Vejledning om dataetisk redegørelse til årsrapporten

Virksomheder i regnskabsklasse C (stor) og D skal fra 1. januar 2021 rapportere om deres arbejde med dataetik i ledelsesberetningen. Denne vejledning fokuserer på de virksomheder, der er omfattet af lovkravet om en dataetisk redegørelse i deres årsrapport. Vejledningen kan bruges til inspiration for arbejdet med dataetik i virksomhederne og udformning af virksomhedernes dataetiske politik, som skal ligge til grund for den dataetiske redegørelse i årsrapporten.

Vejledningens hovedpunkter:

***Hvorfor**: Store virksomheder have en dataetisk politik og lave en dataetisk redegørelse i tilknytning til ledelsesberetningen – eller redegøre for, hvorfor de ikke har en dataetisk politik.*

***Hvornår**: Den dataetiske redegørelse skal placeres i ledelsesberetningen, eller på virksomhedens hjemmeside.*

***Hvem: Ledelsen** skal sørge for, at der en organisatorisk forankring af virksomhedens dataetiske arbejde og sørge for, at der bliver tilvejebragt og godkendt en dataetisk politik. Ledelsen bør være ambassadører for at politikken efterleves i jeres organisation.*

***Hvem: Den eller de personer**, som får ansvaret for dataetikken skal:*

- *Identificere og kortlægge hvad der skal være omfattet af det dataetiske arbejde*
- *Sørge for at udarbejde en dataetisk politik, med de dataetiske principper, som skal guide virksomhedens anvendelse af data*
- *Sørge for at politikken bliver godkendt af ledelsen og bliver genstand for rapportering i form af den dataetiske redegørelse, og at revisor forholder sig til denne.*

***Hvordan**: Den eller de personer, som får ansvaret for dataetikken, bør sikre:*

- *At politikken bliver udbredt, anvendt og lever i organisationen, så den dataetiske redegørelse ikke får karakter af at være en papirtiger*
- *At der er et godt samspil med organisationens øvrige tiltag f.eks. på sikkerhedsområdet og på det persondataretlige område*
- *At principperne i videst muligt omfang bliver designet ind i databehandlingen*
- *At der bliver udarbejdet og gennemført kontroller til arbejdet med dataetik, så politikken bliver efterlevet og resultaterne bliver dokumenteret.*

Om vejledningen

I 2020 blev der indsat en nye bestemmelse i årsregnskabsloven hvorefter virksomheder i regnskabsklasse C (stor) og D skal fra 1. januar 2021 rapportere om deres arbejde med dataetik i ledelsesberetningen.

Afsenderne af denne vejledning har fundet, at der er behov for at konkretisere, hvordan virksomhederne kan arbejde med dataetik, og hvordan en dataetisk redegørelse kan udformes.

Denne vejledning har derfor med baggrund i de udstukne krav i loven til formål:

- At skitsere reglerne for udarbejdelse af en dataetisk redegørelse
- At bidrage til på den ene side grænsedragningen til og på den anden side samspillet med persondataretten
- At tilvejebringe kilder til inspiration til dataetiske principper
- At inspirere til organisering, proces, politik og kontroller
- At give et konkret og operationelt eksempel på og udarbejdelse af en dataetiske politik med tilhørende kontroller

Følgende aktører har bidraget med indhold og/eller været med til at udarbejde denne vejledning:

- Henning Mortensen, Rådet for Digital Sikkerhed (red.)
- Ellen Marie Friis Johansen, FSR – danske revisorer
- Kasper Holton Hülsen, Risma Systems
- Martin Samuel Nielsen, Stibo Systems
- Sebastian RosenKjær, TV2
- Christian von Stamm Jonasson, Dansk Erhverv
- Per Højmark, FSR – danske revisorer
- Jess Kjær Mogensen, FSR – danske revisorer
- Morten Rosted Vang, Dansk Industri
- Mikael Jensen, D-mærket

Baggrunden for dataetik

Dataetik er blevet et nyt fokusområde for mange virksomheder. Det skyldes bl.a. øget politisk opmærksomhed, mere bevidsthed om risici tilknyttet databehandling og et ønske om at bruge ny teknologi, som f.eks. machine learning og kunstig intelligens. Kunstig intelligens kan f.eks. udvikle eller forstærke bias, således at visse grupper behandles på en anden (og ringere) måde end andre grupper[1]. Opsamling af antageligt anonyme lokationsdata kan sammenstilles med andre data og vise et individs bevægelsesmønster[2]. Mere generel opsamling af data om brug af internettet (f.eks. cross-device tracking med webbeacons, flashcookies og tracking-pixels) kan skabe profilering. Hertil kommer diverse mere futuristiske scenarier, som kræver demokratiske dataetiske drøftelser

[1] https://jarnoduursma.nl/blog/the-risks-of-artificial-intelligence/
[2] https://nyheder.tv2.dk/samfund/2021-06-03-otto-jensen-blev-overvaaget-hvert-minut-af-sin-mobil

i det offentlige rum – f.eks. brugen af automatiske autonome våben (og risikoen for misbrug af samme)[3].

Der findes ikke en entydig definition af dataetik, men fra kommissoriet til Det Dataetiske Råd fremgår det, at "Dataetik forstås overordnet som den etiske dimension af forholdet mellem på den ene side teknologi og på den anden side borgernes grundlæggende rettigheder, retssikkerhed og grundlæggende samfundsmæssige værdier, som den teknologiske udvikling giver anledning til at overveje. Begrebet omfatter etiske problemstillinger ved anvendelsen af data"[4]. Dataetik skal således ses som en afvejning af modsatrettede anerkendelsesværdige hensyn. Dataetisk handler med Dataetisk Råds formulering om at "finde en rimelig balance mellem på den ene side de mange fordele, som anvendelse af data og ny teknologi giver, og på den anden side de konsekvenser som brugen af data kan have for det enkelte menneske og for samfundet på både kort og lang sigt" [5].

