGP tildeles også et midlertidigt kodeord, som benyttes til førstegangsidentifikation af brugeren.

Det midlertidige kodeord konstrueres og udskrives maskinelt uden at nogen får kendskab til koden. Hvis brevet med det midlertidige kodeord og/eller brevet med nøgleviseren har været åbnet eller er beskadiget, skal bruger kontakte banken og bestille et nyt midlertidigt kodeord og/eller en ny nøgleviser. Af sikkerhedsmæssige årsager sendes brevene med nøgleviser og midlertidigt kodeord forskudt.

Hvis bruger ikke har modtaget brevet med det midlertidige kodeord inden syv hverdage efter bestillingen, skal bruger af sikkerhedsmæssige årsager kontakte banken for at annullere bestillingen og foretage en ny.

Hvis brugeren har registreret sit mobilnummer i District, får han eller hun mulighed for at modtage den midlertidige adgangskode via sms. Hvis brugeren ikke modtager en sms med den midlertidige adgangskode inden for 15 minutter efter bestilling, skal brugeren af sikkerhedsmæssige årsager kontakte Danske Bank for at annullere bestillingen og foretage en ny. Ved registrering i sikkerhedsløsningen skal brugeren vælge en personlig adgangskode og herefter slette den midlertidige adgangskode. Danske Bank er ikke ansvarlig for eventuelle fejl eller tab som følge af, at bruger eller administrator ikke kunne opdatere brugerens mobiltelefonoplysninger i District.

Ved oprettelsen vælger bruger sit eget personlige kodeord. Kodeordet skal skiftes regelmæssigt og det er kundens ansvar, at det sker. Efterfølgende skal det midlertidige kodeord destrueres af bruger.

12.1 Opbevaring af bruger-id, personligt kodeord og nøgleviser
I skal implementere sikkerhedsprocedurer, der effektivt forhindrer uautoriseret brug af District, herunder uautoriseret adgang til brugers nøglefiler og nøgleviser.
Der gælder følgende regler for brug af eSafeID, e-Safekey, OpenPGP og EDISec

- bruger-id, kodeord og nøgleviser må kun anvendes af bruger
- kodeord, nøgleviser og nøgler er strengt personlige og må ikke deles med tredjepart/andre personer
- kodeord og nøgler må kun anvendes ved kommunikation med banken (på nær OpenPGP, som kunden gerne må benytte i andre sammenhænge)
- man må ikke skrive kodeordet ned og opbevare det sammen med sin nøgleviser
- Danske Bank anbefaler at kunden så vidt muligt opbevarer hemmelige nøgler i krypto hardware.

Læs også de anbefalinger om sikkerhed, der er nævnt i menupunktet Sikkerhed i District, på Danske Banks hjemmesider og i andre vejledninger.

12.2 Afmelding eller spærring af virksomhedens eller en brugers adgang til District
I skal give banken besked, hvis I ønsker, at banken skal slette virksomhedens eller en brugeres adgang til District. I skal straks kontakte banken for at få spærret brugers adgang, hvis

- der er mistanke om misbrug af det personlige kodeord, virksomhedens/brugers nøglefil eller nøgleviser
- andre har fået kendskab til det personlige kodeord, den personlige nøglefil eller er i besiddelse af nøgleviseren.

Meddelelse om spærring eller ophævelse af en spærring kan gives via District, telefon eller via en af bankens filialer. Hvis meddelelsen gives via telefon, skal meddelelsen efterfølgende bekræftes skriftligt. Brugeren vil dog blive spærret i den mellemliggende periode.

I er ansvarlige for alle transaktioner, der gennemføres af bruger, indtil banken har fået besked om at slette eller spærre en bruger. I er også ansvarlige for alle fremtidige transaktioner, der tidligere er bestilt af en slettet/spærret bruger, indtil banken får besked om, at transaktionerne skal slettes og bekræfter, at dette er muligt.

Det er også muligt for en bruger med Administrationsrettigheder både at slette og spærre en brugers adgang til District, jf. pkt. 8.4.2 og 8.4.4.

