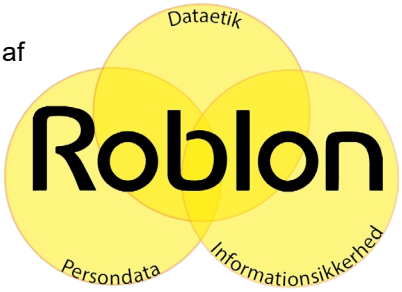
For Roblon er det et central parameter i det at drive virksomhed, at vores samarbejdspartnere kan have tillid til os og være trygge ved vores håndtering af data. Derfor er vi dedikeret til at beskytte data på tre måder.



1) Informationssikkerhed.
   Roblon har stor fokus på at vurdere risici, imødegå disse gennem sikkerhedsforanstaltninger og dermed fastholde et højt niveau af informationssikkerhed. Der er etableret en separat IT-sikkerhedspolitik.

2) Persondata.
   Roblon har stor fokus på altid at efterleve de persondataretlige regler og brugernes rettigheder, når vi behandler data.

3) Dataetik.
   Roblon har desuden fastlagt vores dataetiske regler, i denne dataetiske politik, 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.

Den dataetiske politik kan ikke stå alene, men skal ses som et supplement til lokale love og retningslinjer, samt de allerede etablerede persondata- og IT-Sikkerhedspolitikker i Roblon.

Dataetiske principper:

Roblon har stor fokus på, at data bliver behandlet på en etisk forsvarlig måde. Da data kan være mere end personoplysninger, er der behov for denne supplerende dataetiske politik.

1) Dedikation til dataetik.

   Der er udpeget et team i virksomheden, som skal drive og fastholde Roblon's fokus på dataetik. Dette team er ansvarlig for vurderingen af dataetiske problemstillinger, samt at tage dette videre til ledelsen. Roblon's ledelse er dedikeret til sikre, at de dataetiske principper bliver forankret i det daglige arbejde. Ledelsen sikrer også, at der er en godkendt dataetisk politik.

2) Ansvar for databehandlingen.

   Roblon tager ansvar for behandling af data, både som en del af det eksisterende setup, men også i forhold til kommende systemer. Dette er gældende for såvel interne data, som data vi arbejder med i forbindelse med kunder og leverandører. Vi opbevarer kun relevante data til klare og afgrænsede formål og sikrer at vi er i overensstemmelse med love, regler og konventioner.
   Dette for at risiko for utilsigtede konsekvenser ved brug af data reduceres mest muligt.

3) Retningslinjer for tredjeparters databehandling.

   Vi sikrer, at it-leverandører handler under instruktion, har god sikkerhed omkring behandlingen og er dedikeret til at sikre en etisk omgang med data. Dette betyder at en tredjepart, skal leve op til vores IT sikkerheds- & persondata krav, samt have kendskab til at operere ud fra dataetik.
   Roblon sælger ikke data og videregiver, som udgangspunkt, ikke data, medmindre der er pligt hertil.
   Ibrugtagning af nye teknologier, skal vurderes ud fra disse dataetiske principper.

4) Værdi og tryghed for kunderne.

   Data bruges til at skabe værdi for kunderne, så de mest effektivt, får adgang til de rette løsninger og tilbud.
   Vi tilstræber at kunder og leverandører har tryghed for at data bliver behandlet på en forsvarlig og sikker måde.
   Det bliver løbende vurderet om data kan skabe negative konsekvenser, når der bliver igangsat nye behandlinger af oplysninger - også ved brug af nye teknologier.

5) Medarbejderne bliver trænet og databehandlingen bliver kontrolleret.

   Alle relevante ansatte modtager træning i sikker, lovlig og etisk databehandling. Dette sker både ved tilkøb af eksterne trænings kurser, samt ved interne oplysningskampagner.
   Der gennemføres løbende kontroller med sikkerhed, behandling af personoplysninger og dataetik.

Revision

Denne politik gennemgås og godkendes årligt af Roblons direktion. Politikken danner grundlag for den dataetiske redegørelse i tilknytning til ledelsesberetningen.

Kontroller

Som supplement til eksisterende kontroller og revision vedr. informationssikkerhed og persondata, gennemføres nedenstående kontroller årligt for at sikre, at den dataetiske politik efterleves.

1.1 Har Roblon udpeget en ansvarlig for arbejdet med Roblons dataetiske arbejde?

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

1.3 Har teamet 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 ny teknologi, f.eks. machine learning og/eller kunstig intelligens?

4.2 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?