

# NOTAT

## BESKRIVELSE AF DATA PROTECTION SERVICE, DPS

Kopi til:

Sagsnr.: 165916  
Dokumentnr.: 1870153

8. april 2021

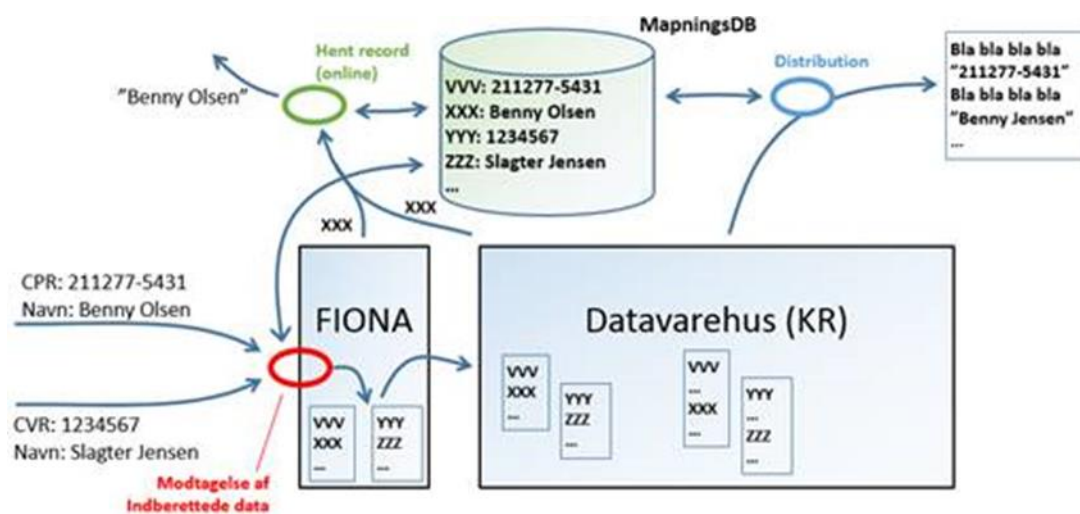
Det danske kreditregister vil indeholde fortrolige personhenførbare data, der er omfattet af GDPR. Informationerne er enten henførbare i sig selv eller i kombination, og det drejer sig om følgende variable:

	Dansk navn		English name	
Nr.	Variabel	Ark	Attribute	Sheet
4.01.02	LEI	1. Modpartsoplysninger	Legal Entity Identifier, LEI	1. Counterparty reference dataset
4.01.03	National identifikation	1. Modpartsoplysninger	National identifier	1. Counterparty reference dataset
4.01.06	Navn	1. Modpartsoplysninger	Name	1. Counterparty reference dataset
4.02.14	Hovedstol/trækningsret	2. Instrumentoplysninger	Commitment amount at inception	2. Instrument dataset
4.07.13	BFE-nummer	7. Pant/sikkerhed	BFE number	7. Protection received dataset
4.07.15	Placering af ejendom: Postnummer	7. Pant/sikkerhed	Postal code	7. Protection received dataset
4.07.16	Placering af ejendom: By	7. Pant/sikkerhed	City/town/village	7. Protection received dataset
4.07.19	Identifikationsnummer for tinglyst pant	7. Pant/sikkerhed	Registered protection identifier	7. Protection received dataset
4.07.20	Ejendomsnummer (BBR.nr.)	7. Pant/sikkerhed	Property identifier (BBR no.)	7. Protection received dataset

For at håndtere disse data, er der udviklet en Data Protection Service (DPS), hvis formål er at beskytte data på detailniveau, således at fortroli-

ge oplysninger om borgere eller virksomheder ikke er identificerbare. DPS'en anvender flere maskeringsmetoder til at beskytte fortrolige data herunder primært pseudonymisering af ID'er og trunkering/afrounding af værdier.

Pseudonymisering betyder i denne forbindelse, at fortrolige data (fx CPR-nummer, navn) omformes til tokens, og det er disse tokens, der efterfølgende gemmes i databaserne i FIONA og Datavarehuset (se figur nedenfor).



Selve pseudonymiseringen foretages ved at udskifte den reelle værdi med et unikt id. På senere/rette tidspunkt kan de lagrede pseudonymer veksles tilbage til de oprindelige dataværdier. Bemærk at virkelighedens pseudonymer er mere komplekse end "XXX" og "YYY" værdierne i illustrationen ovenfor.

Eksempel: En person med CPR-nr. 123456-7890 får det unikke id 59f946171e7641b1. I indberettede data erstattes 123456-7890 nu altid med dette unikke id.

For at muliggøre samkøring af data giver de samme reelle data altid de samme unikke id-værdier. Det er nu muligt at genfinde den samme person på tværs af indberetninger, eksempelvis hvis den pågældende person både har et lån i Danske Bank og i Nordea. Rent teknisk opnås den samme værdi ved, at når en dataværdi skal pseudonymiseres, så tjekkes det først, om den givne token allerede findes, og i givet fald genbruges det eksisterende unikke id.

Trunkering og afrunding bruges til at maskere værdier, der ellers ville kunne bruges til at tilbageføre et lån til en modpart i andre systemer, fx Postnummer (trunkering) eller Hovedstol (afrunding).

Eksempel: Postnumrene 5200, 5210, 5220, 5230, 5240, 5250, 5260, 5270, 5280, 5290 trunkeres alle til 5200.