12.3 Bankens ret til at spærre virksomhedens eller en brugers adgang til District
Banken har ret til at spærre virksomhedens eller en brugers adgang til District, hvis vi konstaterer forsøg på misbrug. Banken forbeholder sig endvidere ret til at spærre virksomhedens adgang til District, hvis virksomhedens udstyr, software eller interfaces skader, forstyrrer eller på anden måde er til gene for banken eller bankens IT-infrastruktur. Hvis vi spærrer adgangen, får I besked hurtigst muligt.

13 Krypteringsforbud

Lokal, national lovgivning i det land, hvor District benyttes, kan indeholde et generelt forbud mod eller begrænsninger for kryptering. Det er derfor vigtigt at kende landets lovgivning.

Del 3 – Aftaleretlige forhold

14 Krav om erhvervsmæssig brug

District må kun bruges i erhvervsmæssig sammenhæng.
De informationer, I får adgang til, herunder kursoplysninger, er kun til jeres eget brug. Det er ikke tilladt at give oplysningerne videre til andre, medmindre vi har givet skriftlig tilladelse til det.

15 Brug af data

15.1 Brug af virksomhedens data
Din virksomhed kan efter aftale give Danske Bank adgang til visse finansielle data med henblik på tilbud af individuelt tilpassede løsninger til din virksomhed i District og Danske Banks analyser af sådanne data. Hvis Danske Bank anonymiserer disse data, kan banken også bruge dem til andre formål.

15.2 Brug af persondata
I accepterer at Danske Bank bruger person data vedr. brugerne, når de bliver registreret i District i overensstemmelse med Persondataloven. Danske Bank kan gennem District indsamle data om en brugers IP-adresser, tider for log-in, forretningskommunikationen mellem brugere og Danske Bank samt andre data som Danske Bank anser for relevante for driften af District.

Funktioner i District kan udføres for Danske Bank af 3. parter på deres servere i henhold til Persondatalovens krav og bestemmelser.

Vi registrerer og bruger data om dig og din virksomhed for at kunne tilbyde jer den bedst mulige rådgivning og løsninger og for at opfylde juridiske forpligtelser for os som finansiel institution. I kan se mere om hvilke data vi registrerer, hvordan vi bruger data og jeres rettigheder i vores behandling af personoplysninger og cookies, der findes på Danske Banks hjemmeside. Her kan I også finde kontakt information, hvis I har spørgsmål.

16 Ændring af District

District giver adgang til de ydelser, som Danske Bank tilbyder eller stiller til rådighed.

Danske Bank kan uden varsel ændre vores eget materiel, basisprogrammer og dertil hørende procedurer for at sikre bedst mulige driftsforhold og serviceniveau. Vi informerer med 30 dages varsel om ændringer, der betyder, at I skal tilpasse jeres udstyr for at opretholde forbindelsen og adgangen. Vi informerer via District hvis relevant, pr. brev eller lignende.

Danske Bank kan udvide ydelsernes omfang og/eller indhold uden varsel. Når banken tilføjer nye services, kræver dette ikke ny underskrift fra jeres virksomhed, hvis ændringerne er til fordel for jeres virksomhed og ikke indebærer væsentlige øgede omkostninger for jer.

Hvis ydelsernes omfang og/eller indholdet derimod begrænses giver vi 30 dages forudgående varsel, med mindre ændringen er påkrævet i henhold til lov.

Disse betingelser kan vi ændre uden varsel, og det informerer vi om i District hvis relevant, pr. brev eller ved annoncering i dagspressen.

De nye betingelser gælder for jer, medmindre I meddeler os, at I ikke ønsker at være bundet af dem.

Hvis I meddeler, at I ikke ønsker at være bundet af de nye betingelser, kan vi anse aftaleforholdet som ophørt på det tidspunkt, hvor de nye betingelser træder i kraft.

17 Ansvar og hæftelse

17.1 Virksomhedens ansvar

Brug af District sker på eget ansvar og for egen risiko.