Dataetik handler altså om at træffe de rigtige valg vedrørende brug af data (drage de rette konsekvenser ved modsatrettede hensyn) og ligger dermed ud over lovgivningen. Dataetik fremgår specifikt af årsregnskabslovens paragraf § 99. Når man foretager rimelighedsbetragtninger efter artikel 5 i databeskyttelsesforordningen indgår dataetik i vurderingen.

Årsregnskabslovens blev i 2020 suppleret med en bestemmelse om, at virksomheder i regnskabsklasse C (stor) og D med virkning for regnskabsåret, der begynder den 1. januar 2021 eller senere enten skal have en politik for dataetik eller også kunne redegøre for, hvorfor en sådan politik ikke er relevant, jf. § 99d[6]. Baggrunden for ændringen var en ud af ni anbefalinger fra den daværende regerings ekspertgruppen om dataetik[7].

Med § 99d i Årsregnskabsloven skal virksomheder enten udarbejde en redegørelse, som indeholder oplysninger om virksomhedens arbejde med og politik for dataetiske spørgsmål eller en forklaring på, hvorfor virksomheden ikke har en dataetisk politik.

Hensigten med ændringen af Årsregnskabsloven er ifølge Erhvervsstyrelsen[8] at sikre, at regnskabsbrugerne[9] får et billede af virksomhedens dataanvendelse, herunder brug af kunstig intelligens, og tager højde for dataetiske overvejelser. Privatliv og databeskyttelse er fundamentale rettigheder jf. EU's Charter, artikel 8[10].

---

[3] https://en.wikipedia.org/wiki/Slaughterbots og https://www.youtube.com/watch?v=9CO6M2HsoIA
[4] https://em.dk/media/13116/kommissorium-for-dataetisk-raad.pdf
[5] https://dataetiskraad.dk/sites/default/files/2021-10/Dataetik%20-%20S%C3%A5dan%20g%C3%B8r%20du.pdf
[6] Årsregnskabslovens § 99c: https://www.retsinformation.dk/eli/lta/2020/741
[7] https://em.dk/media/12191/ekspertgruppens-afrapportering-inkl-anbefalinger.pdf
[8] https://erhvervsstyrelsen.dk/vejledning-vejledning-om-lovpligtig-redegoerelse-dataetik
[9] Bl.a. investorer, medarbejdere og forbrugere
[10] EU's Charter: https://www.europarl.europa.eu/charter/pdf/text_da.pdf, hvor særligt artikel 8 er relevant, bl.a.: "Enhver har ret til beskyttelse af personoplysninger" og "Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag.

Det er tanken med ændringerne i Årsregnskabsloven, at virksomhedernes overvejelser om dataetik "går videre end gældende krav til data- og privatlivsbeskyttelse i snæver forstand"[11], som bl.a. følger af databeskyttelsesforordningen. Erhvervsstyrelsen uddyber videre: "Reglerne om redegørelse for dataetik er derimod et supplement til allerede gældende regler [om beskyttelse af personoplysninger] og handler om virksomhedens etiske overvejelser i forhold til, hvordan virksomhedens dataanvendelse, udvikling og brug af kunstig intelligens m.v. påvirker vores samfund".

Rapportering om dataetik er en ikke-finansiel redegørelse i årsrapporten på linje med redegørelse om samfundsansvar. Erhvervsstyrelsen præciserer, at politikken for dataetik ikke nødvendigvis skal forstås som et præcist afgrænset dataetisk dokument, men mere bredt som interne retningslinjer, der dækker dataetik.

Redegørelsen bl.a. kan indeholde en beskrivelse af et eller flere af følgende emner:

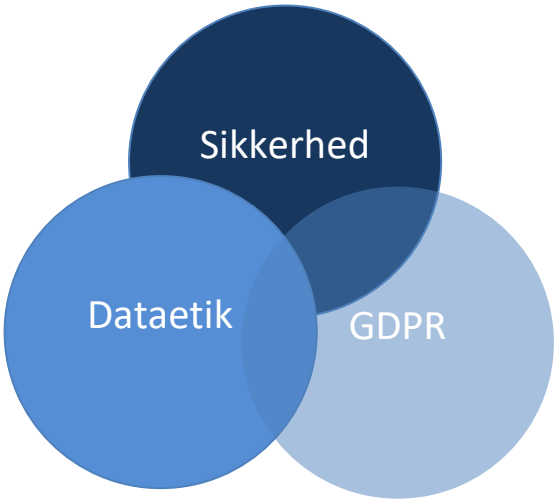
- **Datatyper og behandlinger** – Er der datatyper eller behandlinger virksomheden vælger ikke at behandle/foretage af dataetiske hensyn. Er der datatyper eller behandlinger virksomheden alene vil foretage til bestemte formål?
- **Tredjeparter og tredjeparters datapolitik** - Stiller virksomheden særlige krav til samarbejdspartneres dataetiske retningslinjer og er der typer af tredjeparter der fravælges på baggrund af dataetiske overvejelser i forhold til eksempelvis tredjepartens geografiske placering, datapolitik, øvrige aktiviteter etc?
- **Nye teknologier til bestemte formål** – Stiller virksomheden særlige krav til en dataetisk vurdering inden implementeringen af nye databehandlingsteknologier eller før nye databehandlinger eller behandlinger af data til nye formål iværksættes?
- **Træning af algoritmer og risiko for forudindtagethed** - Stiller virksomheden særlige krav til anvendelsen og udviklingen af algoritmer og hvilke sikkerhedsforanstaltninger er etableret for at undgå, at der opstår risiko for systemmæssig forudindtagethed?
- **Personalisering af produkter og tjenester** - Hvilke værdier er centrale i forhold til anvendelsen af personalisering af produkter og tjenester. Hvordan indgår transparens i disse aktiviteter?
- **Intern kontrol og træning** - Hvordan sikrer virksomheden, at alle medarbejdere har indsigt i virksomhedens dataetiske retningslinjer og forstår at anvende dem i praksis?
- **Forankring i organisationen** - Hvordan har virksomheden valgt at forankre dataetik i organisationen, og hvordan er kommandovejene for dataetiske spørgsmål og beslutninger?

