Tænk før du taster

Indledning

Her kan du læse om regler for brug af TDC A/S og dets datterselskabers (herefter TDC) it-

installationer og terminaler, samt hvordan du skal behandle persondata.

TDC's it-installationer er så vigtige for TDC's forretning, at det er nødvendigt at sikre dem mod misbrug og overbelastning. Derfor gælder disse regler, når du bruger TDC's it-installationer, fx mails og adgang til internettet.

Tænk før du taster omfatter også retningslinjer for, hvordan du som TDC'er opfører dig på sociale netværk som fx Facebook, LinkedIn m.fl., og hvordan du må bruge dit firmabetalte telefonabonnement.

Ydermere indeholder "Tænk før du taster" 10 leveregler for behandling af persondata, idet TDC ønsker at signalere over for vores kunder og medarbejdere, at de kan have tillid til, at TDC behandler persondata sikkerhedsmæssigt fuldt forsvarligt og i overensstemmelse med de regler, der gælder for behandling af persondata.

Endeligt understøttes "Tænk før du taster" af en række tekniske og organisatoriske sikkerhedsregler (herefter TDC's sikkerhedspolitikker), som findes på TDC sikkerhedsportalen: https://eramba.tdc.dk/policy.

1. Hvad er it-installationer og terminaler?

Ved it-installationer forstås pc'er, bærbare pc'er, software o.lign., og ved terminaler forstås mobiltelefoner, smartphones, tablets o. lign.

Reglerne gælder for TDC-ejet og/eller udleveret udstyr, som benyttes i dit arbejde, hvad enten arbejdet udføres fra din koncernarbejdsplads eller hjemmet. Hvis du i stedet ønsker at bruge din privatbetalte terminal arbejdsmæssigt, gælder reglerne også i dette tilfælde, selvom det ikke er fremhævet særskilt i teksten nedenfor.

2. Hvem og hvor gælder reglerne?

Reglerne gælder for alle medarbejdere og alle it-installationer og terminaler i TDC. Vær opmærksom på, at der i din afdeling, eller det selskab du er ansat i, kan gælde lokale, skriftlige regler, som afviger fra reglerne i "Tænk før du taster".

Tænk før du taster gælder, uanset om it-installationen eller terminalen er

- på kontoret
- på skiftende arbejdssteder
- derhjemme
- under transport

Reglerne gælder dog ikke i de situationer, hvor du bruger din egen private terminal til private formål og ikke er koblet til koncernnetværket, selvom du benytter en TDC-betalt bredbåndsforbindelse.

3. Hvilke formål må TDC's it-installationer anvendes til?

- **Kun lovlige formål**
  Du må **ikke** bruge TDC's it-installationer og terminaler til formål, som er i strid med loven. Det betyder bl.a., at du ikke må downloade, lagre, bruge, kopiere eller distribuere materiale, som er i strid med fx ophavsrettigheder eller lovgivning om børnepornografi mv.
- **Forretningsmæssig anvendelse af din pc**
  Du må ikke anvende TDC´s it-installationer og terminaler, herunder din TDC-arbejdsmailadresse eller et TDC-betalt telefonabonnement til andre forretningsmæssige formål end TDC´s samt de forretningsmæssige formål som er gældende for medarbejdere udlånt af TDC til andre virksomheder. Derfor må du fx heller ikke oprette private kommercielle hjemmesider eller lave privat kommerciel annoncering med din TDC-identitet som afsender.
- **Pornografi**
  Uanset at besøg på pornografiske hjemmesider ikke er i strid med lovgivningen, må TDC's it-installationer og terminaler ikke anvendes hertil, hvad enten besøget sker i eller uden for arbejdstiden.
- **Spredning af elektronisk materiale**
  Du må ikke bevidst sprede materiale, som kan forstyrre forretningsdriften eller kunderne, fx kædebreve, virus, reklame eller andet materiale, ligesom du ikke bevidst må sende e-mails ud fra din koncernarbejdsplads som ikke kan tilbageføres til dig. Sender du mails i arbejdsmæssige sammenhænge skal dit navn og/eller din TDC-afsender-e-mail-adresse fremgå af de e-mails du sender, medmindre andet fremgår af en arbejdsinstruks.

Adgangen til at benytte TDC's it-installationer og terminaler er nærmere beskrevet nedenfor under punkt 5.

