

Information från Stiftelsen för rättsinformation

2 oktober 2007 (uppdaterat 6 november 2007)

Ordförande professorn Cecilia Magnusson Sjöberg 08 16 28 93

cecilia.magnussonsjoberg@juridicum.su.se

Redaktör forskningsamanuensen Staffan Malmgren 08 16 25 49

staffan.malmgren@juridicum.su.se

Stiftelsen för rättsinformation (www.rattsinfo.se)

ADBJ – Svenska Föreningen för IT och Juridik (www.adbj.se)

Institutet för rättsinformatik vid Stockholms universitet (www.juridicum.su.se/iri/)

välkomnar till

Vad är gällande rätt? - säkerhetskrav vid rättslig informationsförsörjning

Torsdagen den 29 november 2007, kl. 09.00 till kl.16.00

Rosenbads Conference Center, Drottninggatan 1, Stockholm

Bakgrund

Behovet av informationssäkerhet gör sig allt mer gällande i ett samhälle präglad av nätbaserad kommunikation.

Med utgångspunkt i klassiska säkerhetsfaktorer som tillgänglighet, datakvalitet, konfidentialitet m.m. söker konferensen utmejsla vad som är särskilt angeläget att beakta vid rättslig informationsförsörjning.

Här är ett axplock av frågeställningar som talarna kommer att belysa:

- Vad är säker rättslig informationsförsörjning?
- Vem är kravställare?
- Hur kan säkerhet åstadkommas?
- Vilken uppföljning är motiverad?
- På vilket sätt fördelas ansvar?

Program (med reservation för ändringar)

Tid	Ämne	Talare
09.00 - 09.30	Registrering. KAFFE	
09.30 - 09.45	Inledning	Professor Cecilia Magnusson Sjöberg , Stiftelsen för rättsinformation och Institutet för rättsinformatik (IRI)
09.45 - 10.15	Informationssäkerhetens landskap	Olle Olsson , Forskare, Swedish Institute of Computer Science (SICS)
10.15 - 11.15	Tillgänglighet Statens åtagande Affärsmässiga incitament Rätten till access – räcker det med rättsinformationsförordningen och TF?	Hans Sundström , Chefsjurist, Verva Lars Klasén , Civilingenjör, informationsspecialist, InfoTorg Daniel Westman , Doktorand, IRI
11.15 - 11.30	P A U S	
11.30 - 11.50	Datakvalitet Elektroniskt kungörande av vissa trafikföreskrifter	Jenny Forkman , Rättssakkunnig, Näringsdepartementet
11.50 - 12.30	Konfidentialitet Integritetsskydd vid publicering av rättsinformation på nätet Etiska överväganden och funktionell användning av digital kommersiell rättsinformation	Hans-Olof Lindblom , Dataråd, Datainspektionen David Eriksson , System development lawyer, Mannheimer Swartling
12.30 - 13.30	L U N C H	
13.30 - 14.00	Spårbarhet Behovet av att kunna återskapa tidsmässiga samband, närhet i sak och processer för rättslig dokumentframställning	Rolf Riisnæs , Advokat dr. juris, Wikborg Rein (Oslo)
14.00 - 14.30	Ansvar Statens ansvar för digital rättsinformation vid fel och brister	Ylva Ehrnrooth , Jurist, Riksrevisionen
14.30 - 15.00	KAFFE	
15.00 - 16.00	Paneldiskussion Tillit till rättsinformation	Moderator: Professor emeritus Peter Seipel , IRI Helena Andersson , Doktorand, IRI Peter Danowsky , Advokat, Danowsky & Partners Advokatbyrå Jörgen Nilsson , Chefsjurist, Domstolsverket Nicklas Lundblad , Europeisk policyrådgivare, Google

Anmälan m.m.

Det är ingen konferensavgift. Deltagarna betalar sina egna luncher.

Anmälan kan göras på www.juridicum.su.se/iri/rattsinfo senast den 23 november 2007.

Konferenslokalen rymmer ett begränsat antal platser. Först till kvarn...

”Rättslig Informationsförsörjning – säkerhet”

Stiftelsen för rättsinformation

Svenska Föreningen för ADB och Juridik

29 november 2007

Informationssäkerhet

En modell

Olle Olsson

Swedish Institute of Computer Science



SICS – Swedish Institute of Computer Science

Nationellt
forskningsinstitut

– FoU inom IT

Mål:

– Bedriva avancerad och fokuserad forskning inom strategiskt viktiga IT-områden



Sponsorer:

- TeliaSonera
- Ericsson
- Saab Systems
- FMV
- Green Cargo
- ABB
- Bombardier Transportation

Om informationssäkerhet

Säkerhet:

- Av vad?
- För vem?
- Uppnå vad?