Redegørelsen skal placeres i ledelsesberetningen eller på virksomhedens hjemmeside. Revisor skal foretage et konsistenstjek, som uddybet nedenfor i afsnittet, "Krav til revisors udtalelse".

Enhver har ret til adgang til indsamlede oplysninger, der vedrører ham/hende, og til berigtigelse heraf". Charterets rettigheder kan siges at blive operationaliseret i databeskyttelsesforordningen (GDPR).

[11] https://erhvervsstyrelsen.dk/vejledning-vejledning-om-lovpligtig-redegoerelse-dataetik

Selv om det ikke er tanken, at den dataetiske redegørelse skal være en redegørelse om efterlevelse af de persondataretlige regler, men i stedet en redegørelse, der går ud over behandlingen af personoplysninger (den rette afvejning af modsatrettede hensyn, god opførsel, det rigtige, det ansvarlige og ikke bare en compliant opførsel), skal det bemærkes, at dataetik også spiller en betydelig rolle i persondataretten, hvor man skal foretage vurderinger af "rimeligheden" af en behandling[12] [13].



Som inspiration til hvad den dataetiske redegørelse skal indeholde peger EY[14] bl.a. på følgende elementer: Privacy by design, dataminimering, data diskriminerer ikke, transparens, undgå vildledning af forbrugerne, skabe værdi for forbrugerne, hvem får fordele ved beslutninger om brug af data, diversitet i medarbejdersammensætning, opdateret på dataetiske dilemmaer og tredjeparters håndtering af de data de behandler for os.

PwC har også givet nogle betragtninger på den dataetiske redegørelse[15], hvoraf det bl.a. fremgår, at "Dataetik bygger oven på de regler for virksomheders behandling af personoplysninger, der følger af [databeskyttelsesforordningen]".

PwC henviser også til eksemplerne i lovbemærkningerne, bl.a. hvilke typer af data virksomheden anvender, hvordan data tilvejebringes (f.eks. eksterne parter, sociale medier og data brokers), hvilke dataetiske retningslinjer samarbejdspartnere har, dataetiske overvejelser om ny teknologi

[12] Databeskyttelsesforordningen: https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Se videre Henning Mortensen og Charlotte Bagger Tranberg: "Kan dataetik siges at følge af de persondataretlige regler?", Revision og Regnskabsvæsen, september 2019.
[13] Dataetik kan f.eks. afledes af rimelighedsbegrebet i databeskyttelsesforordningens artikel 5, stk. 1, litra a, som er affattet "Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede". Datatilsynet har således gennem deres praksis foretaget vurderinger af, hvilken behandling som er rimelig / den rette. Videre må man notere sig, at databeskyttelsesforordningens artikel 25 lægger op til, at de fundamentale behandlingsprincipper, som skitseres i artikel 5 (herunder "rimelighed"), skal designes (privacy by design) ind i de teknologiske løsninger, som de dataansvarlige anvender.
[14] https://www.ey.com/da_dk/assurance/nyt-lovkrav-om-redegorelse-for-politik-for-dataetik-er-vedtaget
[15] https://www.pwc.dk/da/artikler/2020/06/krav-om-redegorelse-for-dataetik-for-de-storste-danske-virksomhe.html?utm_source=Metimus&utm_medium=Email&utm_campaign=Ordin%c3%a6r%20Dialog%20uge%2024&utm_content=PwC&utm_term=284011182996092020

(f.eks. machine learning eller kunstig intelligens ved prissætning, udbud eller optimering, træning af algoritmer, indsats for at undgå forudindtagethed, træning af medarbejdere, drøftelser af dataetiske dilemmaer og organisatorisk forankring af beslutninger om anvendelse af data og ny teknologi.

Virksomhedens arbejde med dataetisk politik

Dataetik kan være et nyttigt fokusområde for mange virksomheder. Gennem de senere år er mange virksomheder blevet opmærksom på den store potentielle forretningsmæssig værdi, der ligger i at identificere og anvende data. Data kan bl.a. bruges til at personalisere tjenester, udvikle nye tjenester, tilbyde produkter til en pris, som køberen vil betale, understøtte beslutninger med valide statistikker og helt generelt skabe vækst. Men det er også nødvendigt at vurdere, om man bruger data på etisk og ansvarlig måde.

Hvis virksomheder behandler data på en etisk måde, kan man bygge tillid til sine samarbejdspartnere bl.a. ved at skabe sikkerhed og gennemsigtighed. Virksomheden kan også afhjælpe fejl og måske endda forudsige hændelser inden der opstår og på den måde håndtere og reducere risici. Virksomheder kan give deres kunder adgang til at benytte data om dem selv på lige præcis den måde, kunderne efterspørger.

Dataetisk råd anbefaler, at virksomhederne i deres praktiske dataetiske arbejde læner sig op af en fem-trins-model[16]:

1. **Identificer** hvordan du håndterer data i dit projekt og hvad dit overordnede formål er
2. **Analysér** hvilke hensyn der taler for og imod din databehandling
3. **Afvej** modstående hensyn
4. **Beslut** hvilke hensyn der vejer tungest
5. **Evaluer** de dataetiske konsekvenser løbende

Virksomheden skal have en politik, procedurer, retningslinjer eller tilsvarende for dataetik, og det er den, der skal redegøres for i årsrapporten. På denne baggrund er anbefalingerne i denne vejledning at:

1) **Ledelsesbestemt organisatorisk forankring**
   Dataetik bør forankres i topledelsen. Ledelsen bør sikre, at der arbejdes med dataetik i virksomheden, og at dette arbejde er organisatorisk forankret. Man kan f.eks. udpege en ansvarlig for dataetik, nedsætte en arbejdsgruppe eller nedsætte et dataetisk panel med ledelsesdeltagelse i virksomheden. Hermed opretter virksomheden et centralt sted, hvor dataetikken bliver forankret (i denne vejledning vil vi herefter anvende termen Panel, som betegnelse for den organisatoriske forankring). Ledelsen bør også tage stilling til, hvilken magt i organisationen Panelet får f.eks. i forhold til om virksomheden må foretage konkrete behandlinger.