4. Beskyttelse af data og ændringer i sikkerhedsnivauet

4.1. Beskyttelse af data

Du skal sørge for at beskytte TDC's data, derfor skal du iagttage følgende regler:

- **Personlig identifikation og password**
  For at få adgang til TDC's data og systemer får du tildelt en personlig identifikation, og du skal vælge et kodeord. Kodeordet må ikke udleveres til andre, hverken til teknisk support, din leder eller andre. Du er ansvarlig for alle handlinger, der foretages, når dit kodeord er brugt til login.
- **Adgang til TDC-data og TDC's netværk**
  Du må kun etablere adgang til TDC's netværk ved hjælp af TDC-godkendte opkoblingsformer og med udstyr, der er godkendt til formålet af TDC's IT-afdeling. Udstyr med adgang til TDC-data og systemer, uagtet ejerforholdet til udstyret, må kun benyttes af andre med ansættelse i TDC og kun med anvendelse af de pågældendes eget personlige password. Du må ikke anvende eller forsøge at anvende IT-arbejdspladsen til etablering af ikke-autoriseret adgang til TDC's IT-installationer og –udstyr.
- **Opkobling til kunders netværk**
  Hvis du kobler en PC til en kundes netværk, skal du være klar over, at Koncernen har et ansvar, hvis f.eks. PC'en spreder virus og lignende til kundens netværk. Du bør derfor altid sikre dig kundens accept af tilslutningen, inden den foretages.
- **Opbevaring af TDC-dokumenter, mails mv.**
  Det er ikke tilladt, at gemme eller behandle TDC fortrolige og følsomme oplysninger på udstyr der ikke tilhører TDC. Det betyder, at du ikke må bearbejde modtagne filer eller downloade TDC dokumenter eller TDC-mails til din private PC, dropbox, cloudløsning etc.

- **Tredjemandsrettigheder**
  Du må ikke nedtage, lagre, bruge, kopiere eller distribuere materiale, som er i strid med tredjemands rettigheder, f.eks. ophavsrettigheder.
- **Videregivelse af internt materiale**
  Du må kun videregive internt materiale til eksterne modtagere efter »need to know«-princippet og i henhold til materialets dataklassifikation. Når du skal distribuere eller opbevare klassificeret materiale uden for Koncernen, skal du være særligt omhyggelig og kryptere dette med en af Koncernen anvist krypteringsmetode.
- **Lagring på USB og andre eksterne medier**
  Lagringsmedier såsom USB-nøgler, eksterne harddiske m.v. må kun benyttes, hvis klassificeret materiale fjernes eller krypteres ved hjælp af TDC anvist krypteringsmetode. Såfremt lagringsmedier medbringes uden for TDC's kontorer, skal klassificeret materiale altid krypteres.
- **Fortrolighedsstempling**
  E-mails, dokumenter og anden information med "TDC FORTROLIG"-stempling skal håndteres på en sådan måde, at uvedkommende ikke kan få kendskab til indholdet.
- **Kryptering**
  Når du skal distribuere fortrolige og følsomme informationer uden for TDC, skal du være særligt omhyggelig og bruge kryptering. Du kan læse, hvordan du krypterer på
  https://tdc.sharepoint.com/sites/checkin/Koncernnyheder/2017/Sider/Kryptering.aspx
- **Aktivering af pauseskærm**
  Visse dokumenter indeholder oplysninger, der kan skade TDC eller Koncernens kunder, hvis de kommer i de forkerte hænder. Husk derfor at aktivere din pauseskærm, når du efterlader pc-arbejdspladsen u-overvåget og at opbevare fysiske dokumenter aflåst.

4.2. Anvendelse af programmer, der ikke er standard I TDC

- **Licensreglerne skal følges**
  Du må kun anvende programmer, der følger licensreglerne. Du må ikke "pirat"-kopiere programmer. Du skal være opmærksom på, at en del gratis software (såkaldt "freeware") ikke må bruges i dit arbejde, uden at du har sikret dig, at licensforholdene er i orden. Du vil kunne risikere at skulle have din maskine reinstalleret, hvis du installerer software, som påvirker it-udstyrets funktionalitet negativt.
- **Spærring for visse programmer**
  Koncernen vil i visse tilfælde benytte muligheden for at spærre brug af visse PC-applikationer, såfremt de vurderes skadelige for Koncernen.
- **Arbejdsbetinget behov til software, der ikke er standard**
  I tilfælde af arbejdsbetingede behov for software, der kan kompromittere det til hver en tid gældende sikkerhedsniveau, skal der foretages passende foranstaltninger, således at dette ikke kan skade Koncernens øvrige IT-installationer og –udstyr, hvis du er i tvivl kontakt Servicedesk du finder telefonnummeret på din PCs skrivebord.

