

VÅRE «SIDER»

*Professor Kjell Bratbergsengen,
Institutt for datateknikk og informasjonsvitenskap,
NTNU*

kjellb@idi.ntnu.no

906 17 185

Arr:

*Seniornett Trondheim
mandag 26. mai kl. 14:00
Gulhuset, Voll*

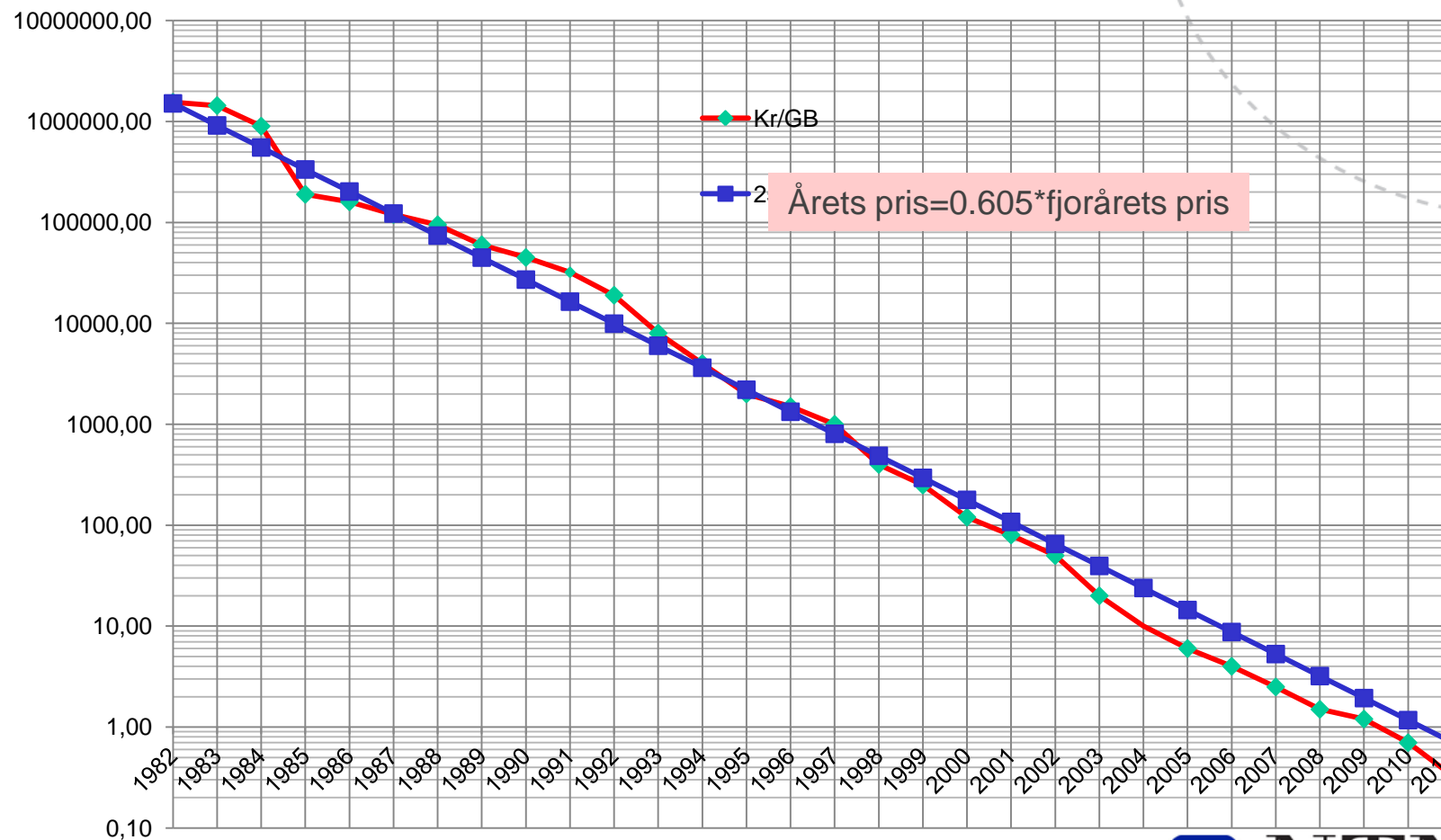
Bakgrunn

- Startet på NTH Bygg 1963, fullførte vår 1968
- Arbeidet med data siden 1964
- Fast ansatt NTNU siden 1970, lektor, dosent 75, professor 85
- Instituttleder, dekanus, phd-veileder for forrige rektor 😊
- Utstyr, metoder og programvare for lagring, bruk og utnyttelse av store datamengder
- De siste år: Bruk av informasjonssystemer i offentlig forvaltning, særlig helse, pleie og omsorgssektoren
- Velferdsteknologi

