DRAMMEN KOMMUNE
– et godt sted å leve

Tematime for kommunestyret om informasjonssikkerhet og personvern

19. mars2024

Rådgiver Jan Fredrik Mulder Røste

Personvernombud Pål Tore Larsen

DRAMMEN KOMMUNE
– et godt sted å leve

Trusselbilde

- Den teknologisk utviklingen går svært fort
- Kravet til informasjonssikkerhet, ressurser og finansielle midler vil øke
- Vi adresserer trusselbildet og de digitale truslene ved økt fokus på informasjonssikkerhet
- Et av de viktigste tiltak er kulturbygging

Sikkerhetskultur

- Nanolearning på epost
- Status gjennomføring
- Risikovurdering
- Kultur for å melde avvik
- Vær kritisk
- Vær bevisst verdien av data
- Ha kontroll på data

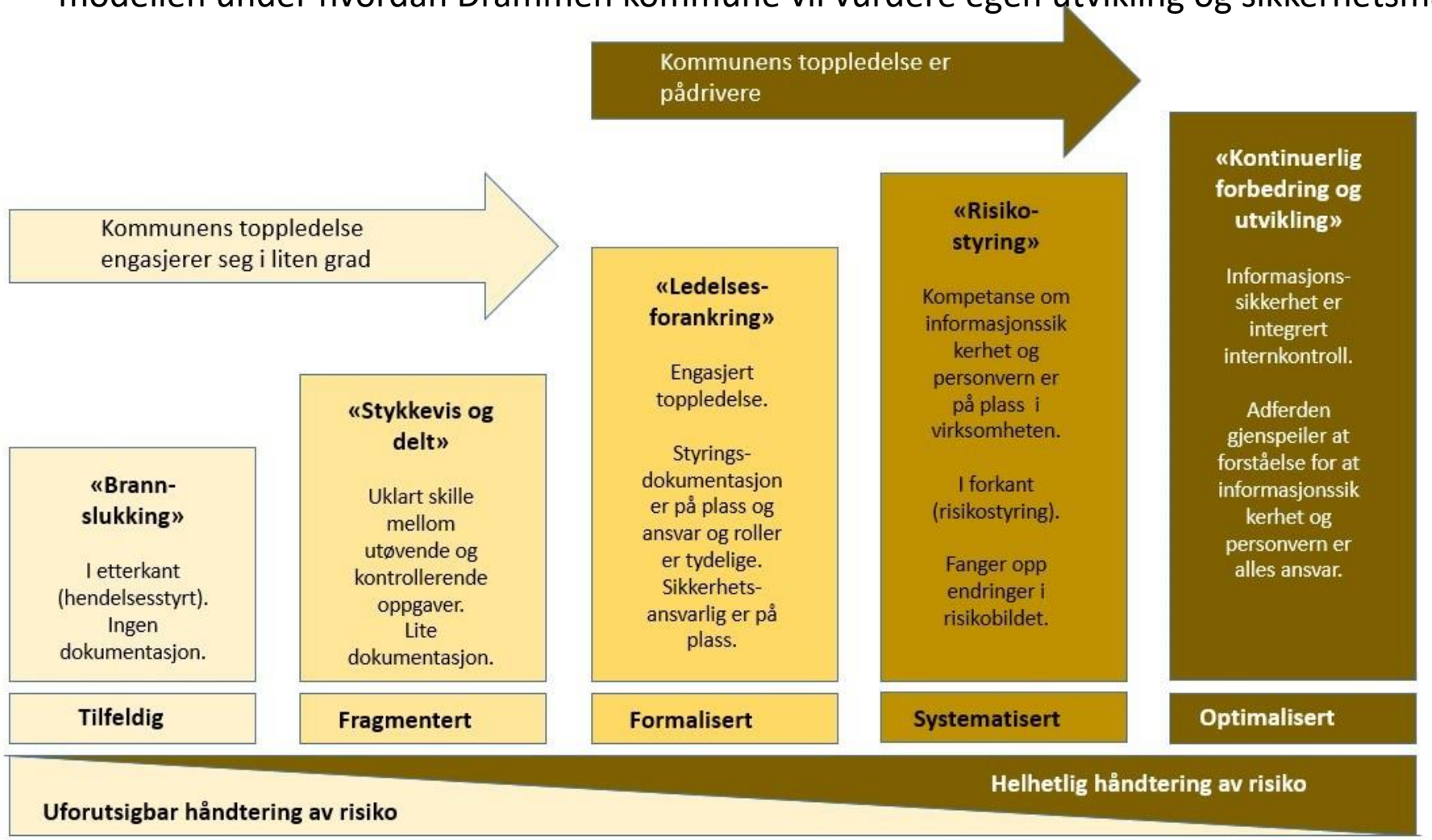
DRAMMEN KOMMUNE
– et godt sted å leve

Arbeid med informasjonssikkerhet

- Kommunen baserer seg på anerkjent rammeverk for informasjonssikkerhet: ISO 27001
- Legger NSM grunnprinsipper for informasjonssikkerhet til grunn
- Zero-trust
- Risikobasert tilnærming fører til at vi må prioritere tiltak hvor effekten er størst