4.3. Ændring af sikkerhedsniveauet på TDC's it-installationer og terminaler

- **Firewall, antivirus, adgangskoder**
  Du må ikke ændre sikkerhedsniveauet på TDC's it-installationer, dvs. ændre opsætning af fx firewall, antivirus, brug af adgangskoder m.m. Hvis du selv installerer software, har du ansvar for at holde det sikkerhedsmæssigt opdateret. Du er forpligtet til at følge instruktionerne i de sikkerhedsadvarsler, du eventuelt modtager på din pc.
- **Sikkerhedsindstillinger telefoner**
  Ved brug af privatbetalt mobiltelefon, smartphone eller tablet til synkronisering af din TDC-mailkonto

må du ikke ændre de sikkerhedsindstillinger, der opsættes automatisk ved opkobling mod TDC's mailserver.

- **TDC's web-mail**
  Ved opkobling til TDC arbejds-webmail er du forpligtet til at følge anvisningerne ved login til webmail.
- **Antivirus mv. på dine egne private terminaler**
  Det anbefales, at du installerer antivirus og andre beskyttelsesprogrammer på dine egne terminaler.

5. Brug af internettet og din arbejdsmail

5.1.Under ansættelsen

- **Private formål**
  Du må gerne bruge TDC's it-installationer og terminaler til private formål, såfremt det ikke forstyrrer dit arbejde. Hvis du er en del af en vagtplan må kommunikation via sociale netværk kun ske i pauser eller uden for arbejdstiden, med mindre andet aftales lokalt.
- **Fildelingstjenester mv.**
  Du må ikke oprette fildelingstjenester, dele netværksdrev, dele harddiske og lignende til private formål. I forretningsmæssigt øjemed må du kun anvende offentlige fildelingstjenester til deling af TDC-offentligt materiale.
- **Elektroniske spor**
  Når du bruger din TDC-mailadresse eller besøger hjemmesider, eksterne debatfora og andre sociale tjenester (fx Facebook, blogs o.lign.) efterlader du elektroniske spor, der kan føres tilbage til TDC. Du skal generelt være opmærksom på de sikkerhedsmæssige risici, når du bruger internettet, så brug internettet med omtanke og i overensstemmelse med nærværende regler.
- **Facebook, LinkedIn mv.**
  Når du er ansat i Koncernen er du samtidig ambassadør for vores virksomhed. Det betyder, at du gerne må dele indhold fra vores sociale platforme (Fx Facebook og LinkedIn) i dit eget netværk og dermed fortælle de gode TDC-historier. Du må gerne like indhold på vores brands sociale platforme. Men du må ikke besvare kundehenvendelser på de sociale platforme, idet vi har et team, der er uddannet hertil, og som overvåger siderne.
- **Private mails, foto og dokumenter**
  Du skal opbevare private mails og dokumenter i en særlig mappe, markeret "PRIVAT". Private billeder, video og andet omfangsrigt materiale må kun gemmes på pc'ens lokaldrev (C-drev) i en separat mappe, der ikke ligger under mappen Dokumenter. Bemærk at det er ens eget ansvar at tage backup.
- **Arbejde på kunders udstyr**
  Når du arbejder på kundernes udstyr/installationer, skal du til enhver tid efterleve de krav, der fremgår af kundens driftshåndbog, kundens informationssikkerhedsretningslinjer eller andre regler, som du får oplyst.

5.2. Afslutning af ansættelsesforholdet

- **Tilbagelevering af udstyr mv.**
  I forbindelse med fratræden - opsigelsesvarslets udløb eller fritstilling - tilbageleveres alle it-installationer, tablets, simkort. mv., der tilhører TDC.
- **Stop af adgang til Netværket**
  Din adgang til Outlook og koncernnetværket slettes ligeledes ved din fratræden. Herefter kan adgang ikke opnås, hverken fra telefoner, tablets, pc'er eller andre it-installationer. I visse tilfælde, hvor der vurderes at være et særligt sikkerhedsmæssigt behov, vil adgangen kunne lukkes tidligere. En sådan situation vil kunne foreligge, hvis du har indtaget en stilling, hvor det vil have store strategiske og økonomiske konsekvenser for TDC, hvis du i opsigelsesperioden tilsidesætter din loyalitetspligt.