[16] https://dataetiskraad.dk/sites/default/files/2021-10/Dataetik%20-%20S%C3%A5dan%20g%C3%B8r%20du.pdf

Output: Organisatorisk forankring

2) **Panelets arbejde**
Panelet bør udarbejde en dataetisk politik med principper, som guider virksomheden i arbejdet med dataetik og omsætter principperne i operationelle leveregler i organisationen. Panelet kan også forholde sig til konkret behandling af data og vurdere, om det er i overensstemmelse med virksomhedens dataetiske politik.
Panelet kan også sikre, at de dataetiske principper bliver designet og integreret i de tekniske løsninger, som virksomheden anvender.
Panelet kan endvidere sikre, at det i interne processer bliver kontrolleret, om virksomhedens leveregler for dataetik bliver efterlevet. Der bør med andre ord være kontroller tilknyttet politikken. Dataetik er ikke en complianceøvelse, men der er dataetiske vurderinger indbygget i persondataretten, og dataetik står ovenpå persondataretten. Panelet bør i det lys også sikre, at virksomheden har et godt samspil med (eller evt. er en del af) den organisatoriske enhed, der adresserer persondataretten. En overvejelse kan være at placere det daglige arbejde med dataetik hos den, der varetager arbejdet med informationssikkerhed og/eller persondataret. På den måde bliver det sikret, at regler, procedurer og kontroller på alle tre områder hænger sammen. De interne audits bør dog gennemføres af virksomhedens risiko og compliance funktion, ligesom det bør gøre sig gældende for audits af IT-sikkerhedsreglerne og de persondataretlige regler.
Output: Dataetisk politik, Dataetiske kontroller, Driftsmæssige dataetiske beslutninger

3) **Ledelsesgodkendelse**
Ledelsen bør drøfte og godkende virksomhedens dataetiske politik og sikre, at den er i overensstemmelse med både lovgivning og med virksomhedens vision, mission og værdier. Ledelsen bør være involveret i kommunikation af indholdet i den dataetiske politik, så der bliver sendt et klart signal om, at den skal tages seriøst i hele organisationen.
Output: Synlig ledelsesinvolvering

4) **Dataetisk redegørelse**
I tilknytning til ledelsesberetningen bør ledelsen sørge for, at der laves en redegørelse for virksomhedens politik for dataetik – herunder hvordan denne er omsat til praksis og efterleves.
Output: Dataetisk redegørelse

Virksomhedens valg af dataetiske principper

Det bliver ikke i lovgivningen fastsat, hvad indholdet af en dataetisk politik bør være. Virksomhederne har dermed et betydeligt rum for at vælge principper og metode til at implementere disse. I dette afsnit samt bilag 1 kan findes nogle dataetiske principper til inspiration for det videre arbejde.

Virksomhederne skal vælge hvilke dataetiske principper, de anser som relevante for deres forretning. Lovgivningen præciserer heller ikke, hvordan principperne skal udformes i en politik. Erhvervsstyrelsen har udarbejdet en vejledning om dataetiske retningslinjer og henviser bl.a. til DataEthics og Dataetisk Råd[17].

Her har vi indsamlet en række principper fra forskellige kilder, som kan bruges som inspiration for virksomhedernes valg af principper.

Ved valg af principper kan virksomhederne vælge at lægge vægt på:

- At det er bredt anerkendt som dataetiske principper
- At de afspejler anbefalingerne fra Erhvervsstyrelsen
- At de ligger tæt op ad og er i overensstemmelse med de lovpligtige persondataretlige principper
- At de ligger i forlængelse af virksomhedens øvrige værdier som f.eks. fastsat i virksomhedens redegørelse for samfundsansvar
- At de skaber værdi for virksomhedens forretning og kunder
- At de realistiske og operationelle.

Med inspiration i ovenstående samt bilag 1 kunne man f.eks. udforme principper som følger nedenfor[18] i en dataetisk politik. Det er vigtigt, at virksomhederne tilpasser principperne til de konkrete udfordringer, som virksomheden står overfor.

1. **Dedikation til dataetik**
   Ledelsen har udpeget en ansvarlig for dataetik, og der er nedsat et panel til at foretage dataetiske vurderinger. Ledelsen går forrest og medvirker til at sikre, at principperne bliver integreret i det daglige arbejde. Ledelsen sikrer også, at der er udarbejdet og godkendt en dataetisk politik, og at den er afbalanceret mod virksomhedens øvrige interesser.

2. **Ansvar for databehandlingen**
   Organisationen tager ansvar for behandling af data og sikrer, at behandling af samarbejdspartneres data kun sker, når det er nødvendigt og til klare afgrænsede formål, er kortlagt og i overensstemmelse med love, regler og konventioner, således at risici for utilsigtede konsekvenser ved brug af data reduceres mest muligt.