Oppgaven slik den ble gitt

- *Mer og mer baserer både offentlige myndigheter og private selskaper og organisasjoner seg på at deres kommunikasjon med oss brukere skal skje på nettet gjennom ulike versjoner av «Min side» eller hva nå man kaller det.*
- *For eksempel skal regjeringen i de neste 3-4 årene gjennomføre et stort digitaliseringsprosjekt som har som mål at all kommunikasjon mellom det offentlige og oss innbyggerne som hovedregel skal skje elektronisk. For å få f. eks. selvangivelsen på papir må vi spesielt be om det.*
- *Vi må leve nye prosedyrer og sikkerhetsrutiner på nettet i en verden hvor også teknologien og redskapene stadig endrer seg. Her blir det mye å lære.*
- *Gi en orientering om utviklingen og hvordan systemene vil være bygget opp: passord, tallkoder Java, etc. slik at man kan føle seg noenlunde trygg når man beveger seg i skogen av de ulike oppleggene*

Diskpriser over 30 år



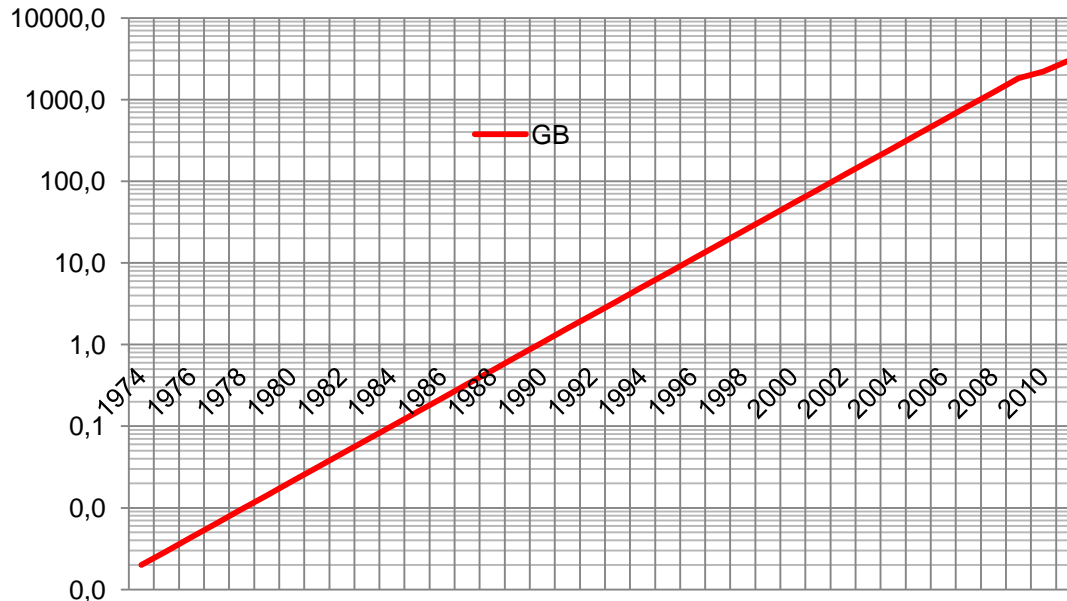
Prisutvikling for magnetisk disk

- Prisen er 40-60 øre per GB i 2014
- Prisen har gjennomsnittlig sunket med en faktor 0.61 per år siden 1982.
- Ikke kjøp disk før du trenger plassen
- Også kapasiteten per lagringsenhet har økt dramatisk.
- 2 MB disk i 1974,
- 6 TB disk i 2014
- Diskens størrelse øker med ca. 40% per år.

Typiske databasestørrelser

- K – kilo = 1024 = $2^{10} \approx 10^3$
- M – mega = 1024 K = $2^{20} \approx 10^6$
- G – giga = 1024 M = $2^{30} \approx 10^9$
- T – tera = 1024 G = $2^{40} \approx 10^{12}$
- P – peta = 1024 T = $2^{50} \approx 10^{15}$
- E – exa = 1024 P = $2^{60} \approx 10^{18}$

Største magnetiske disk i GB versus år



Størrelsen doubles hver 18. måned (Moore's law).