Kommunens informasjonssikkerhetsmål

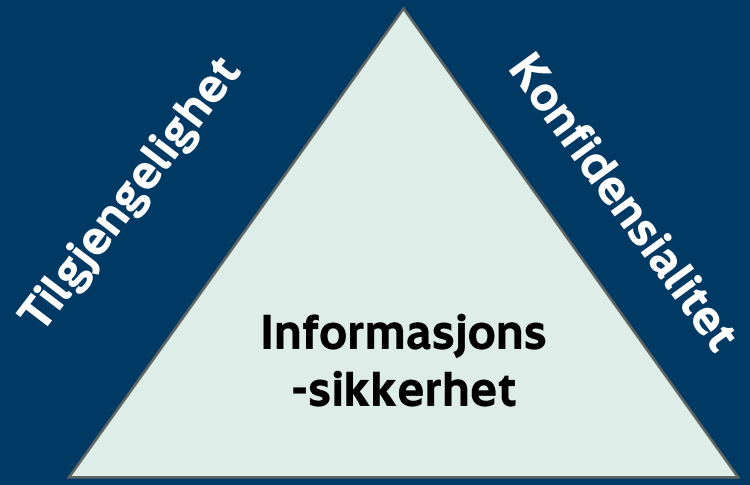
Med utgangspunkt i **nasjonal sikkerhetsmyndighets** modell for modenhetsnivå for sikkerhetsstyring, viser modellen under hvordan Drammen kommune vil vurdere egen utvikling og sikkerhetsmål.



Drammen kommunes har som målsetning å være på modenhetsnivå **Systematisert** innen utgangen av 2024. I løpet av 2026 skal kommunen være på nivå Optimalisert. I lys av dagens trusselbilde, lovkrav, og de potensielt katastrofale konsekvensene ved sikkerhetsbrudd er det avgjørende med høy måloppnåelse.

Hva er informasjonssikkerhet?

Tjenesten oppfyller bestemte krav til stabilitet, slik at aktuell data er tilgjengelig ved behov



Informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til den

God datasikkerhet starter med folk
"Experis"

Informasjon og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig og et resultat av autoriserte og kontrollerte aktiviteter

Informasjonssikkerhet i praksis

- Vi skiller mellom tiltakstyper
  - Tekniske
  - Fysiske
  - Personell
  - Organisatorisk

