Bruk av skytjenester

Sikkerhet, personvern og juridiske forhold i skyen

Hallstein Husand, fagdirektør

IKA Trøndelag
Trondheim 24. mars 2015

Datatilsynet

Utgangspunktet

- Det er Datatilsynets utgangspunkt at det er mulig å oppnå godt personvern også i nettskyen

- Dette er et syn vi deler med øvrige personvernmyndigheter

- http://www.datatilsynet.no/Teknologi/Nettsky---Cloud-Computing/Cloud-Computing/

"Kan vi bruke skyen?"

- Ja!

- Men det er alltid et "men"...

Overordnet
Kort om skytjenester (Cloud Computing)

- Er det egentlig skytjenester noe nytt?
  - ASP, Fjerndrift, stormaskin, hosting, …

- Rokker ikke ved ansvarslinjene
  Virksomhet ⟹ Leverandør
  Behandlingsansvarlig ⟹ Databehandler

- Bruk av sky betyr ikke fravær av kontroll
  (i så fall er det uforenelig med regelverket)

Overordnet
Vi avgrenser oss til personopplysninger

- Regulert av personopplysningsloven og personopplysningsforskriften
- Informasjonsverdien som skal sikres er **personopplysninger**
- Virksomheten (behandlingsansvarlig) skal etterleve regelverket
- Det kan også være andre sikkerhetsbehov og myndighetskrav

Overordnet
Andre myndighetskrav

- Eksempler på mulige andre sikkerhetsbehov og myndighetskrav

- Interdepartemental arbeidsgruppe
  Kartlegging av hindringer i regelverk for skytjenester - Mandat for arbeidsgruppe
  Ventet til sommeren 2015

- Riksarkivaren seier nei til skyarkivering i utlandet

- Nordisk Ministerråd – Skytjenester i offentlig sektor

Et eksempel

«Narviksaken»

Bakgrunn

- Skytjenester hos
  - Narvik Kommune (Google Apps) og
  - Moss kommune (Microsoft Office 365)

- 2011 Klage på Narviks bruk av Google Apps. Datatilsynet varslet vedtak om opphør

- Moss kommune: Veiledningsspor

- Dialog med kommunene og leverandørene

COMPUTERWORLD – it-nyheter døgnet rundt
IDG – verdens største mediehus innen it

Sier nei til Google apps

Nard Schreurs
24.01.2012 kl 15:24

Epost

Datatilsynet vil ikke ha Googles nettjenester inn i norsk offentlig sektor, og gir Narvik kommune "nei".

STOPP: Bjørn Erik Thon sier nei til Google Apps i offentlig sektor. (Foto: Nard Schreurs)

Datatilsynet har i dag bekreftet at de vil forsøke å stoppe Narvik kommune hvis den fortsetter med å ta i bruk Googles verktøy fra nettskyen, Google Apps.

I Datatilsynets vurdering sier direktør Bjørn Erik Thon at «tjenesten strider mot personvernlovgivningen på flere punkt».

Tweet 14 +1 0 Anbefal

ANNONSE

Resultat

- Åpner for bruk av skytjenester
- Ingen blancofullmakt
- Behandlingsansvarlig har ansvaret
  - Skal gjøre selvstendige vurderinger
  - Skal ha kontroll med underleverandører
  - Skal ha tilfredsstillene informasjonssikkerhet
- Noen klare forutsetninger:…

Forutsetninger

1. Grundige risiko- og sårbarhetsanalyser
   Virksomheten må akseptere sikkerheten
   (POL § 13, POF § 2-4)
2. Databehandleravtale som er i tråd med norsk regelverk
   (POL § 15 og §13, jf POL § 2-15)
3. Sikkerhetsrevisjoner
   Bruk av tredjepart?
   (POL § 13 jf. POF § 2-5, samt POL § 14)
4. Databehandleravtalen gjelder! Ikke eventuelle ”drøye” standardvilkår

Hva er så kravene?

…Først litt bakgrunn

Personopplysningsloven

- § 14 – Internkontroll

- § 13 – Informasjonssikkerhet
- § 15 – Databehandlerens rådighet over personopplysningene

Informasjonssikkerhet - Personopplysningsloven

- Plikten ligger på den behandlingsansvarlige
  - Virksomheten v/ledelsen

- § 13 om Informasjonssikkerhet
  - planlagte og systematiske tiltak - rutiner
  - tilfredsstillende informasjonssikkerhet - risikovurdering
  - konfidensialitet, integritet og tilgjengelighet

Informasjonssikkerhet
Personopplysningsforskriften

- § 2-3 Sikkerhetsledelse
- § 2-4 Risikovurdering
- § 2-6 Avvik
- § 2-7 Organisering
- § 2-8 Personell
- § 2-11 Sikring av konfidensialitet
- § 2-12 Sikring av tilgjengelighet
- § 2-13 Sikring av integritet
- § 2-14 Sikkerhetstiltak
- § 2-15 Sikkerhet hos andre virksomheter

10 gode grunner til å...