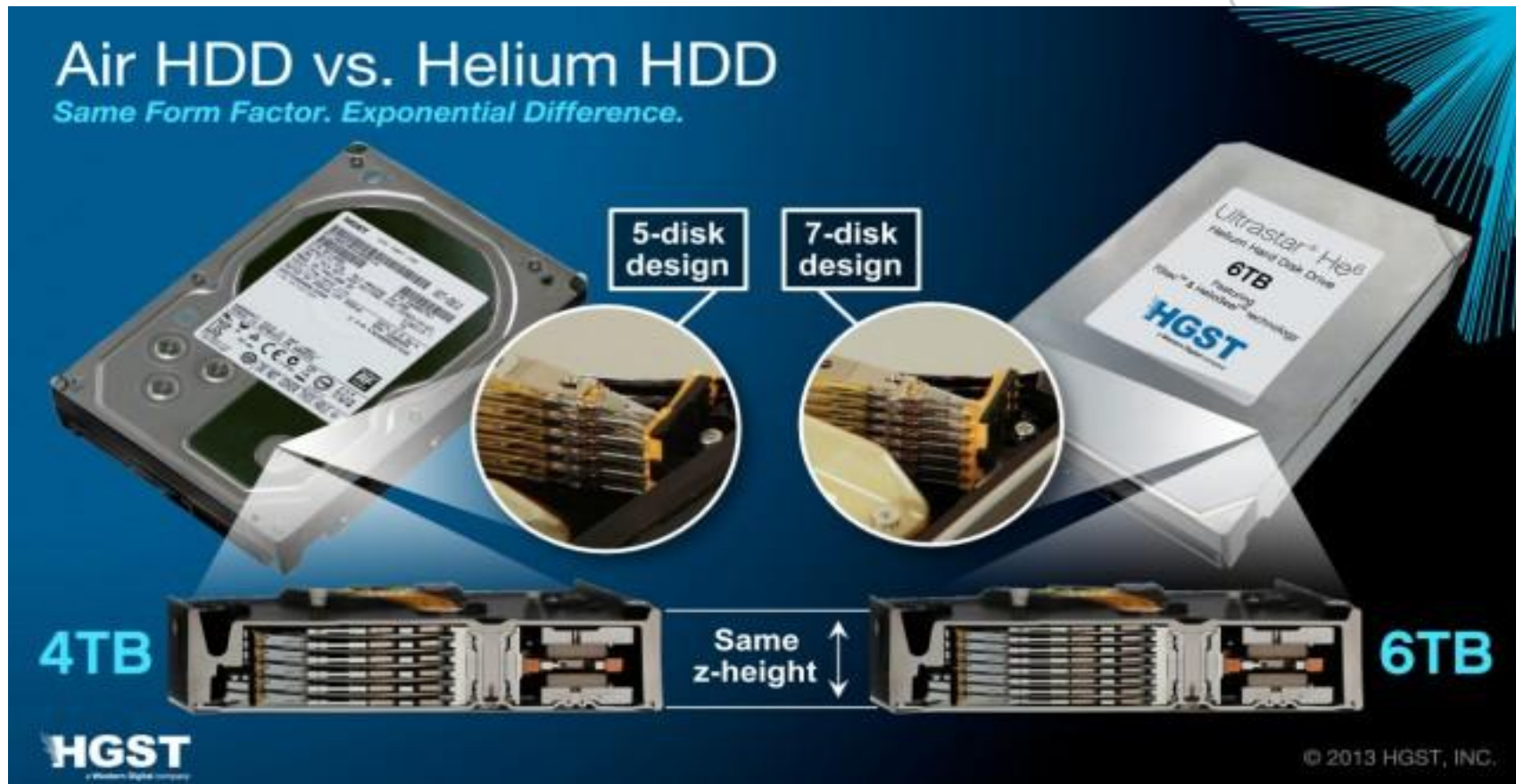
Nå: 6 TB, mer enn 1,5 millioner fotografier, 1,5 milliarder sider med tekst

Pris: 900-1400 NOK for 3 TB disk

Energiforbruk: 9 W,

Vekt: 0,75 kg

6 TB disk er tilgjengelig



Hvor kommer datavolumene fra?