I bærer f.eks. - men ikke begrænset hertil – risikoen for

- forsendelse af oplysninger til Danske Bank og risikoen for, at en forsendelse tilintetgøres, bortkommer, beskadiges, forsinkes, eller der opstår fejl og mangler i forsendelsen, blandt andet ved tredjemands behandling eller bearbejdelse af datamateriale
- at oplysninger kommer til tredjemands kendskab som følge af fejl eller uberettiget indtrængen på datatransmissions forbindelsen
- alle dispositioner og transaktioner, der foretages med jeres egen nøgle eller en af de tilsluttede brugeres nøgler
- at brugere sikrer, at deres personlige kode opbevares forsvarligt og ikke kommer til tredjemands kendskab
- at sikre datasikkerheden i forbindelse med lagring af brugernes nøgler i virksomhedens IT-miljø, så uautoriseret adgang til nøglerne forhindres
- de tilsluttede brugeres eventuelle fejlagtige brug eller misbrug af District
- misbrug i District.

I kan ikke gøre banken ansvarlig for følgerne heraf. I kan heller ikke gøre indsigelser gældende mod banken, for fejl og mangler, der skyldes jeres egne forhold, herunder manglende overholdelse af sikkerheds- og kontrolprocedurer.

Det er også jeres ansvar at

- kontrollere, at indholdet af brugerfuldmagterne altid stemmer overens med de fuldmagter, som I og en eventuel tredjemand har givet til bruger
- indholdet af brugerfuldmagten i øvrigt stemmer overens med jeres virksomheds ønsker
- åbne og kontrollere de elektroniske dokumenter, der sendes fra banken i samme omfang, som hvis de elektroniske dokumenter var sendt som almindelig post på papir
- meddele banken, hvis I i en periode ikke har adgang til District og derfor ønsker at modtage elektroniske dokumenter som almindelig post på papir.

Det er også jeres ansvar, at bruger(e) kender Betingelser for District og de enkelte moduler, og at hver bruger overholder dem og følger anvisningerne i de hjælpetekster, der kan ses på skærmbillederne.

Hvis virksomheden, eller en anden person på vegne af virksomheden, udleverer personoplysninger (f.eks. navn og CPR-nummer) til Danske Bank, indestår virksomheden for, at han eller hun er berettiget til at videregive sådanne personoplysninger, og at den registrerede har givet sit samtykke til, at Danske Bank behandler personoplysninger i forbindelse med anvendelse af produktet i overensstemmelse med disse vilkår og betingelser.

Derudover indestår virksomheden for, at den registrerede rettidigt har modtaget den nødvendige information om Danske Banks behandling af personoplysninger som anført i bankens information om behandling af personoplysninger. Danske Banks information om behandling af personoplysninger i den til enhver tid gældende version kan findes på bankens hjemmeside.

På Danske Banks anmodning, eller hvis offentlige myndigheder anmoder om relevante oplysninger, skal virksomheden udlevere dokumentation til banken, der gør det muligt for den at påvise, at der findes et korrekt og gyldigt retsgrundlag i henhold til GDPR for Danske Banks behandling af personoplysninger som anført ovenfor.

17.2 Bankens ansvar

Banken er erstatningsansvarlig, hvis den på grund af fejl eller forsømmelser opfylder aftalte forpligtelser for sent eller mangelfuldt.

Banken er dog ikke erstatningsansvarlig for fejl og mangler, der skyldes

- en brugers afsløring af engangspinkoden og/eller personlig kode
- ændringer af sikkerhedssystemet (der ikke er gennemført af banken)
- sikkerhedssystemets integration med andre systemer eller software, der ikke er leveret af banken
- services, oplysninger og data leveret af tredjemand.

Selv på områder, hvor der gælder et strengere ansvar, er banken heller ikke ansvarlig for tab, som skyldes

- nedbrud i eller manglende adgang til IT-systemer eller beskadigelser af data i disse systemer, der kan henføres til nedennævnte begivenheder, uanset om det er banken selv eller en ekstern leverandør, der står for driften af systemerne
- svigt i bankens strømforsyning eller telekommunikation, lovindgreb eller forvaltningsakter, naturkatastrofer, krig, oprør, borgerlige uroligheder, sabotage, terror eller hærværk (herunder computervirus og -hacking)
- strejke, lockout, boykot eller blokade, uanset om konflikten er rettet mod eller iværksat af banken selv eller dens organisation og uanset konfliktens årsag. Det gælder også, når konflikten kun rammer dele af banken
- andre omstændigheder, som er uden for bankens kontrol.

