BikeCorp Inc. – GDPR

# Baggrund

Jeg har været administrator i CRM-systemet på mit gamle arbejde (Dansk Vegetarisk Forening), og jeg har taget en del udgangspunkt i mine erfaringer herfra.

# Overvejelser

* Forståelse af opgaven og vores rolle: Vi er blevet hyret af BikeCorp Inc. til at samle alt deres data i én samlet database. Vores opgave er nu at lave en ”gateway” til databasen, hvor kunderne og medarbejdere får tildelt rettigheder, og på baggrund af disse rettigheder kun kan se et udpluk af data.
* I ”virkelighedens verden” vil virksomhedens medarbejdere have en brugerflade, f.eks. et CRM-system, og vil altså ikke interagere med databasen via Python kodning. Så vores opgave er at programmere ”indmaden” til dette CRM-system
* Der skal oprettes følgende integrationer og rettigheder
  + **Systemrettigheder/integrationer:**
    - **Webshop** skal bl.a. kunne se kunders ordrer og lagerbeholdning
    - **Indkøbssystem** skal kunne se lagerbeholdning
    - **Lokale lagerdatabaser** skal kunne se en altid opdateret lagerbeholdning
    - **Lønsystem** skal kunne se medarbejdere
    - **Google Maps** skal kunne se butikkernes placeringer (specielt relevant ved evt. flytning eller lukning)
  + **Brugerrettigheder:**
    - **Kunder:** Skal kunne se alle de personoplysninger, virksomheden har på dem. Derudover skal kunder kunne se deres ordre og transaktioner, foruden indhold i webshoppen
    - **Medarbejdere:** Skal kunne se kunders ordre og acceptere disse. Derudover skal de have adgang til lagerbeholdningen
    - **Chefer:** Skal kunne se medarbejdernes oplysninger. Derudover samme oplysninger som *Medarbejdere*, såfremt chefen også udfører kundeordre, håndterer lagerbeholdning m.m.
    - **Administrator:** BikeCorp skal udpege en administrator i organisationen, der skal kunne håndtere rettigheder, heriblandt tilføje og fjerne rettigheder. Administratoren har også, som den eneste, adgang til *alle* oplysninger
    - **Investorer:** En mulig tilbygning kunne være at give investorer adgang til salgsdata. Dette er vist ikke kutymen inden for investering, men det kan indgå som en overvejelse.
* Det er ”best practice” at alle har adgange til så få oplysninger som muligt. Altså kun ”need to have” oplysninger. Derudover skal adgange også fjernes, hvis de ikke skal bruges længere. F.eks. hvis en chef ”degraderes” til almindelig ansat.
* Fuld adgang (læse og skrive) eller kun læseadgang? For at undgå, at der opstår ”kuk” i data’en, enten ved fejl eller overlagt hærværk, er der en del scenarier hvor det giver mening kun at tildele læseadgang. Det kan f.eks. være kunder, der navigerer rundt i webshoppen; de skal kun have mulighed for at ”læse” lagerbeholdningen, og ikke skrive i den. Samtidig kan det være en fordel, at lagerbeholdningen kræver et ekstra ”trin” for at give en medarbejder skriveadgang, så vedkommende ikke ved en fejl ændrer i denne, men kun får ændret i den hvis intentionen er reel, f.eks. ved lageroptælling.
* Virksomheden har personlige oplysninger, som kunders navne, adresser og E-mails; samt medarbejderes navne, E-mails og telefonnumre. Men virksomheden er ikke i besiddelse af nogle personfølsomme oplysninger, og heller ikke CPR-numre (eller USA-ækvivalenter hertil. Security number?), hvorfor der umiddelbart ikke er behov for særlig kryptering, i den løsning vi udvikler til virksomheden.
* Adgangskontrol: Det nemmeste for brugerne vil umiddelbart være, at adgangen er koblet op på deres Microsoft bruger (hvis de bruger Windows), så de slipper for at logge ind manuelt, når de skal ind i databasen. Alternativt må det være en browser-login løsning.