- **Sikker dine private mails, dokumenter mv.**
  For at beskytte medarbejderens private informationer, herunder opretholdelsen af brevhemmeligheden, skal medarbejderen derfor inden sin fratrædelse huske at:
  - slette alle private filer, fx dokumenter, regnskaber o. lign. fra servere
  - slette alle private informationer på USB-nøgle, mobiltelefon o.lign.
  - overdrage forretningsrelevante dokumenter og mails til nærmeste leder
  - opsætte autosvar om, hvortil private/arbejdsrelaterede mails skal videresendes
  - du er selv ansvarlig for at tage kopi af private mails og dokumenter, som du ønsker at beholde. Hvis din adgang til koncernnettet pga. særlige forhold er blevet lukket, før du har taget en sådan kopi, skal du kontakte HR og aftale, hvilke mails du ønsker en kopi af. Koncernssikkerhed vil efter anmodning fra HR fremfinde de aftalte mails og via HR udlevere disse til dig. Bemærk at det ikke vil være muligt at fremskaffe kopi af private dokumenter, da disse slettes ved din fratræden.

Bemærk, at alle mails arkiveres (sættes på legal on hold) i 3 år efter seneste databehandling herunder sletning, baggrunden herfor er at sikre, at TDC ikke mister vigtige informationer pga uberettiget eller utilsigtet sletning. Efter din fratræden vil de kun i særlige tilfælde kunne tilgås af sikkerhedsgodkendte medarbejdere i Koncernsikkerhed.

6. Sociale netværk

6.1. Generelt

Sociale netværk skal forstås bredt som værende digitale fora, netværk og sites, hvor brugerne har mulighed for at starte eller engagere sig i en debat. Eksempler herpå er Facebook, Twitter, Instagram og sites med debatmulighed som eb.dk eller mobilsiden.dk

De sociale medier er værdifulde til opbygning af netværk og relationer, og derfor bør du tænke over sproget og anvende sædvanlig god omgangstone. Overvej derfor altid, inden du sender en mail etc., om du kan stå inde for indholdet.

- **Publicering**
  Vær opmærksom på, at alt hvad du publicerer, vil være offentligt tilgængeligt permanent, og at du efterlader elektroniske spor, når du bruger din TDC-mailadresse eller besøger hjemmesider, eksterne debatfora og andre sociale tjenester fra din pc.
- **Lukkede grupper**
  Du må gerne oprette Facebook-grupper for fx din afdeling, men grupperne skal være lukkede for andre, og det skal tydeligt fremgå, at gruppen kun er for TDC-medarbejdere og ikke have eller fremstå som havende et markedsføringsøjemed. TDC's officielle side på Facebook er bl.a. på adressen facebook.com/TDCGroupComm og facebook.com/tdcgrouptalent. Oprettelse af åbne sider på Facebook, Twitter etc. skal altid ske i samråd med de ansvarlige for markedsføring og kommunikation i det pågældende selskab.

6.2. Tavshedspligt og loyalitet

- **Hvis du udtaler dig offentligt**
  Det vil fx kunne være i strid med din loyalitetspligt, hvis du offentligt udtaler dig ufordelagtigt om TDC, herunder TDC's produkter og ledelse. Tænk derfor altid over, hvad du oplyser om TDC, dine kolleger og dine arbejdsopgaver - aktuelle eller potentielle.
- **Plads til offentlig debat**
  I private sammenhænge kan du naturligvis sige, hvad du vil og som medarbejder er der også plads til debat på Workplace, jf. dog Takt og tone på Workplace i TDC

- **Netværk**
  Du skal i øvrigt huske, at når du deltager i de forskellige netværk, skal du passe på ikke at overskride din tavshedspligt og pligt til loyalitet omkring TDC's forretning og beslutninger.

Du kan læse mere om din loyalitetspligt og tavshedspligt i din ansættelseskontrakt og på Check-In.

6.3. Debat på TDC's officielle sider på sociale netværk (Facebook, Twitter etc.)
TDC har etableret tilstedeværelse på en række sociale netværk, bl.a. Facebook og Twitter for en række af vores brands som fx YouSee, Telmore, Fullrate etc. Disse sider og kanaler bruges bl.a. til at yde kundeservice og generelt til at komme i dialog med vores kunder.