3. **Retningslinjer for og kontrol af tredjeparters databehandling**
   Det skal sikres, at it-leverandører handler under instruktion, har god sikkerhed om

[17] https://virksomhedsguiden.dk/erhvervsfremme/content/temaer/dataetik/ydelser/dataetiske-retningslinjer-—-saadan-kommer-i-i-gang/e310389d-7316-47e8-941e-84cc586ab8eb/ og https://virksomhedsguiden.dk/erhvervsfremme/content/temaer/dataetik/ydelser/viden-om-dataetik/d4f395ca-07a7-4d3d-b5e2-66396a9b3c26/

[18] Disse principper har karakter af at være formuleret på et generelt niveau, men skal tilpasses den enkelte virksomhed og således gøres virksomhedsspecifikke og relevante.

behandlingen, er dedikeret til at sikre en etisk omgang med data og selv har kendskab til og en dataetisk politik. Data sælges og videregives som udgangspunkt ikke, medmindre der er pligt hertil. Brug af ny teknologi skal vurderes ud fra disse dataetiske principper.

4. **Værdi, gennemsigtighed og tryghed for kunderne**
   Data bruges til at skabe værdi for kunderne, så de mest effektivt, herunder personaliseret, får adgang til de rette løsninger og tilbud. Gennemsigtighed er designet ind i løsningen så kunderne i videst muligt omfang har direkte indsigt i data om dem, og de behandlinger, der bliver foretaget, således kunderne kan være trygge ved, at data om dem er beskyttet bedst muligt. Det vurderes om der er eventuelle negative konsekvenser (f.eks. overvågning, eksklusion eller stigmatisering) for kunderne, når der bliver igangsat nye behandlinger af personoplysninger – også ved brug af nye teknologier.

5. **Medarbejdere bliver trænet og databehandlingen bliver kontrolleret**
   Alle relevante ansatte skal have mulighed for og pligt til at modtage træning i sikker, lovlig og etisk databehandling. Sikkerhedsarbejdet, persondataretlige problemstillinger og dataetiske dilemmaer bliver håndteret, og der bliver gennemført målbare årlige kontroller med sikkerhed, behandling af personoplysninger og dataetik.

Integration og sammenhæng i dataetikken

For at sikre, at de valgte dataetiske principper ikke blot står som et lovbestemt appendiks til årsrapporten, men faktisk er integreret i virksomhedens daglige virke, foreslår vi at sikre, at der opgaven bliver placeret i organisationen, at principperne bliver integreret i en procedure for design på linje med virksomhedens tilsvarende krav fra databeskyttelsesforordningen, at principperne bliver integreret i det øvrige sæt af sikkerhedsmæssige og persondataretlige regler (herefter regelsættet), og at der bliver etableret kontrolfunktioner, som sikrer efterlevelsen. På den måde sikres der et sammenhængende og kommunikerbart flow fra etableringen af dataetiske principper og den dataetiske politik, efterlevelse af lovpligtige principper og krav fra standarder til den måde virksomheden vælger og designer teknologiske løsninger samt kontrollerer og rapporterer efterlevelsen.

Dataetik/persondataret/informationssikkerhed			
Compliance-organisation	Tekniske og organisatoriske foranstaltninger	Kontroller i årshjul	Auditrapporter
ISMS PIMS	Fortegnelse over informationsaktiver	ISO27002 ISO27701	SoA GDPR-rapportering

EIMS	Fortegnelse over behandlingsaktiviteter Regelsæt • ISO27002 • ISO27701 • Designprocedure • Dataetisk politik Tekniske foranstaltninger Træning	Dataetik	Dataetisk redegørelse

Kontroller

Regelsættet og designproceduren indeholder i forvejen en række kontroller med, at reglerne bliver efterlevet. De kan suppleres med kontroller fra den dataetiske politik, der også indeholder virksomhedens dataetiske principper. Eksempler på disse kontroller omfatter[19]:

- Har ledelsen tilvejebragt passende rammer for arbejdet med dataetik?
  - Har ledelsen udpeget en ejer eller ejergruppe for det dataetiske arbejde?
  - Har ledelsen godkendt det dataetiske arbejde og herunder prioriteret dataetiske forhold overfor andre af virksomhedens interesser?
- Bliver relevante interessenter inddraget i arbejdet med dataetik?
  - Bliver kunder, medarbejdere eller eksterne eksperter konsulteret?
- Bliver der foretaget en vurdering af konsekvenser for de registrerede ved en påtænkt behandling?
  - Er der særlig fokus på dataetik, når der bliver udviklet nye teknologiske værktøjer?
  - Er der særlig fokus på at vurdere brug af ny teknologi, f.eks. machine learning, kunstig intelligens, sammenstilling af data til profilering, overvågning eller opsamling af geolokationsoplysninger
  - Hvis løsningen påvirker adfærd, er det så gennemsigtigt, hvordan denne påvirkning sker?
  - Tages der særlige hensyn til svage målgrupper, bliver registreredes rettigheder begrænset, kan der f.eks. ske etnisk baseret forskelsbehandling eller kan personer med handicaps blive ekskluderet?
- Er behandlingen gennemsigtig for de registrerede?

[19] En række af disse kontroller er inspireret af D-mærkets dataetiske kontroller, https://d-maerket.dk/

    - Bliver de registrerede oplyst om behandlingen?
- Er det vurderet, om de registrerede kan få mere kontrol med de behandlinger, der foretages?
    - Har de registrerede f.eks. direkte adgang til at slå op i data om dem selv og kan de evt. redigere data?
- Er det vurderet, om de registrerede kan modtage mere værdi af de data, der behandles?
    - Kan de registrerede bruge data om dem selv i en anden kontekst end den, hvori de er indsamlet?
- Er de dataetiske principper designet ind i den behandling af personoplysninger som bliver foretaget?
    - Er virksomhedens privacy by design strategier kommunikeret offentligt?
- Sikrer ledelsen, dataetisk panel eller andre, at virksomhedens medarbejderne løbende modtager kommunikation om den dataetiske politik og anvendelsen heraf?

Når de dataetiske principper er formuleret og indarbejdet i regelsættet og designproceduren, kan man følge implementeringen i virksomheden på årlig basis gennem tilknyttede kontroller.