Databehandleravtale (1)

- Vurder databehandleravtalen
- Tilfredsstiller tjenesten kravene etter risikovurderingen?
- Sikkerhetstiltak

http://www.kiss925.com/2012/05/29/nightly-nonsense-maybe-the-worst-babysitter-of-all-time/

Databehandleravtale (2)

- Generelle databehandleravtaler
- Må følge norsk regelverk
  - Behandlingsansvarlig har fortsatt ansvaret for at lovens krav følges
- Sikkerhetsrevisjon
  - Påse at databehandler iverksetter tiltak og dekker hele kjeden
  - Alternativt tredjepartsrevisjon – krev å få se rapporten!
- Viktige momenter
  - Sikkerhetskopiering
  - Sletting
  - Tilgangsstyring
  - Segmentering av databaser

Databehandleravtale (3)

- Problemstillinger
- Bruk av data til egne formål? (forbedre egne tjenester)
- Leverandørens personvernvilkår (eller andre vilkår), må ikke gå utover databehandleravtalen
- Hvor lagres data? (overføring til utlandet)
- Dataportabilitet
- Sikker kommunikasjon – kryptering mellom:
  - Behandlingsansvarlig ⟷ Databehandler
  - Datasentre
  - Databehandler ⟷ Underleverandør

Problemstillinger generelt (oppsummert)

1. Åpenhet
2. Overføring til utlandet
3. Kompliserte avtaler
4. Oppfølging av leverandøren
5. Sikkerhetstiltak (mot eksterne og «mot» leverandøren)
6. Skille mellom ulike behandlingsansvarliges data
7. Dataportabilitiet
8. Databehandleravtalen gjelder!

Ansvaret…

- … Ligger ikke i skyen!

Er informasjonen som forvaltes verdifull?

- **… Da er det en dårlig ide å ikke ha kontroll på den!**

Den ansattes bruk av private skytjenester

- Selvfølgelig skal ikke de ansatte bruke sine private skyløsninger til å behandle personopplysninger
  - Behandlingsansvarlig har ikke kontroll – derfor er det ikke lov
  - Blir opplysningene utlevert?
  - Kan være en stor forskjell på skyløsninger virksomheten velger å ta i bruk, og løsninger den ansatte selv velger

- … spørsmålet er hvordan dere skal hindre de?
  - Teknisk og administrativt?,
  - Eller bare administrativt?

Teknologi
- Applikasjoner
- Datalagringsdirektivet
- Biometri
- **Nettsky - Cloud Computing**
- GPS og sporing
- Internett og sosiale medier
- Kameraovervåking
- Lydopptak
- Strømmåling
- Webanalyse

Nettskytjenester - Cloud Computing

(Publisert: 25.11.2011 Sist endret: 20.09.2012)

Virksomheter som tar i bruk nettskytjenester er juridisk ansvarlig, og må sørge for at personopplysningene behandles i tråd med personvernregelverket.

I denne veilederen vurderer Datatilsynet nettskyen i lys av kravene i personopplysningsloven og helseregisterloven. Personopplysningsloven gjelder når private eller offentlige virksomheter som er etablert i Norge, behandler personopplysninger ved hjelp av slike nettskytjenester.

Hva er nettskytjenester?

Nettsky, eller Cloud Computing er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett. Disse serverparkene kjennetegnes ved at de er laget for dynamisk skalering. Det betyr at datakraft kan tilpasses kapasitetsbehov, og kunden kan betale for den faktiske bruken. Mange eksterne serverparker står utenfor Norges grenser, og en utfordring for virksomhetene er å sørge for at avtalene er i samsvar med norsk lovgivning.