Bankens ansvarsfrihed gælder ikke, hvis

- banken burde have forudset det forhold, som er årsag til tabet, da aftalen blev indgået, eller burde have undgået eller overvundet årsagen til tabet
- lovgivningen under alle omstændigheder gør banken ansvarlig for det forhold, som er årsag til tabet.

Banken har kun ansvar for direkte tab, og dermed ikke for indirekte følger eller videregående skadevirkninger, selvom disse skyldes bankens fejl.

Banken er erstatningsansvarlig efter ovenstående regler i pkt. 17.2. § 104 i Lov om betalinger gælder derfor ikke.

18 Andre vilkår og betingelser

18.1 District-aftalens opbygning

En District-aftale består af følgende dokumenter

- District - Tilslutningsaftale
- Brugerfuldmagt(er) til District
- Modulbeskrivelse for District
- Betingelser for District
- Almindelige forretningsbetingelser - Erhverv
- Regler for betalingstilladelse
- Priser og tidsfrister - Danmark
- Danske Bank District - Priser for virksomheder i Danmark
- Priser og vilkår for udenlandske betalinger samt betalinger i fremmed valuta i Danmark
- Hjælpedokumenter og programmer.

Alle dokumenter indgår som en integreret del af District-aftalen, når I underskriver tilslutningsaftalen.

Ved uoverensstemmelse mellem de nævnte betingelser og regler gælder de i den opstillede rækkefølge.
Derudover gælder også de betingelser og regelsæt, som er knyttet til de enkelte modulaftaler eller tilslutningsaftalen.
Når I underskriver District - Tilslutningsaftale, kvitterer I samtidig for at have læst og accepteret disse betingelser og regelsæt som en integreret del af aftalen.

Nye betingelser for services tilbudt i District, herunder betingelser for services tilbudt af udvalgte 3-parter, kan løbende blive tilføjet, alt efter virksomhedens aktuelle brug af services.

Hvis andet ikke er aftalt, og virksomheden tager en service tilbudt i District i brug, så anses de tilhørende servicebetingelser herved for accepteret, ligesom ændringer i separate betingelser anses for accepteret ved fortsat brug.

Betingelser for District og andre forretningsbetingelser og vilkår kan ses på og downloades fra bankens hjemmeside.

18.2 Priser og gebyrer

Vi debiterer afgifter og gebyrer på den konto eller de konti, vi har fået oplyst som gebyr-konto(i), med mindre der er aftalt andet i de særskilte betingelser, der knytter sig til det enkelte modul.

Banken har ret til at samle og debitere gebyrer senere end en måned efter, at den transaktion, der skal betales gebyr for, er gennemført.

Banken har ret til at kræve gebyr for levering af supplerende oplysninger/hyppigere oplysninger end aftalt, da District-aftalen blev indgået.

Banken kan tage gebyrer for de betalinger, som I foretager fra en konto, ligesom vi kan tage gebyrer for at sende oplysninger til jer om de betalinger, som er gennemført.

Ændring af priser og gebyrer sker i overensstemmelse med det beskrevne i bankens Almindelige Forretningsbetingelser. En ændring vil blive annonceret i District, i dagspressen eller via brev.

18.3 Overdragelse, videregivelse og tredjeparter

Denne aftale er indgået af Danske Bank på vegne af Danske Bank-koncernen. Det indebærer, at ethvert medlem af Danske Bank-koncernen har ret til at opfylde og håndhæve denne aftale.

Det betyder også, at vi på ethvert tidspunkt kan overdrage vores rettigheder og pligter til et andet medlem af Danske Bank-koncernen.

Vi har ret til at overdrage vores rettigheder til underleverandører i henhold til denne aftale. En overdragelse påvirker ikke det ansvar, som vi har ifølge denne aftale.

18.4 Særligt om betalingskonti og Lov om betalinger

I forbindelse med betalingstjenester gælder Lov om betalinger.

Vi har fraveget loven i det omfang, den giver mulighed for det, jf. lovens § 6, medmindre andet følger af disse betingelser eller er aftalt med os.