Tekniske

Sikkerhet på «datarommet» jfr NSM grunnprinsipper

Fysiske

Ha kontroll på hvem som kommer og går

Personell

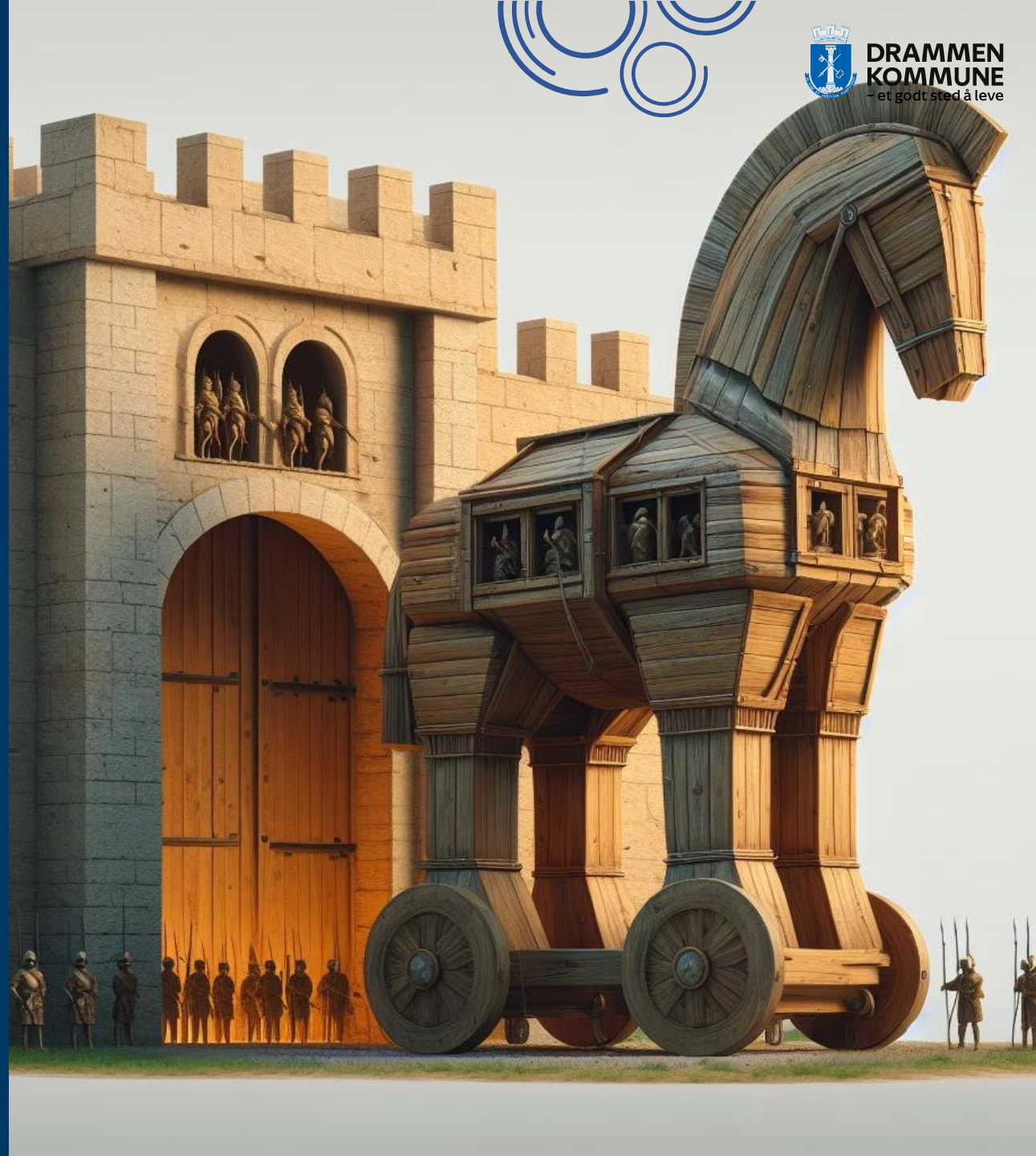
Ha kontroll på hvem vi ansetter

Organisatoriske

«Alt annet» som ikke passer inn i de andre.

Hva betyr dette for deg?

- Standardiserte PC-brukere (Drammen til sky)
  - NSM Grunnprinsipper stadfester at en skal ha kontroll på enheter og all programvare.
  - Whitelisting heller enn blacklisting (godkjent programvare)
- Overvåking og logging av aktiviteter
- Mer robust kommune
- Sikkerhet er alles ansvar



DRAMMEN KOMMUNE
– et godt sted å leve

Som politiker er du et mål

- Myndighetspersoner er utsatte mål for fremmede staters etterretningstjenester
- Russisk etterretningsvirksomhet vil være rettet mot mål i hele Norge
- Kinesiske etterretningstjenester bruker sine cyberkapasiteter mot politiske myndighetsmål i Norge
- Den kinesiske partistaten jobber også gjennom norske lokalpolitikere og næringslivsaktører for å fremme sin utenrikspolitikk og omgå nasjonale beslutningsprosesser.