Virksomheten har behandlingsansvar

Verktøy

Databehandleravtale

Risikovurdering

Artikler

24.09.2012
Åpner for bruk av nettskytjenester

28.12.2011
Lagring i nettskyen

Internasjonalt

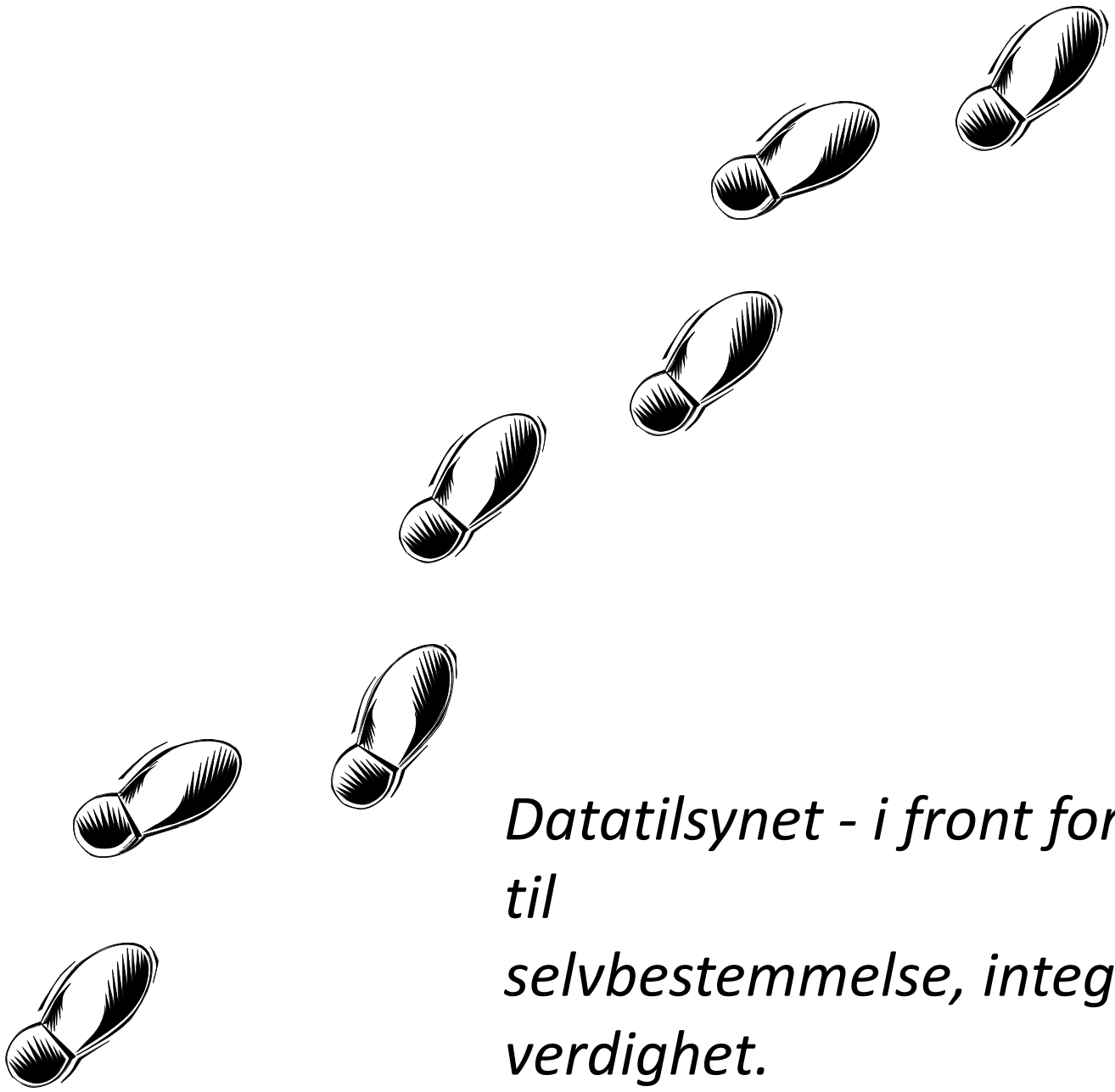
Cloud Computing og ansvarsforhold (uttalelse fra EDPS)

Om Cloud Computing (Uttalelse fra Art. 29-gruppen)

Det italienske datatilsynets veiledning om nettskyen (eng)

Berlingruppens uttalelse

www.datatilsynet.no



Datatilsynet - i front for retten til
selvbestemmelse, integritet og verdighet.

Internasjonalt

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

- Read the Verizon court order in full here
- Obama administration justifies surveillance

telephone calls in its systems, both within the US and between the US and other countries.

The Washington Post

Prices may vary in areas outside metropolitan Washington.

MD DC VA SU V3

Rain 76/69 • Tomorrow: Showers 84/68 • DETAILS, C10

FRIDAY, JUNE 7, 2013

washingtonpost.com • $1.25

U.S. mines Internet firms' data, documents show

Google, Facebook, Apple, Yahoo deny giving NSA direct access to servers

BY BARTON GELLMAN AND LAURA POITRAS

The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post.