Hvis I kan disponere over en betalingskonto via et særligt betalingsinstrument som f.eks. betalingskort, er vilkårene for det særskilt reguleret i aftalerne for de betalingsinstrumenter, der er tale om. Der henvises i øvrigt til Vilkår og betingelser for betalingskonti.

I har pligt til løbende at kontrollere posteringerne/bevægelserne på jeres konti og depoter. Hvis I ved kontrollen opdager transaktioner, som I ikke mener at have foretaget, skal I straks kontakte banken og senest 4 måneder efter, at beløbet er hævet på kontoen.

Banken har ret til at kræve betaling for at hjælpe jer med at forsøge at tilbageføre beløb, som I ved en fejl har fået overført til en forkert person, fordi der er oplyst en forkert identifikationskode.

Det gælder også, hvis I i District sender en opkrævning, der senere viser sig at være uautoriseret og kræves tilbage af debitor.

19 Opsigelse og misligholdelse

I kan opsige tilslutningsaftalen skriftligt uden varsel. Ordrer og aftaler, der er indgået før en opsigelse, bliver gennemført. Betalt abonnementsafgift og evt. forudbetalte gebyrer betales ikke tilbage.

Banken kan opsige tilslutningsaftalen skriftligt med 30 dages varsel.

Vi kan dog opsige aftalen uden varsel, hvis I misligholder aftalen eller betingelserne for District. Misligholdelse er blandt andet, hvis I undlader at betale som aftalt i tilslutningsaftalen, standser jeres betalinger, kommer under konkurs eller anden insolvent bobehandling, indleder akkord eller udsættes for udlæg eller arrest.

20 Lovvalg

Denne aftale er underlagt dansk ret og værneting.

Hvis I tilmeldes et modul, som helt eller delvis skal bruges i udlandet, accepterer I – på samme måde som Danske Bank – at det er de udenlandske bankers forretnings-betingelser og de retsregler og sædvaner, der gælder for at gennemføre forretningen.