Svindelforsøk, phishing og sosial manipulasjon

- Gode tekniske tiltak - Mennesket er foretrukken angrepsvektor
- Svindelforsøk kommer i mange former
  - E-post
  - SMS
  - Telefon
  - QR
  - Skadevare
- Konsekvenser

Kjennetegn

- Hvordan kan du vite om avsender er den de utgir seg for å være?
- Forventer du en slik henvendelse fra avsenderen?
- Fremstår henvendelsen som troverdig eller sannsynlig?
- Tidspress og økonomisk konsekvens?
- Hva kan du gjøre?

Hva er et godt passord?

- 8 tegn
- Stor bokstav
- Tall
- Spesialtegn
- Regelmessig passordbytte

- passord
- Passord
- Passord1
- Passord1!
- Sommer2024!

Alle kravene oppfylles, men gir dette oss gode passord?

DRAMMEN KOMMUNE
– et godt sted å leve

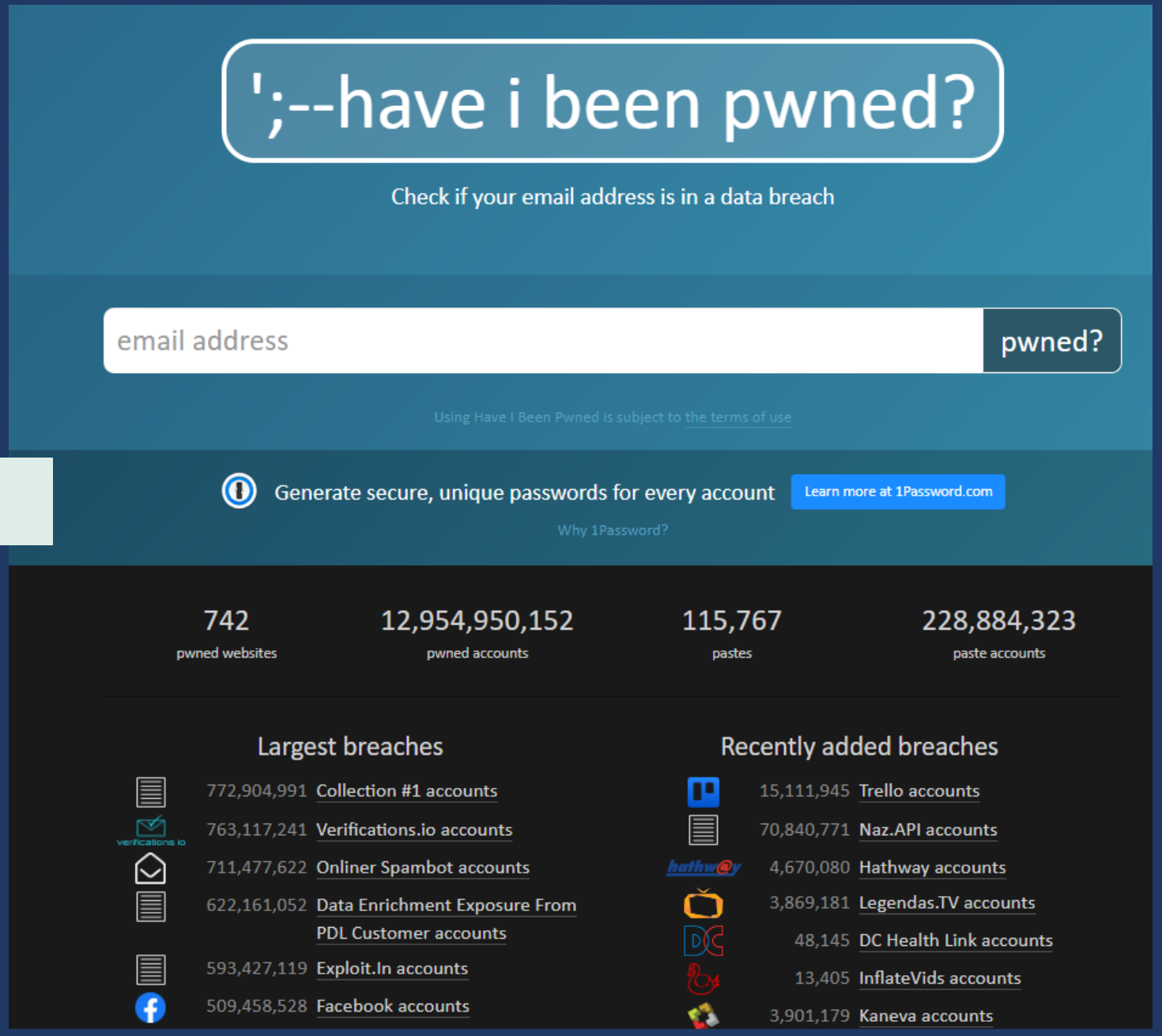
Passordhygiene

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

- Benytt MFA hvor mulig
- Aldri del eller gjenbruk passord
- Minimum 16 tegn
- Lag en setning det er lett å huske
- Bruk mellomrom mellom ordene som vanlig
- Skriv gjerne på dialekt

https://haveibeenpwned.com/

Kontrollert eller kompromittert



Rød = lekkasje av data
Grønn = ikke rammet ennå!

[Have I Been Pwned: Check if your email has been compromised in a data breach]