Årsrapporten

I ledelsesberetningen skal virksomheden redegøre for indholdet af virksomhedens arbejde med og politik for dataetiske spørgsmål.

Man kan f.eks. redegøre for hvilke principper, der gælder for brug of behandling af data, hvordan leverandører og teknologi bliver udvalgt, hvilke designmæssige kriterier, der er opstillet, hvordan medarbejderne bliver trænet m.v.

Redegørelsen kan placeres i ledelsesberetningen eller på virksomhedens hjemmeside.

Krav til revisors udtalelse

I henhold til årsregnskabsloven § 135 stk. 5, skal revisor afgive en udtalelse om, hvorvidt oplysningerne i ledelsesberetningen er i overensstemmelse med årsregnskabet og et eventuelt koncernregnskab. Revisor skal foretage et såkaldt ”konsistenstjek”.

Revisors konsistenstjek omfatter ledelsens redegørelse for virksomhedens dataetiske politik, der er en del af ledelsesberetningen, uanset om redegørelsen er placeret i ledelsesberetningen eller på virksomhedens hjemmeside via en henvisning hertil i ledelsesberetningen.

Såfremt revisor under sin gennemlæsning af ledelsesberetningen bliver opmærksom på eventuelle væsentlige fejl eller mangler i ledelsesberetningen, skal revisors beskrive sådanne væsentlige fejl og mangler i udtalelsen. Mangler kan bestå i, at der savnes en eller flere oplysninger, som lovgivningen kræver. Fejl kan bestå i, at de lovkrævede oplysninger ikke er givet på korrekt vis.

Det forudsættes, at revisor har kendskab til det regelgrundlag, der regulerer ledelsesberetningen. Revisor skal således gennemlæse ledelsesberetningen og

- sammenholde oplysningerne heri med oplysningerne i årsregnskabet og et eventuelt koncernregnskab og udtale sig om eventuelle uoverensstemmelser,
- sammenholde oplysningerne heri med den viden og de forhold, revisor er blevet bekendt med i forbindelse med sin revision af regnskabet, og udtale sig om eventuelle uoverensstemmelser
- ud fra sin viden om regelgrundlaget tage stilling til, om der er fejl eller mangler i ledelsesberetningen.

Bilag 1: Dataetiske principper til inspiration

A. DataEthics dataetiske principper

https://dataethics.eu/da/dataetiske-principper/

1. Mennesket i centrum
   Menneskets interesser har altid forrang for institutionelle og kommercielle interesser.
2. Individuel datakontrol
   Det er det enkelte menneske, der har den primære kontrol over, hvad deres data bruges til og i hvilke sammenhænge, samt over hvordan deres data aktiveres.
3. Gennemskuelighed
   Databehandling og automatiserede beslutninger skal give mening for det enkelte menneske. De skal være transparente og skal kunne forklares.
4. Ansvarlighed
   Mindske risici for individet samt at inddæmme sociale og etiske konsekvenser
5. Ligeværdighed
   Demokratisk databehandling tager udgangspunkt i, at datasystemer er med til at e bevare, reproducere og skabe magtfordelingen i samfundet. I en databehandling skal der tages særlige hensyn til sårbare mennesker, som eksempelvis på grund af deres økonomiske, sociale og sundhedsmæssige forhold er særligt udsatte for profilering, der kan have negativ effekt på deres selvbestemmelse og kontrol, eller udsætte dem for diskrimination eller stigmatisering.

DataEthics har en liste over værktøjer til virksomheder: https://dataethics.eu/tools/.

B. Fra Erhvervsstyrelsens inspiration til at komme igang

https://virksomhedsguiden.dk/erhvervsfremme/content/temaer/dataetik/ydelser/dataetiske-retningslinjer—-saadan-kommer-i-i-gang/e310389d-7316-47e8-941e-84cc586ab8eb/

1. Skab en positiv fejlkultur
   Sørg for at medarbejderne tør tale om fejl, at fejl opdages og hav planer for håndtering af fejl.
2. God kommunikation sikrer transparens og tillid
   Orientering og kommunikation til kunder og andre interessenter
3. Undgå vildledning
   Design løsninger så man hjælper kunderne til at fokusere, være kreativ og tænke klart
4. Skab værdi for kunden
   Informer kunder og gør det synligt, hvad de kan få af værdi, hvis vi får data
5. Undgå utilsigtede konsekvenser
   Vi skal reflektere over om vi skaber utilsigtede konsekvenser og gener for bl.a. kunderne

6. Skab diversitet
   Medarbejdere skal sammensættes med forskellige baggrunde og kompetencer for at undgå bias
7. Husk de dataetiske dyder
   Faglige kompetencer skal suppleres med ydmyghed, grundighed, ærlighed og medfølelse.

C. Fra Erhvervsstyrelsens vejledning

https://erhvervsstyrelsen.dk/vejledning-vejledning-om-lovpligtig-redegoerelse-dataetik

1. Datatyper, anvendelse og tredjeparter
2. Tredjeparters datapolitik
3. Nye teknologier
4. Træning af algoritmer og risiko for forudindtagethed
5. Personalisering af produkter og tjenester
6. Intern kontrol og træning af kompetencer
7. Forankring i organisationen

D. Rådet for Digital Sikkerheds Dataetiske Principper

https://static1.squarespace.com/static/5592479ee4b0224fac5497af/t/5d00e6560187cc00011c703b/1560340055738/RfDS%2BDE-principper.pdf

1. NØDVENDIGHED
   Er det umuligt at opfylde formålet med løsningen helt uden at indsamle personoplysninger eller med fuld anonymisering af data? (hvis nej, så vælg at re-designe løsningen)
2. LOVLIGHED
   Er der fuld klarhed over hjemmelsgrundlaget? (er metoden lovlig pga. samtykke, legitime interesser, kontrakt eller særlov)
3. ETISK DESIGN
   Sikres individets rettigheder og principperne i GDPR gennem it-løsningens design? (forudbestemt formål, kun indsamling af nødvendige data, indsigt, oplysningspligt, kontrol over egne data, sletning m.v.)
4. KONSEKVENSER
   Er der på forhånd taget stilling til, hvilke konsekvenser forslaget/løsningen kan have for de registrerede på kort og på lang sigt?
5. VALGFRIHED
   Er det valgfrit for den enkelte, hvorvidt data om vedkommende registreres eller ej?
6. SIKKERHED
   Er der etableret en passende sikkerhed i og omkring systemet i tråd med de nødvendige og bedst tilgængelige tekniske og organisatoriske metoder?