Budskap:

- Säkerhet bidrar till tillförlitlighet
- Medel för balansering av intressentintressen

Historiska drivkrafter

”Datacentraltiden” – fokus på:

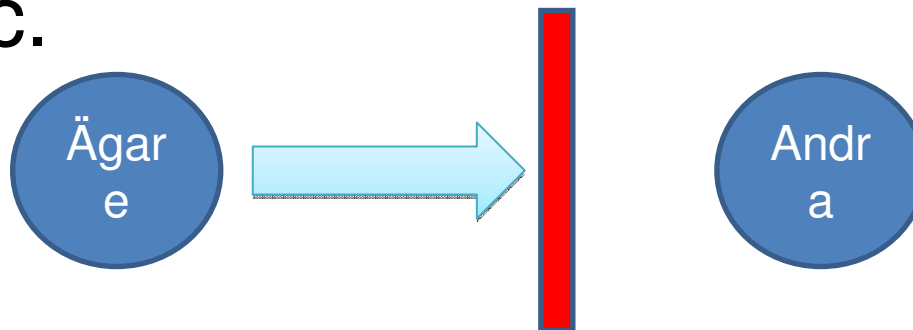
- Fysiskt skydd av data (media)
 - Ej förlora/ej förstöra (förlora egen åtkomst)
 - Oavsiktligt
 - Avsiktligt
 - Ej sprida (andra får åtkomst)
 - Stöld
- Säkerställa arkivering
 - Åtkomst inom viss framtid

Informationssäkerhet – förr

Betoning på:

- Mål: hemlighållande
- Objekt: ett hanterligt antal databaser

Begränsa tillgång, bygg murar, stäng in, etc.



Dagens drivkrafter

Sammanhanget IKT (**I**nformations- och **k**ommunikation**s**teknol

Bred användning	verksamhet på IT-bas
Föränderligt landskap	teknik, verksamhet, ...
Sammanvävda	nätverkssamhället
Kritisk infrastruktur	för samhälle och aktörer
Logiskt skydd	digitala sfären – data och program
Fysiskt skydd	datorer, nätverk, minnen, ...

Övergripande mål

Information (i samhället) skall bidra till:

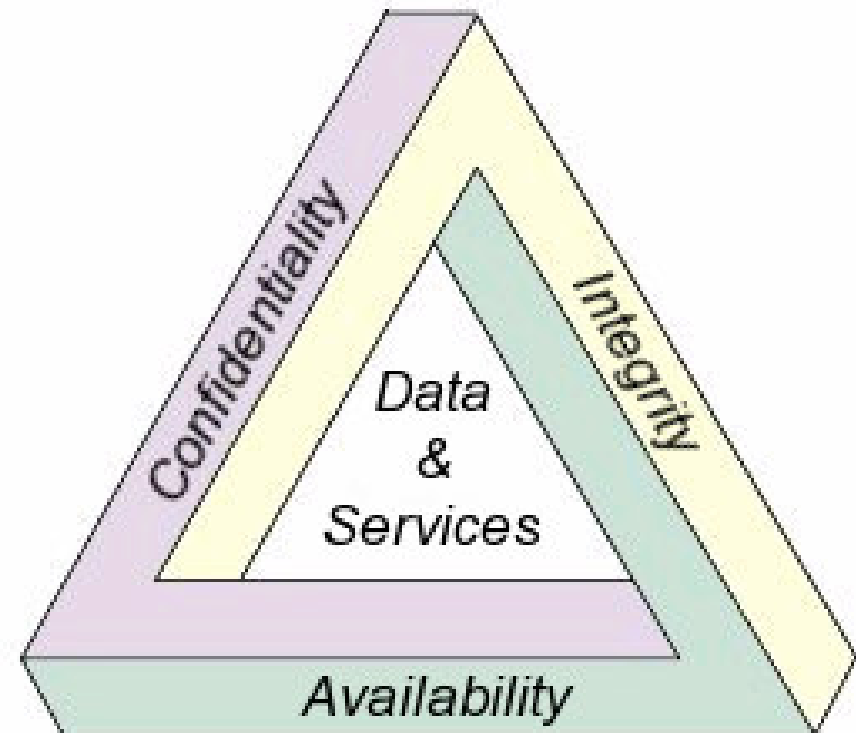
- Kostnadseffektivitet
- Kvalitet
- Transparens
- Uniformitet
- Delaktighet
- Innovativitet
- Etc. ...