DRAMMEN KOMMUNE
– et godt sted å leve

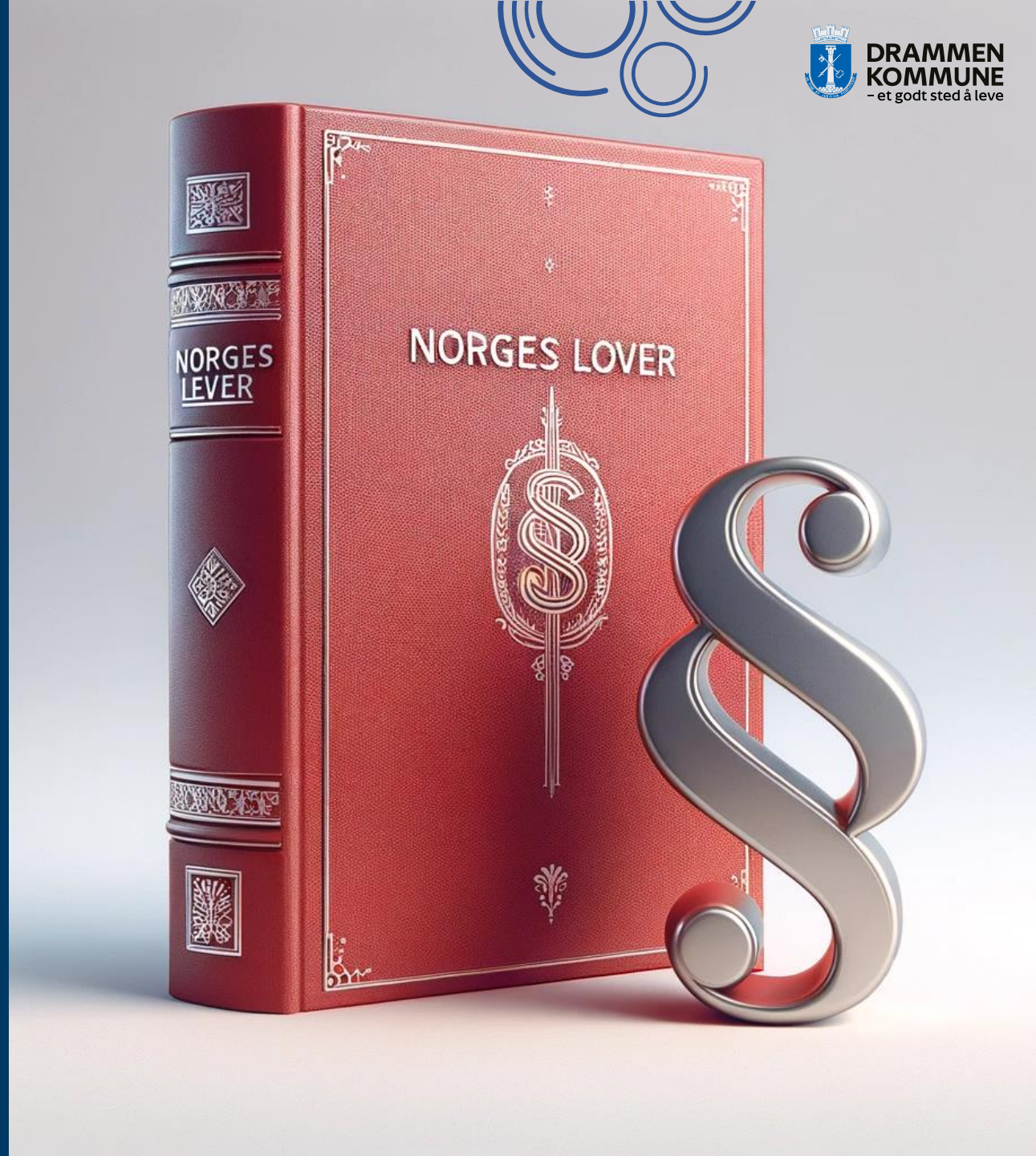
Personvern

Det store bildet

- Digitaliseringen går fort
- AI øker datamengde og hastighet
- Datadrevet økonomi gjennom EU - 2030 Policy Programme «Path to the digital decade» EU har satt av 100 milliarder
- 116 rettsakter knyttet til digitalisering!
- «Forordning om europeisk helsedataområde (EHDS)» og «KI-forordningen om kunstig intelligens» «eIDAS - elektronisk identifisering og tillitstjenester for elektroniske transaksjoner i det indre marked»
- Gapet mellom våre «verdier» og kontrollen over disse øker (regulatorisk og reelt)
- Personvernet taper mot digitaliseringen

Personvernforordningen

- Menneskerettighet – trinnhøyde som grunnlov
- Gjelder digitale data
- Krav til lovlighet og åpenhet
- Formålet skal være klart definert – ikke brukes til annet formål
- Krav om risikovurderinger og dokumentering
- Krav til informasjonssikkerheten
- Drammen kommune er ansvarlig – bøter på opptil 4% av 8 mrd.



Politiker – uten hjemmel

PERSONVERN

Jussekspert: Politiske e-poster til foreldre i Stavanger kan være brudd på GDPR

De rødgrønne partiene i Stavanger brukte kontaktlister fra skolene til å sende ut politiske budskap på e-post til foreldre. Nå reagerer eksperter.