7. TRANSPARENS
   Er der gennemsigtighed i behandlingen, herunder ved brug af algoritmer og er der menneskelig kontrol med resultaternes rimelighed?
8. RESPEKT FOR MENNESKERETTIGHEDER
   Er der sikkerhed for, at databehandlingen ikke er bias med risiko for diskriminering, marginalisering eller stigmatisering af individer?
9. PROPORTIONALITET
   Er der foretaget en proportionalitetsafvejning og dermed sikret, at individets rettigheder ikke undermineres ud fra en "målet helliger midlet" tankegang?
10. ANSVARLIGHED
    Er der klarhed om ansvarsplacering, løbende tilsyn og klageadgang?

E. Dataetisk Råds vejledning, "Dataetik – Sådan gør du":

https://dataetiskraad.dk/sites/default/files/2021-10/Dataetik%20-%20S%C3%A5dan%20g%C3%B8r%20du.pdf

1. Velfærd
2. Værdighed
3. Privatliv
4. Selvbestemmelse
5. Lighed
6. Frihed
7. Retssikkerhed
8. Gennemsigtighed
9. Sikkerhed
10. Ansvarlighed

F. Dataetisk Råds Dataetisk vurderingsskema til datasamkøring i det offentlige (meget overordnet gengivelse)

https://dataetiskraad.dk/sites/default/files/2020-11/Dataetisk-vurderingsskema.pdf

1. Hvad er formålet med behandlingen
2. Hvad er konsekvenserne for de registrerede (demokrati, negativ forskelsbehandling, administrative og økonomiske hensyn)
3. Sker der begrænsning af grundlæggende rettigheder (frihed, beskyttelse af personoplysninger, ytring, forsamling, m.v.)
4. Automatisering, profilering og forudsigelse
5. Karakteren af oplysningerne (grad af følsomhed)
6. Begrænsning af mængde og forældelse
7. Gennemsigtighed i teknologier

8. Ansvarlige teknologianvendelse (erfaringer med teknologi, negative konsekvenser for de registrerede, er der lavet risikovurdering, m.v.)
9. Retssikkerhed
10. Er der særlige interesser i målgruppen (f.eks. svage personer)

Rådet har lavet en supplerende dataetisk konsekvensanalyse, som ikke gengives her:

https://dataetiskraad.dk/dataetisk-konsekvensanalyse.

G. DTUs dataetiske principper ved brug af kunstig intelligens

1. Safe AI er selvbevidst – forstår sin egen rolle og usikkerhed, kan f.eks. afslå at handle.
2. Safe AI kan holde på en hemmelighed – har indbygget beskyttelse af privatliv, 'privacy by design'.
3. Safe AI har veldefinerede værdier – er renset for stereotyper, 'bias', og forstår emotioner
4. Safe AI har sociale kompetencer – forstår sociale relationer, forstår brugerens viden og kompetencer.
5. Safe AI forstår magt – forstår data og handlingers kontekst og konsekvens
6. Safe AI er dokumenteret – transparent, kommunikerende, "right to explanation".
7. Safe AI er "open source" – metoder, kode og testresultater er tilgængelige

H. Den tyske dataetik kommission

https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=1.

Generelle etiske og juridiske principper

1. Menneskelig værdighed
2. Selvbestemmelse
3. Privacy
4. Sikkerhed
5. Demokrati
6. Retfærdighed og solidaritet
7. Bæredygtighed

Faktorer som skal forme rettigheder og pligter ved behandling af data

1. Magtbalance mellem parterne
2. Grad af legitimitet i forhold til at få adgang til data
3. Graden af bidrag til at skabe data
4. Omfanget af mulig konflikt mellem parterne
5. Offentlighedens interesse

Bilag 2: Udkast til dataetisk politik med kontroller

Dataetisk politik for VIRKSOMHED

Introduktion

Vi lever i en tidsalder, hvor vi hele tiden får nye digitale processer og ny teknologi til rådighed, så vi kan forøge vores viden og forbedre vores tjenester overfor kunder, kolleger og andre samarbejdspartnere. Drivmidlet i de nye processer og teknologier er som hovedregel data og det er derfor helt centralt for VIRKSOMHED at have fokus på det ansvar, der påhviler os, når vi foretager denne behandling.

For VIRKSOMHED er det en central parameter i det at drive virksomhed, at vores samarbejdspartnere kan have tillid til os og være trygge ved vores håndtering af data. Derfor er vi dedikeret til at beskytte data på tre måder. For det første har VIRKSOMHED stor fokus på at vurdere risici, imødegå disse gennem foranstaltninger og dermed fastholde et højt niveau af informationssikkerhed. For det andet har VIRKSOMHED stor fokus på altid at efterleve de persondataretlige regler og brugernes rettigheder, når vi behandler data. For det tredje har VIRKSOMHED fastlagt vores egne ekstra interne etiske regler, for at sikre at vi både ud fra den enkeltes perspektiv og ud fra samfundets perspektiv bedst kan bevare den tillid vi er blevet givet af samarbejdspartnerne, når vi behandler data.

Denne politik adresserer VIRKSOMHEDs etiske regler for behandling af data.

