## Week 4 – A3 and GDPR

## Agenda:

## Forklar konceptet af privacy by default og by design.

## Forklar hvad sensitive data er ift. EU lovgivning.

## Vis eksempel på hvordan man krypterer og dekryptere I Java.

## Enumerate the major kinds of sensitive data as defined by the EU law (Danish law is the same).

## Personlige informationer, som f.eks. fulde navn, adresse og e-mail.

## CPR-nummer

## Lokationsdata

## IP-adresser (hvad du laver på internettet)

## Personligt data der afslører race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger.

## Trade-union medlemskab.

## Genetisk data, biometrisk (DNA, fingeraftryk, iris) data bearbejdet med formålet at identificere et inidvid.

## Helbredsrelateret data.

## Data der omhandler en persons sexliv eller seksuel orientering.

## Explain the concepts of privacy by default and by design

## 

## Privacy by default, vil efter den nye GDPR-lov sige, at en virksomhed skal have tilladelse (give samtykke) til at bruge informationer, fremfor at brugeren skal bede virksomheden om ikke at bruge informationerne. Derudover skal det være lige så nemt at trække tilladelsen tilbage.

## Explain the difference between controller and processor roles in the protection of private data.

## Data controller afgør hvorfor og hvordan personlige data skal behandles.

## Data processor behandler personlige data, men kun på vegne af data controller. Det er ofte en tredje part (ekstern virksomhed).

## Explain how to use Java to encrypt and decrypt information

## For at kryptere og dekryptere data i Java skal der bruges en key, som i vores tilfælde er en tilfældig key der er 16 bytes/128 bits. Key bliver sat til at anvende AES algoritmen for kryptering.

## 

## Java bruger et API/bibliotek der hedder “crypto”. For at kryptere data, skal der bruges en initialization vector, der skal være 12 bytes frem for 16 bytes, da det er hurtigere og mere sikkert. Det er vigtigt at bruge en pseudo-random number generator (i vores tilfælde er secureRandom).

## Ved initialisering af Cipher, angives krypteringsalgoritmen AES og krypteringsmode GCM = Galois/Counter Mode.

## New GCMParameterSpec : 128 bits = størrelsen på MAC

## ByteBuffer samler alle informationer i en besked: 4 bytes = længden på en Integer (vi vil gerne have længden af vores vektor angivet som det første i vores ciphertekst).

## Et billede, der indeholder skærmbillede Automatisk genereret beskrivelse

## Vector length, vector og cipher tekst, bliver hentet ud af buffer, og bruges til at dekryptere beskeden.

## Et billede, der indeholder skærmbillede Automatisk genereret beskrivelse