21 Definitioner og ordforklaringer

- **Bankdage** – lørdage, søn- og helligdage samt grundlovsdag, juleaftensdag, nytårsaftensdag og fredag efter Kr. Himmelfartsdag er ikke bankdage i Danmark.
- **Basisprodukter** er enkle bankprodukter, for eksempel konti.
- **Betalingskonti** er konti oprettet med henblik på at gennemføre betalingstransaktioner.
- **Betalinger** mellem tilmeldte konti er betalinger mellem tilmeldte konti i samme land inden for Danske Bank-koncernen.
- **Bruger** er en person (f.eks. en medarbejder), der er bemyndiget af virksomheden til at disponere på virksomhedens vegne via District. Ved direkte integration mellem virksomhedens og Danske Banks edb-system, kan en bruger desuden være en computer eller et system hos virksomheden.
- **Bruger-id** er et sekscifret nummer, der tildeles den enkelte bruger af District. Bruger-id står i brugerfuldmagten.
- **Brugerfuldmagt er** virksomhedens fuldmagt til bruger, der specificerer, hvilke services, konti, fuldmagter og rettigheder den enkelte bruger har adgang til.
- **Business Online** er den tidligere en betegnelse for Danske Banks Internetbaserede betalings- og informationssystemer for virksomheder.
  En reference til Business Online, er derfor en reference til District.
- **Dataleverance** er overførsel af data mellem kunde og bank. En dataleverance kan f.eks. indeholde betalings-instruktioner.
- **Digital signatur** er en elektronisk underskrift, der gives ved forpligtende transaktioner, f.eks. betalinger og ved opkobling til banken.
- **District** er en overordnet betegnelse for DanskeBanks Internetbaserede betalings- og informations-Systemer for virksomheder.
- **Engangspinkode** er en kode, der udstedes og sendes af banken til virksomhedens bruger(e). Koden består af fire eller otte tegn og benyttes af virksomhedens bruger(e) til sikkerhedsoprettelse i District.
- **eSafeID** er et webbaseret sikkerhedssystem der anvendes til at logge på District. eSafeID er et 2 faktor-sikkerhedssystem, som består af henholdsvis noget, bruger ved (personligt kodeord), og noget bruger har (nøgleviser).
- **e-Safekey** er et sikkerhedssystem i de nævnte programmer.
- **EDISec** er et sikkerhedssystem, der benyttes ved andre opkoblinger end de nævnte programmer.
- **Fortrolige betalinger** er betalinger (f.eks. lønninger), som kun må ses eller behandles af brugere med særlige rettigheder.
  Betalinger, som er markeret som fortrolige, vil kun kunne behandles af brugere, som har denne rettighed.
- **Fuldmagter** enten brugerfuldmagten til District, Fuldmagt – erhverv, District kontofuldmagt eller en af bankens andre fuldmagtsblanketter til District.
- **Fuldmagtshaver** er en eller flere tilknyttede myndigheder og/eller fysiske personer, der er tildelt en fuldmagt.
- **Grænseoverskridende betalinger** er betalinger, der passerer **en landegrænse** – også selvom det foregår i samme valuta, f.eks. euro. Lokale bestemmelser kan gælde for betalinger effektueret i udlandet.
  Det gælder både betalinger mellem tilmeldte konti og til ikke-tilmeldte konti.
  Betalingen passerer ikke landegrænser, hvis den sker mellem to konti i samme land i de lande, hvor Danske Bank-koncernen er repræsenteret.
  Betalinger, der håndteres via SWIFT, falder heller ikke ind under denne kategori.
- **Instruktion** er en elektronisk, skriftlig eller mundtlig ordre til banken om at gennemføre ændringer, transaktioner m.m.
- **Midlertidigt kodeord** er en kode, der udstedes og sendes af banken til virksomhedens bruger(e).
  Koden består af fire eller otte tegn og benyttes af virksom-hedens bruger(e) til oprettelse i District.
- **Modulaftale** er en aftale, der indeholder bestemmelser om det enkelte modul, f.eks. Trade Finance, Collection Service m.fl.
- **Modulbeskrivelse** er en beskrivelse i punktform af funktionerne i de enkelte moduler, der er tilmeldt aftalen.
- **Nøgler** skal bruges i sammenhæng med bruger-id og personligt kodeord, når der logges på District med eSafeID sikkerhedssystemet. Nøglen kan kun bruges én gang.

- **Nøglefiler** er elektroniske filer, der anvendes i sikker hedssystemerne e-Safekey og EDISec. Hver bruger danner en nøglefil (der indeholder et nøglepar) – en privat nøgle, der bruges til at danne digitale signaturer, og en offentlig nøgle, der bruges til at bekræfte den digitale signatur og kryptere data fra banken til virksomheden. Hver bruger har sin egen hemmelige nøglefil, så bruger kan danne unikke, personlige digitale signaturer. Adgangen til at benytte nøglefilen er beskyttet af brugers personlige kodeord. Nøglefilen opbevares i på virksomhedens edb-system.
- **Nøgleviser** er personlig og kan antage forskellige formater. Fælles for dem er, at de kan vise en nøgle, der skal bruges, når der logges på District med eSafeID sikker-hedssystemet
- **Kundesupporter** en hjælpefunktion i Danske Bank, der via telefonen yder teknisk support eller support til District-brugere.
- **On-site supporter** uddannelse, teknisk bistand eller anden hjælp, der ydes af banken ude i virksomheden.
- **Personlig kode** er en kode, der beskytter brugers hemmelige nøgle, som bruges til at danne digitale signaturer (elektroniske underskrifter). Koden er på mellem otte og 16 tegn og bør bestå af store og små bogstaver, tal og symboler.
- **Sikkerhedsoprettelse** er den oprettelsesprocedure, bruger gennemløber, inden District kan tages i brug.
- **Stamoplysninger** er fornavn, evt. mellemnavn, efternavn, brugernavn, kundenr., CPR-nr./tildelt kundenr. og tilknyttet virksomhedsadresse.
- **Tilslutningsaftale** er en aftale mellem jeres virksomhed og Danske Bank om brug af District.
- **Transaktioner** er betalinger, opkrævninger, andre dispositioner og forespørgsler i District.