Formål

Denne politik beskriver, hvordan VIRKSOMHED søger for, at der opstilles etiske principper, som udgør rammer for VIRKSOMHEDs behandling af data, foretages etiske vurderinger af VIRKSOMHEDs behandling af data samt beskrives en proces for håndtering af etiske dilemmaer.

Scope

Denne politik gælder for alle behandlinger i hele VIRKSOMHEDs koncern. Politikken gælder videre for personoplysninger såvel som andre data. Yderligere gælder politikken også for valgte samarbejdspartneres behandlinger, i det omfang VIRKSOMHED kan påvirke disse. Endelig gælder politikken også for alle teknologier og processer, som er under VIRKSOMHEDs indflydelse.

Dataetiske principper

Nedenstående principper udgør grundlaget for VIRKSOMHEDs ansvarlige behandling af data og supplerer de sikkerhedsmæssige og persondataretlige tiltag vi i forvejen efterlever:

1. **Dedikation til dataetik**
   Ledelsen har udpeget en ansvarlig for dataetik, og der er nedsat et panel til at foretage dataetiske vurderinger. Ledelsen går forrest og medvirker til at sikre, at principperne bliver

integreret i det daglige arbejde. Ledelsen sikrer også, at der er udarbejdet og godkendt en dataetisk politik, og at den er afbalanceret mod virksomhedens øvrige interesser.

2. **Ansvar for databehandlingen**
   Organisationen tager ansvar for behandling af data og sikrer, at behandling af samarbejdspartneres data kun sker, når det er nødvendigt og til klare afgrænsede formål, er kortlagt og i overensstemmelse med love, regler og konventioner, således at risici for utilsigtede konsekvenser ved brug af data reduceres mest muligt.

3. **Retningslinjer for og kontrol af tredjeparters databehandling**
   Det skal sikres, at it-leverandører handler under instruktion, har god sikkerhed om behandlingen, er dedikeret til at sikre en etisk omgang med data og selv har kendskab til og en dataetisk politik. Data sælges og videregives som udgangspunkt ikke, medmindre der er pligt hertil. Brug af ny teknologi skal vurderes ud fra disse dataetiske principper.

4. **Værdi, gennemsigtighed og tryghed for kunderne**
   Data bruges til at skabe værdi for kunderne, så de mest effektivt, herunder personaliseret, får adgang til de rette løsninger og tilbud. Gennemsigtighed er designet ind i løsningen så kunderne i videst muligt omfang har direkte indsigt i data om dem, og de behandlinger, der bliver foretaget, således kunderne kan være trygge ved, at data om dem er beskyttet bedst muligt. Det vurderes om der er eventuelle negative konsekvenser (f.eks. overvågning, eksklusion eller stigmatisering) for kunderne, når der bliver igangsat nye behandlinger af personoplysninger – også ved brug af nye teknologier.

5. **Medarbejdere bliver trænet og databehandlingen bliver kontrolleret**
   Alle relevante ansatte skal have mulighed for og pligt til at modtage træning i sikker, lovlig og etisk databehandling. Sikkerhedsarbejdet, persondataretlige problemstillinger og dataetiske dilemmaer bliver håndteret, og der bliver gennemført målbare årlige kontroller med sikkerhed, behandling af personoplysninger og dataetik.

Revision

Denne politik gennemgås og godkendes mindst årligt af VIRKSOMHEDs direktion. Compliance med politikken vurderes ud fra ledelsesgodkendte kontroller. Politikken danner grundlag den dataetiske redegørelse i tilknytning til ledelsesberetningen.

Kontroller

Det sikres at denne politik efterleves ved mindst årligt at gennemføre nedenstående kontroller.

1.1 Har VIRKSOMHED udpeget en ansvarlig for arbejdet med VIRKSOMHEDs dataetiske arbejde?

1.2 Forefindes der en indenfor det seneste år godkendt ledelsesgodkendt dataetisk politik?

1.3 Har panelet været indkaldt til at gennemføre dataetiske vurderinger og er disse vurderinger dokumenteret?

1.4 Er der foretaget overvejelser om hvordan de registreredes rettigheder bliver prioriteret i forhold til virksomhedens (f.eks. kommercielle) interesser?

2.1 Forefindes der en vedligeholdt kortlægning af alle behandlinger af personoplysninger?

2.2 Er der et konkret afgrænset formål med alle behandlinger?

3.1. Overlades personoplysninger uden instruktion?

3.2. Videregives personoplysninger uden hjemmel eller uden dataetisk vurdering?

4.1 Er der foretaget dataetiske vurderinger af brug af machine learning og kunstig intelligens?

4.2 Hvis behandlingen har til formål at påvirke adfærd, er der så foretaget en vurdering af de registreredes konsekvenser ved en påtænkt behandling (f.eks. behandling, der påvirker adfærd)

4.3 Er behandlingen gennemsigtig for de registrerede (er de registrerede oplyst om behandlingen)?

4.4 Er det vurderet om de registrerede kan gives mere kontrol med de behandlinger der foretages?

4.5 Er det vurderet om de registrerede kan modtage mere værdi af de data, der behandles?

4.6 Er det vurderet om der er utilsigtede konsekvenser ved behandlingen (f.eks. overvågning, spredning af misinformation, m.v.)?

4.7 Er det vurderet om der er behov for at iværksætte beskyttelse af særlige målgrupper (f.eks. børn eller ressourcesvage individer)?

4.8 Resulterer behandlingen i begrænsning af de registreredes rettigheder i bred forstand?

4.9 Er det overvejet om behandlingen kan forstærke sociale og etiske problemstillinger (f.eks. ulighed)?

4.10 Er de dataetiske principper indarbejdet i virksomhedens privacy by design procedurer?

4.11 Er virksomhedens privacy by design strategier kommunikeret offentligt?

5.1 Har medarbejderne modtaget træning i principperne i den dataetiske politik?