- Ikke skreven tekst, en A4-side med tekst er ca. 4000 tegn (byte)
- Det er sensorer som genererer volumer.
 - Et vanlig amatørbilde 1-20 MB
 - Film, sensorer
- DNA: mennesket 3 G-verdier (CGTA), minst 2 M verdier er forskjellige fra individ til individ.

Egen lagring kontra felleslager

- Fordeler med egen lagring
 - Billig
- Ulemper med egen lagring
 - Risikabelt, sikker lagring krever både utstyr og rutiner
 - Vanskelig å dele data mellom enheter og mellom familiemedlemmer og venner
 - Slitsomt å følge med, dataene må skrives om hvert 3. år
 - Krever kompetanse
 - Kan etablere egen felles server

Datahotell, det frie marked

- Google
 - Twitter
 - Facebook
 - Instagram
 - Dropbox
 -
-
- De første GB er gratis, plass utover en grense må betales
 - Laster opp privat materiale
 - Betales helt eller delvis med reklame

Det offentliges databaser

- Brønnøysundregistrene
- Skatt, pensjonspoeng, selskapsinformasjon, matrikkel (eiendommer, grenser, eiere)
- Journaler, 17 000 systemer som lagrer helsejournaler
 - Specialisthelsetjenesten: sykehus
 - Primær: Fastlegen
 - Pleie og omsorg: Kommunene
 - Andre: Tannleger, fysioterapeuter,
- Førerkortregister
- Veidatabaser
- Kartdata (stat og kommune)
- ... alt mulig ...

Private selskapers databaser

- Banker og finansinstitusjoner
- Interessant utvikling:
 - Før drev de største bankene selv sine datasystemer
 - I dag settes det ut til profesjonelle aktører
 - Typisk i Norge: EVRY
- NETS - tidligere BBS Bankenes betalingssentral - utfører alle transaksjoner som går mellom banker.

Personnummeret

- dd mm yy lll cc
- 01 01 00 000 00
- 31 12 99 999 99

Gjennomgående identifikator av alle personer som bor i Norge.

Må endres senest 2050

“Sprekker” kanskje allerede i 2030

Personnummeret, detaljerte regler

Norwegian Personal Identification Number - NPIN

Norwegian personal identification number has following elements: $d_1d_2m_1m_2y_1y_2l_1l_2l_3k_1k_2$. The first 6 digits are: *day*, *month* and 2 last digits in *year* for date of birth. $l_1l_2l_3 = L$ is a *serial number*. Since *year* only has 2 digits, one must use L to determine century - following these rules:

Condition	Year
$0 \leq L \leq 499$	1900 to 1999
$(500 \leq L \leq 749) \wedge (y_1y_2 > 54)$	1855 til 1899
$(500 \leq L \leq 999) \wedge (y_1y_2 < 55)$	2000 til 2054

l_3 indicates sex - odd number for males, even number for females. Last 2 digits k_1 and k_2 are check digits, calculated after following formulas. Indexing is assumed to be self-explanatory.

$$S_1 = 3d_1 + 7d_2 + 6m_1 + 1m_2 + 8y_1 + 9y_2 + 4l_1 + 5l_2 + 2l_3$$

$$Q_1 = S_1 \div 11$$

$$k_1 = 11 - (S_1 - 11 \times Q_1)$$

Q_1 is an integer - always truncated, never rounded. If k_1 is 10, this serial number is not used. Instead, next serial number is taken. If k_1 is 11, then k_1 is set to 0. Other values are used as is.

k_2 is calculated in similar way. Note that first check digit is used for check digit calculation.

$$S_2 = 5d_1 + 4d_2 + 3m_1 + 2m_2 + 7y_1 + 6y_2 + 5l_1 + 4l_2 + 3l_3 + 2k_1$$

$$Q_2 = S_2 \div 11$$

$$k_2 = 11 - (S_2 - 11 \times Q_2)$$

If k_2 is 10, serial number is not used. If k_2 is 11, k_2 is set to 0. Other values are used as is. Design of control digits are so that common typing errors, for example, reverse order of digits, will surely be discovered.

Source: Tax Directorate and Central Population Register.