Begreppet "säkerhet"

- Samlingsbegrepp
 - Ett antal icke-funktionella aspekter
- Säkerhet mångfacetterat
 - Mångdimensionellt
- Konkreta målsättningar
 - I varje sammanhang
 - För varje aspekt

Aspekter: CIA-triaden

- Konfidentialitet ("confidentiality")
 - Skyddas information mot otilbörlig åtkomst?
- Integritet ("integrity")
 - Har data ändrats otilbörligt/oönskat?
- Tillgänglighet ("availability")
 - Fås information inom rimlig tid?



Aspekter: Parkers hexad

- Konfidentialitet (“confidentiality”)
 - Vem ska inte få tillgång till information?
- Innehav (“possession”, “control”)
 - Har någon annan tillgång till information?
- Integritet (“integrity”)
 - Är informationen oförändrad?
- Autentisering (“authenticity”)
 - Är informationen tillskriven rätt källa?
- Åtkomlighet (“availability”)
 - Kan information åkommas inom rimlig tid?
- Användbarhet (“utility”)
 - Kan informationen användas på avsett sätt?

Aspekter: ytterligare några

- Autentisering av aktör (“authentication”) – Vem är du?
- Auktorisering av aktör (“authorization”) – Vad får du göra?
- Tillförlitlighet (“admissibility”) – Kan jag lita på dina mekanismer?
- Säkerhetsgranskning (“auditing”) – Är säkerheten väldefinierad och underbyggd?
- Spårbarhet (“accountability”) – Vem har gjort vad med data?
- Icke-förnekelse (“non-repudiation”) – Hur visa vem som gett vad till vem?

Medel för informationssäkerhet

Typer av medel:

- Tekniska
 - Fysiska – apparater , sladdar, kort, minnen, ...
 - Logiska – digitala mekanismer
- Administrativa
 - arbetsgång, hantering, processer
- Policies
- Lagar, förordningar, ...
- Standarder
- Etc. ...

Tekniska medel - exempel

- Konfidentialitet
 - Kryptografi
- Integritet
 - Checksummer & digitala signaturer
- Åtkomlighet
 - Indexering och sökning
- Autentisering
 - Signering

Säkerhet m.a.p. vad?

- Objekt-perspektiv:
 - Information/data
 - Tillämpning/program
 - Dator
 - Nätverk
- Process-perspektiv
 - Användande
 - Vidareförädling
 - Etc.

Riskhantering

- Komplementärt synsätt
 - Fokusskifte
- Innefattar
 - Riskanalys
 - Hot
 - Sårbarhet
 - Konsekvensanalys
 - Kostnader
- Konkret
 - Riskhanteringsplan
 - Riskhanteringsprocess

Säkerhet/risk – ekosystemet

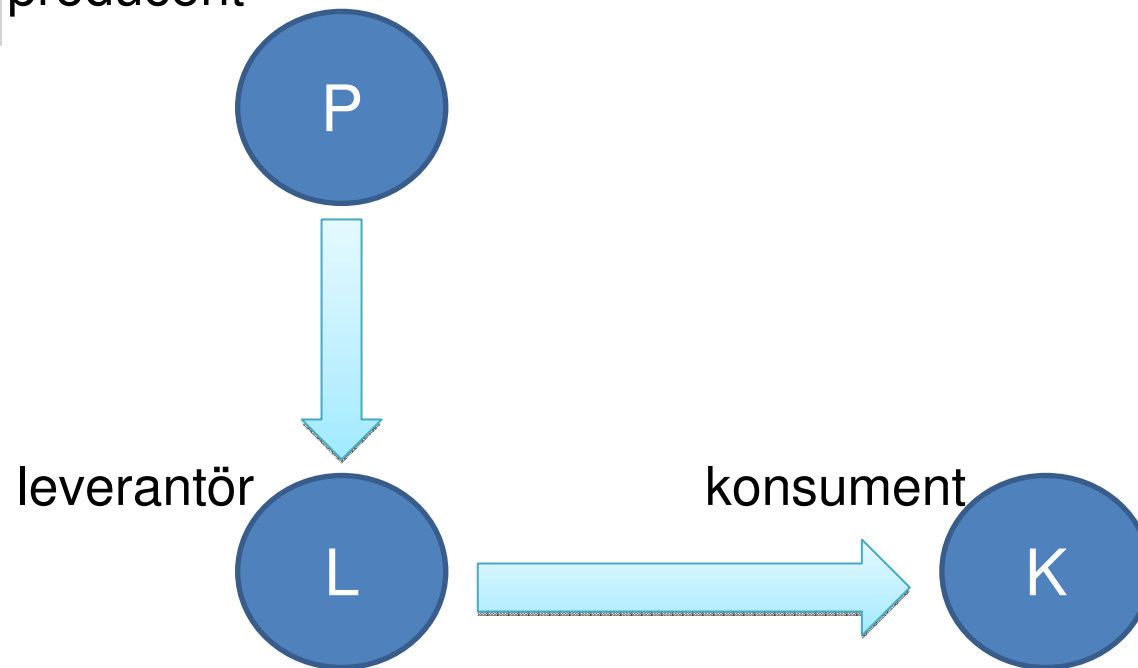
- Nätverkad värld
 - Intressenter (*stakeholders*)
 - Beroenderelationer
 - Egennytta och ömsesidig nytta
 - Säkerhet är gemensam utmaning
- Uppnå goda effekter
 - Tillit/förtroende
 - Kostnadseffektivitet

