NOTAT

DESCRIPTION OF THE DATA PROTECTION SERVICE, DPS

DANMARKS NATIONALBANK

Kopi til:

Sagsnr.: 165916
Dokumentnr.: 1872003

8 April 2021

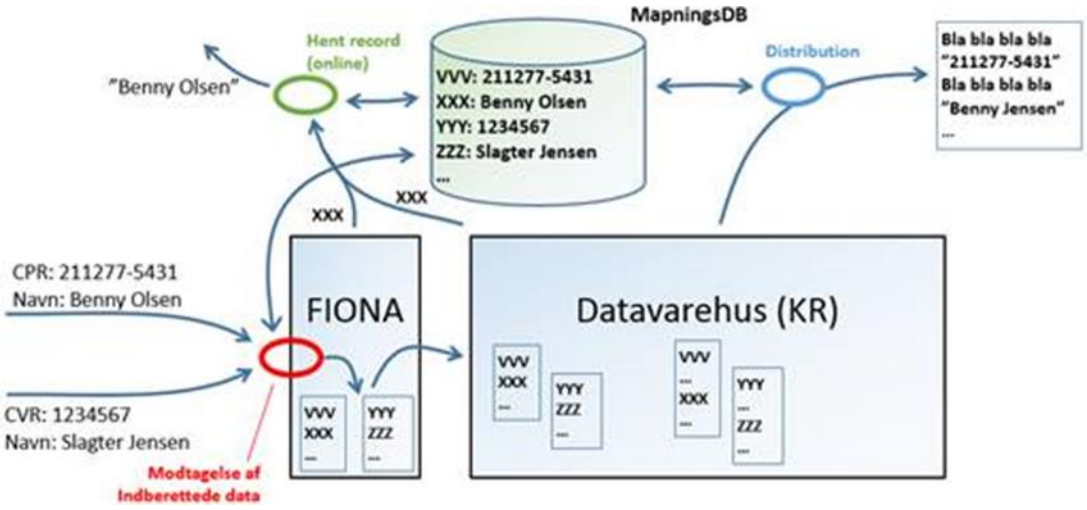
The Danish Credit register will contain confidential personal data protected by GDPR. The information is either identifiable in and on their own or in connection with other attributes. The attributes in question are:

	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

To handle these attributes, DN has developed a Data Protection Service, DPS, with the purpose of protecting the data on micro level, making con-

fidential personal data unidentifiable. The DPS uses a range of techniques to protect confidential data, most notably pseudonymization of identifiers through use of tokens and truncation or rounding of values.

Pseudonymization in this context refers to that confidential data is transformed to tokens. It is these tokens that are saved to the databases in FIONA and the Data warehouse and not the original data (e.g. National identifier, name). The process is sketched in the following figure.



Tokenization provides a consistent token for each unique name and requires access to additional information to re-identify the data at a later stage. Please note, that the tokens are more complex than "xxx", "yyy", "zzz" that are merely used to illustrate the principle.

Example: A person with CPR-no. 123456-7890 (Danish National ID) will be provided with the unique ID 59f946171e7641b1 and this unique ID will be used as a token for CPR-no. 123456-7890 in all future reports.

Using the same token as a unique ID makes it possible to identify the same counterparty across reports, reporters and reference periods, e.g. if the same counterparty is a customer at both Danske Bank and Nordea. This is done by checking of the token exist and if so reuse the token to pseudonymize the new piece of data.

Truncation or rounding is used on values to mask values that can be used to identify a specific counterparty through other systems, such as postal code (truncation) or Commitment amount at inception (rounding). Example: The postal codes 5200, 5210, 5220, 5230, 5240, 5250, 5260, 5270, 5280 and 5290 are all truncated to 5200.