Offentlig forvaltning

- Ikke et entydig begrep
- To grupper:
 - Stat
- Ståldør
 - Kommunal

- Kommunalt selvstyre er hellig.
- Som innbygger pendler vi mellom begge

Digitale postkasser (1)

- Hvorfor:
 - Vanlig post er tungt, kostbart og langsomt
 - En digital postkasse nås uavhengig av geografi og mobilitet
 - Slipper adresseendringer eller forsinket post i ferier o.l.
 - Kan gi brukeren tjenester utover tilgang til meldinger og dokumenter

Digitale postkasser, spørsmål (2)

- Abstrakt
- Adgang til egen postkasse
- Innsyn i egen postkasse
- Opplæring
- Hvordan bistå dem som trenger hjelp?
- Hvordan få hjelp?
- Hvordan vite når en trenger hjelp?
- Sikkerhet
- Pålitelighet
- Hva skjer hvis en leverandør går konkurs?
- Hvilket ansvar har postkasseleverandør for tap av data?
- Hvordan kan du vite om alt du har lagret faktisk fortsetter å bli lagret?

Hvordan?

- Eget register som forteller hvem som har digital postkasse og hvilken det er
- Dette kalles Meldingsformidleren og er et eget register som sier hvilken postkasse man har.
- Kunne ha vært en utvidelse av Folkeregisteret
- Kan vi ha mange digitale postkasser?
- Hvordan kan vi skifte fra en digital postkasse til en annen
- Hvordan blir vi varslet når det kommer noe nytt i postkassen?
- Hvordan blir vi varslet hvis vi ikke leser eller henter ut det som ligger i postkassen

Digitale postkasser i Norge

Vinnere av DIFs anbuds konkurranse

- Digipost – eid av posten
- e-Boks – eier ukjent skandinavisk aktør

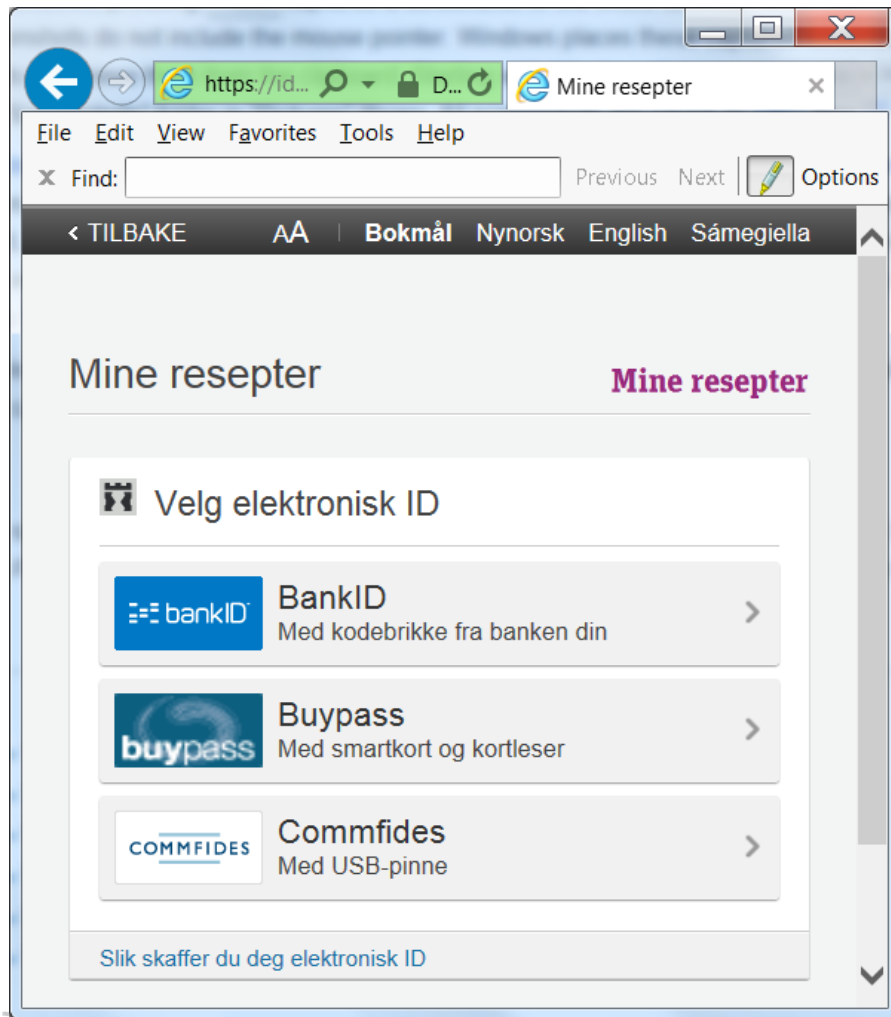
Offentlig post skal gå digitalt i løpet av 2014

- Reservasjonsrett, men ...
- Aktiv reservasjon

Bøygen ?