- **Like og deling af indhold**
  Som medarbejder er du velkommen til at like og dele indhold fra vores sociale platforme, men du må ikke svare på henvendelser fra vores kunder, idet vi har et team, der uddannet hertil, og som overvåger siderne.
- **Kontakt social media-teamet**
  Hvis du støder på en sag i et socialt medie, der vil kunne påvirke TDC's omdømme, påvirker vores medarbejdere negativt eller på anden måde kræver handling, så kontakt: 70 22 23 03, tdcsocial@tdc.dk

6.4. Anbefalinger
I visse netværk fx LinkedIn er det almindeligt at vedhæfte anbefalinger herunder anbefalinger fra kollegaer og chefer.

- **Anbefalinger af ikke fratrådte**
  Din leder har ikke pligt til at udarbejde anbefalinger, og hovedreglen i TDC er, at der ikke gives anbefalinger, men der er ikke noget forbud imod det, hvis medarbejderen henvender sig. En leder bør dog aldrig give anbefalinger til en medarbejder, der ikke er fratrådt eller under opsigelse.
- **Anbefaling af sideordnede**
  En medarbejders anbefaling af en sideordnet medarbejder er i orden, selvom begge medarbejdere er ansat.

7. Bortkomst af terminaler, der betales af TDC eller bruges arbejdsmæssigt

- **Kontakt**
  Hvis en it-installation bortkommer, skal det meddeles med det samme til Service Desk, 7011 0511 # 1, der starter proceduren for bortkomst. Ved bortkomst af terminaler, der betales af TDC, eller som bruges arbejdsmæssigt, skal det ligeledes meddeles til Service Desk.

Bemærk! at såfremt terminalen er koblet op til en TDC mailkonto, vil der ved 5 fejltastninger af adgangskode ske en automatisk sletning og 0-stilling af terminalen. Det betyder, at også evt. private data, billeder mv. slettes.

8. Registrering af din færden på nettet, og reaktion ved misbrug af din pc-arbejdsplads

- **Formålet**
  TDC registrerer al it-anvendelse på og til og fra koncernnettet og datterselskabernes net, herunder brug af internettet og mails. Det gør TDC af drifts- og sikkerhedsmæssige hensyn og for at vurdere behovet for forebyggende og beskyttende foranstaltninger. Registreringen kan også anvendes i efterforskning af begrundet mistanke om misbrug.
- **Dekryptering**
  Krypteret kommunikation via internettet kan dekrypteres og logges i TDC's systemer, undtaget vil være kommunikation på de gængse portaler, hvor brugeren nødvendigvis skal oplyse følsomme data, fx banker, skat, e-boks, sundhedsportaler m.fl. På den måde kan TDC frasortere uønskede mails (fx spammails) og spærre for adgangen til visse hjemmesider.
- **Anvendelse af data ved misbrug**
  Hvis der konstateres brug af pc-arbejdspladsen i strid med TDC's sikkerhedsprincipper, vil Koncern Sikkerhed, via HR, orientere den nærmeste leder, som så følger op på sagen. Hvis der er begrundet mistanke om groft eller gentaget misbrug i forhold til TDC's sikkerhedsprincipper, kan medarbejdernes anvendelse af internettet, dataopbevaring, mails og tekstbeskeder (sms o.lign.) sendt fra en telefon, hvor TDC betaler abonnementet blive genstand for gennemgang, efter bemyndigelse fra chefen for Vilkår og HR-jura eller én af ham bemyndiget person hertil.
- **Adgang til dine data**
  Koncern Sikkerhed (SOC'en) har mulighed for at få adgang til medarbejdernes data lagret på TDC's it-installationer og terminaler, herunder personlige drev og mailboks. I TDC-selskaber, der har egen tilslutning til internettet og mailsystem, kan anvendelsen af pc-arbejdspladsen i strid med reglerne søges afdækket af den it-sikkerhedsansvarlige. En sådan efterforskning kan kun finde sted med bemyndigelse fra chefen for Vilkår og HR-jura eller én af ham bemyndiget person hertil.
- **Mails markeret privat**
  Hvis du som medarbejder har markeret mails med "PRIVAT" eller opbevarer mails i en særlig mappe, markeret "PRIVAT", vil det klart fremgå, at der er tale om private mails. Bortset fra særlige undtagelsestilfælde vil mapper markeret "PRIVAT" ikke være omfattet af den konkrete bemyndigelse til at kontrollere din anvendelse af internettet, dataopbevaring og e-mails. Private mails er desuden beskyttet af reglerne om brevhemmeligheden.
- **TDC's rolle som Teleoperatør**
  TDC er bevidst om sin dobbeltrolle som såvel teleoperatør og arbejdsgiver og sikrer, at oplysninger om medarbejderes brug af it- og telefonitjenester i ingen situationer vil blive benyttet i personalesager, medmindre der er tale om oplysninger, som enhver anden arbejdsgiver i henhold til gældende lovgivning vil kunne have adgang til internt eller få udleveret for sine medarbejdere.