En ordfører i Belgia sendte ut politiske e-poster ved hjelp av epostadresser samlet inn i løpet av sin tid som ordfører. I denne konkrete saken gjaldt det e-poster en innbygger hadde sendte til ordførerens kontor knyttet til en klage.

Han fikk en bot på € 5000.

Tyskland - publisering av skjermdump

En politiker publiserte en skjermdump fra et rådgivende styremøte på sin egen side. På dette bildet kunne man blant annet se en annen lokalpolitiker.

- Publiseringen ble påklaget
- Datatilsynet påla sletting og forbød fremtidige opptak, og liknende skjermdump fra disse møtene
- Begrunnelsen:
  - Til tross for en offentlig person og av interesse for allmennheten, krenket det personvernet
  - Informasjon fra møte var tilgjengelig i protokollen
  - Formålet med skjermdumpen kunne tolkes som ærekrenkende og ikke knyttet til arbeidet

FOTO: MARTIN GUNDERSEN / NRK

Sosiale medier

- Ensomhet
- Psykiske lidelser
- Narsissisme
- Desinformasjon
- Fake news
- Polarisering
- Distrahering
- Konspirasjonsteorier
- Populisme
- Kulturkrig
- Demokratiet svekkes (i 2010 på topp)

Kort om KI

- Risiko – KI benyttes av trusselaktør
- Potensiale
- Er det vill vest og fritt frem?
  - NEI!
  - Regelverk – AI act kommer, men GDPR gjelder fortsatt. Art 5 og at 32.
- Kjøreregler - KIT

Takk for oppmerksomheten!