- I en digital postkasse ligger brevene åpne uten konvolutt.
- Konvolutten er selve postkassen
- Derfor må vi sikre oss at de som kan se i postkassen faktisk har lov.
- Postkassen er personlig - ingen felles postkasser?
- Adgang til postkassen følger en sikkerhetsrutine som er lik de vi har til bank, AltInn og helsedata, osv.
- Problemet er at vi har mange alternativ og også forskjellig sikkerhetsnivå

Innlogging



Mange forskjellige systemer

BankId

- Bestilles i banken
- Krever passord
- Kodegenerator

- Noe de fleste har ?
- Mest anvendelig, men også tungvint

Buypass

- Identitet i smartkort
- Krever smartkortleser
- Passer godt for dem som logger seg av og på terminaler mange ganger I løpet av en arbeidsdag
- Eies av Evry og Norsk Tipping (50-50)

Commfides

- Pålogging med USB-pinne
- Næringslivsorientert?
- Enkelt?

Opphør, Digipost (1)

- Ved opphør av avtalen ved oppsigelse vil Brukerens adgang til å sende og motta Meddelelser deaktiveres på opphørstidspunktet.
 - Brukeren vil ha adgang til lagrede data i tre måneder etter opphørstidspunktet. Deretter slettes lagrede data.
 - Brukeren er selv ansvarlig for å ta kopi av alle data Brukeren ønsker å beholde etter opphørstidspunktet.
 - Posten forbeholder seg retten til å beholde data som er nødvendig for oppfølging av kundeforholdet.

Opphør, Digipost (2)

- Dersom Brukerens Digipostkonto har vært inaktiv i mer enn 14 måneder, kan Posten deaktivere muligheten til å sende og motta Meddelelser.
- Dersom Brukeren dør, vil Brukerens Digipostkonto og lagrede data slettes tre måneder etter Posten fikk beskjed om dødsfallet. De(n) som kan forplikte Brukeren må kontakte Digipost for å få tilgang til Brukerens Digipostkonto innen sletting. Posten forbeholder seg retten til å beholde data som er nødvendig for oppfølging av kundeforholdet.

E-Boks – egenreklame (1)

- **Visste du at...**
- med e-Boks kan du **få brev både fra offentlige og private virksomheter**
- du kan laste opp **verdifulle dokumenter** og lagre dem trygt i din e-Boks
- du kan **gi andre tilgang** til din e-Boks
- med e-Boks sin app har du **alltid tilgang** til dine viktige dokumenter
- e-Boks' løsning har **universell utforming** slik at alle kan bruke tjenesten
- du **får beskjed på e-post** når du har fått post
- du kan opprette et oversiktlig, **digitalt arkiv** ved hjelp av vår brukervennlige mappe-struktur
- over **åtte millioner** mennesker allerede bruker e-Boks
- vi har laget en liten film der du kan **lære mer om e-Boks**. [Se filmen her](#)

E-Boks (2)

Slik oppretter du e-Boks

- Du trenger **BankID** for å opprette deg som bruker av e-Boks.
- Velg **Opprett e-Boks**
- Deretter vil du bli veiledet gjennom en enkelt opprettelsesprosess der du kan taste inn e-epostadresse og godta vilkårene for bruk av e-Boks.
- Til slutt velger du hvilke avsendere du ønsker å motta post fra i e-Boks.

Deretter er du klar til å motta posten i e-Boks, og du vil automatisk få en e-post når det er ny post til deg.

Sikkerhet, “praktiskhet”

- Lagring –
 - Mot innsyn fra uvedkommende: God, lagres kryptert
 - Mot tap av data: God, lagres i flere kopier
 - Kontrollerbart: Nei, ikke angitt metode, bare ved gjennomsyn av dokumenter.
 - Tilgang ved tap av nøkler? Usikkert
 - Sikkerhet for å overse viktige meldinger? Varsling: SMS, email
- Overføring – god, overføres kryptert
- Tilgang, god sikkerhet, men tungvint

Krav til innlogging?

- **En felles innloggingsmekanisme ?**
 - Barnehage
 - Skole
 - Bank
 - Sosiale medier
 - Offentlige og private tjenester
 - Et virvar av passord og prosedyrer som ikke huskes