9. Persondata i TDC – 10 leveregler

- **Hvad er persondata**
  Persondata er alle oplysninger, der kan knyttes til et individ uanset om formen er skrift, billede, lyd, fingeraftryk, fysisk eller elektronisk materiale.
- **Hvorfor skal du passe på persondata**
  Der har altid været behov for at beskytte personoplysninger, idet der er risiko for, at sådanne informationer kan bruges imod individets interesser. Derfor er reglerne, der skal sikre beskyttelsen af de personoplysninger, vi har registreret om vores kunder og medarbejdere også defineret i TDC's sikkerhedspolitikker.
  Det er vigtigt, at du tænker over, hvordan du behandler, videregiver og opbevarer sådanne oplysninger. Det er også vigtigt, at du som medarbejder sikrer, at personoplysningerne behandles efter de retningslinjer og vejledninger, TDC har udarbejdet.
- **10 leveregler**
  For at understrege vigtigheden af at persondata er noget, vi værner om i TDC, har TDC opstillet 10 leveregler, som du skal efterleve, når du behandler persondata:

1. Aktivér din pauseskærm, når du forlader din pc-arbejdsplads.

2. Beskyt papir eller andet fysisk materiale med personoplysninger i aflåst skab eller skuffe, når du forlader din arbejdsstation.
3. Undlad at gemme personoplysninger på USB-nøgle el.lign.
4. Sørg altid for at mails med i) fortrolige eller ii) følsomme personoplysninger er krypteret, når de sendes til eksterne uden for TDC. Tjek dette link, hvis du vil se, hvordan du gør.
5. Bortskaf papir eller andet fysisk materiale med personoplysninger ved makulering eller anden lignende sikker destruktion.
6. Behandl kun personoplysninger, hvor der er et sagligt og konkret formål til behandling og undgå, at personoplysninger senere bruges til et andet formål.
7. Videregiv kun personoplysninger, hvis du er sikker på, at oplysningerne må gives videre.
8. Opbevar såvidt muligt kun personoplysninger i IT-systemer, der er beregnet til det, og undgå at gemme kopier af personoplysninger, der allerede er gemt i andre systemer.
9. Slet personoplysninger der ikke længere skal bruges.
10. Bær altid dit ID-kort synligt.

Kontakt DPO-kontoret eller din lokale DPM, hvis du konstaterer noget, du vurderer kan udgøre en risiko for sikkerheden for behandling af personoplysninger. Ved anden risiko for sikkerheden kontakt Koncernsikkerhed.

De 10 leveregler om persondata understøttes af de 10 gode råd om sikkerhed defineret af Group Security og bør ikke forveksles mellem hinanden. De 10 gode råd om sikkerhed finder du https://tdc.sharepoint.com/sites/checkin/Organisation/Stabe/Koncernsikkerhed/Sider/Ti-gode-r%C3%A5d-om-sikkerhed.aspx

Hvor kan du læse mere om persondata

- **Medarbejderdata**

  Du kan på Check In læse mere om hvordan, TDC behandler de data der behandles i forbindelse med løn og personaleadministration:
  https://tdc.sharepoint.com/sites/checkin/Medarbejder/Persondata/Sider/default.aspx

- **Kundedata**
  Det er tilsvarende beskrevet, hvordan du skal behandle vores kunders persondata på:
  https://tdc.sharepoint.com/sites/checkin/Organisation/Stabe/persondata/Sider/Persondata-kunder.aspx

10. Sanktioner for overtrædelse

- En overtrædelse af ovennævnte regler kan udløse påtale, advarsel, opsigelse eller bortvisning alt efter overtrædelsens karakter.

Hvem er ansvarlig for reglerne:

Disse retningslinjer er udarbejdet af HR Jura og Persondata i samarbejde med Group Security og Kommunikation. Retningslinjerne er godkendt af Hovedsamarbejdsudvalget, HSU, den 26. november 2019.