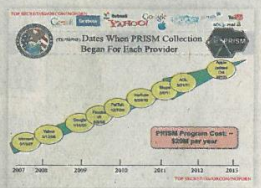
The program, code-named PRISM, has not been made public until now. It may be the first of its kind. The NSA prides itself on stealing secrets and breaking codes, and it is accustomed to corporate partnerships that help it divert data traffic or sidestep barriers. But there has never been a Google or Facebook before, and it is unlikely that there are richer troves of valuable intelligence than the ones in Silicon Valley.

Equally unusual is the way the NSA extracts what it wants, according to the document: "Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple."

PRISM was launched from the ashes of President George W. Bush's secret program of warrantless domestic surveillance in 2007, after news media disclosures, lawsuits and the Foreign Intelligence Surveillance Court forced the president to look for new authority.

Congress obliged with the Protect America Act in 2007 and the FISA Amendments Act of 2008, which immunized private com-

NSA CONTINUED ON A12



Defense and criticism
Lawmakers have split reactions to the revelations regarding the NSA's program to collect data from phone and Internet records. **A14**

Online coverage
A graphic explains key components of the PRISM collection program.

Agency knows much about public, but we know little about it

BY ANNE GEARAN

The National Security Agency, nicknamed "No Such Agency" because of its ultra-secrecy, is the government's eavesdropper-in-chief.

Charged primarily with electronic spying around the globe, the NSA collects billions of pieces of intelligence from foreign phone calls, e-mail and other communications. But in the past two days, the focus has shifted to its role in compiling massive amounts of the same information on millions of ordinary Americans.

Regarded as the most secretive of the nation's intelligence agencies, the NSA is part of the military but answers to the director of national intelligence. Its major operations are housed in uber-secrecy at Maryland's Fort Meade Army base, the site of the court-martial of Pfc. Bradley Manning, who is charged with stealing government electronic communications and passing them to the anti-secrecy organization WikiLeaks.

The agency is so secretive that estimates of the number of employees range from the official

SECRECY CONTINUED ON A13

REUTERS EDITION: U.S. SIGN IN

OPINION BREAKINGVIEWS

Mirror

NEWS

Real news, real entertainment . .

How we use

theguardian

FRONT PAGE NEWS SPORT

Search News World news

Merkel spying row showdown with U

Oct 25, 2013 03:57 By Sam Adams 2 Commen

Share Share Tweet

German Chancellor Angela Merkel revealed tapped by the US intelligence service, the N

Anger: German Chancellor Angela Merkel holds a 'tap

The leaders of France and Germany have cal resolve the spying row.

German Chancellor Angela Merkel revealed the move amidst claims her phone was

Meny Økonomi

Siste nytt: - Stram av vilkår adelegger barseloppholdet

Avganger fra Drammen kl 04:02.

Google, Microsoft, Apple, Facebook, LinkedIn, Yahoo, AOL og Twitter har undertegnet brevet som er adressert til president Barack Obama. FOTO: Afp/Scanpix

Teknologigiganter går hardt ut mot USAs overvåking

Øystein Kløvstad Langberg

Del Tweet E-post Lagre artikkelen i leselisten

I en uvanlig koalisjon mellom åtte av USAs største teknologiselskaper, tar blant andre Google, Microsoft og Apple til orde for betydelig strengere lovgivning når det kommer til overvåking av datatrafikk.

Selskapene har mandag sendt brev til president Barack Obama og den amerikanske kongressen.

Omfattende overvåking

Pensum inntil 40 % rabatt!

Business Money Life & style

illance

Europe threatens to aring arrangements ations, EU executive underlines US w and 'how things have gone badly'

2013 18.40 GMT

missioner Viviane Reding is negotiating with ndal. Photograph: Frederick Florin/AFP/Getty

o freeze crucial data-sharing se of the Edward Snowden revelations e National Security Agency.

The US will have to adjust their surveillance activities to comply with EU officer 'too busy'

KONKURRANSEFORTRINN: Roland Rabben (til venstre) i norske Jottacloud tror norsk personvern gjør Norge attraktivt som land å lagre data i. Spesielt etter at Edward Snowden avslørte amerikanske myndigheters brede overvåking av hjemlige og utenlandske borgere gjennom CIA- og NSA-programmet Prism.

FOTO: SAUL LOEB / THE GUARDIAN / JOTTACLOUD

Snowden ga kundeboom for norsk nettsky-firma

Norsk personvern er så bra at det kan bli en eksportartikkel for norsk IT-bransje, mener gründer.

Internasjonale kilder

- Article 29 Working Party (Art. 29 WP), Opinion 5/2012
  - Etterlevelse av personverndirektivet

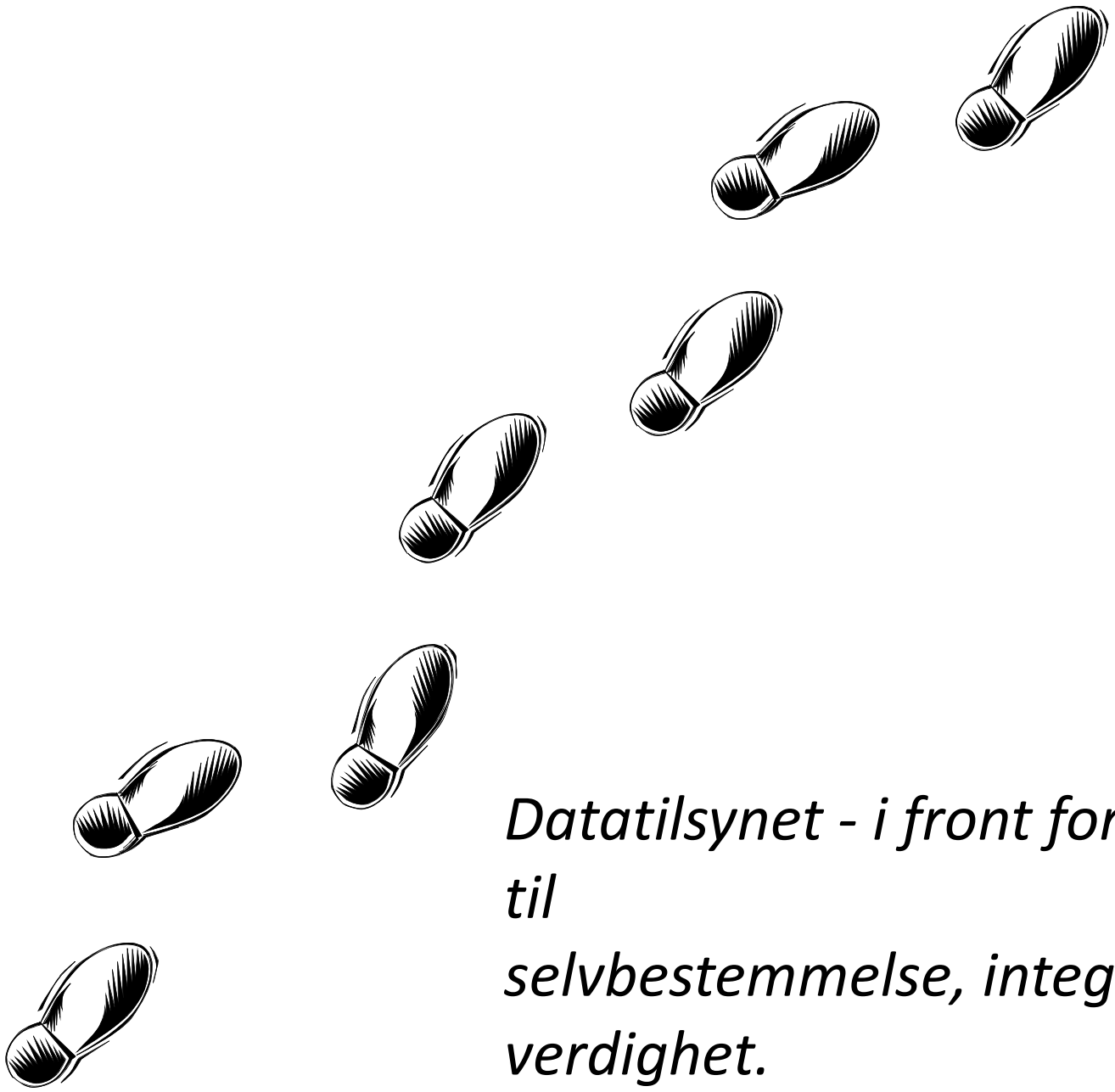
- International Conference of Data Protection and Privacy Commissioners, Resolution October 2012
  - Overordnet

- Berlin gruppen (the International Working Group on Data Protection in Telecommunications (IWGDPT)), Sopot Memorandum April 2012
  - Best Practice - kulepunkter

Internasjonale kilder …

- Industrien
  - Arbeider med en Code of Conduct
  - Vil gå gjennom en prosess med Article 29
  - https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

- Nytt regelverk på vei – forordningen
  - Gjennom parlialmentet 12/3-14
  - Neste stop er Rådet
  - http://europa.eu/rapid/press-release_MEMO-14-186_en.htm



Datatilsynet - i front for retten til
selvbestemmelse, integritet og verdighet.