Ekosystemet – roller

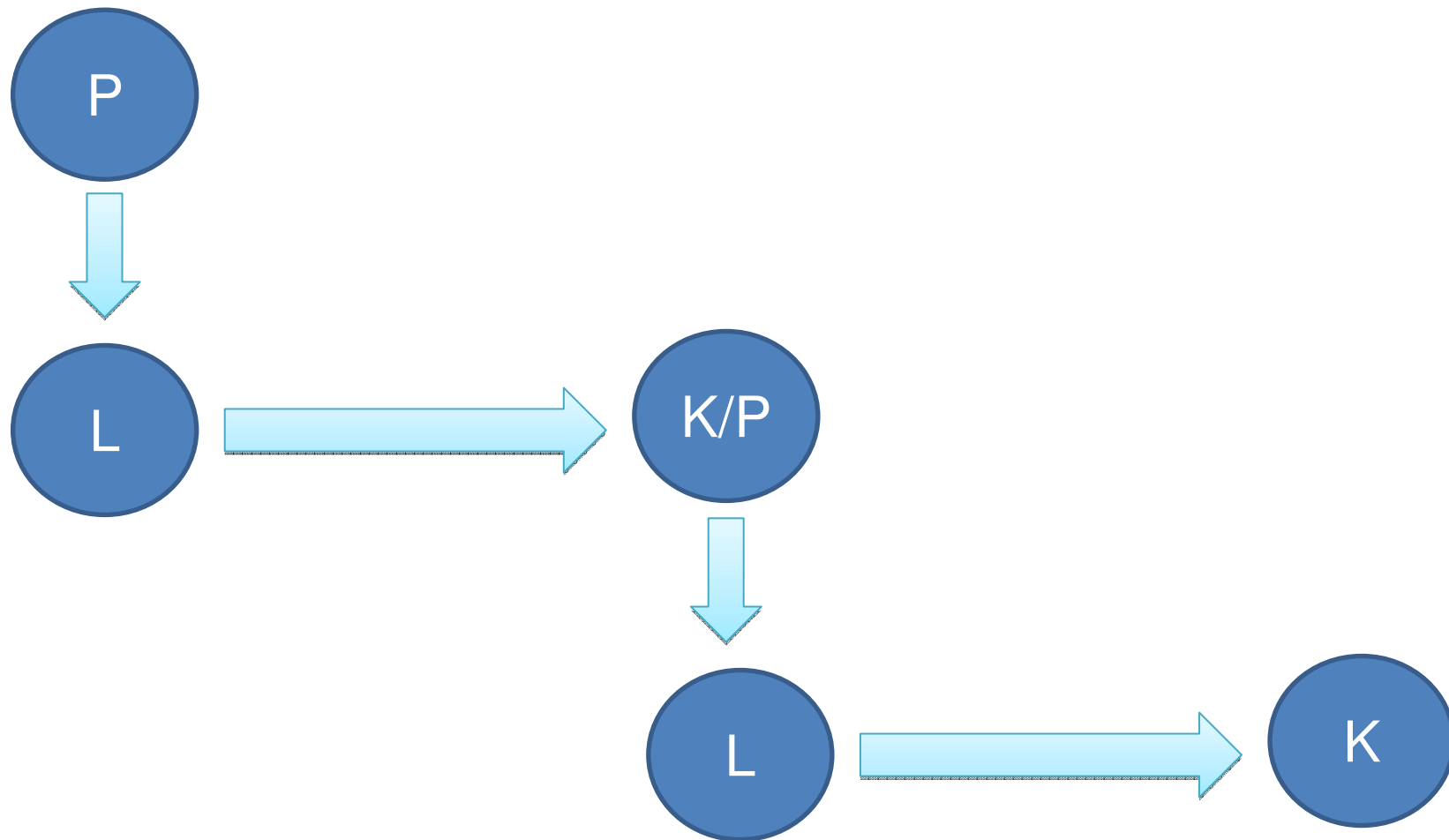
- Informationsproducenter
 - Säkerställa information ("data")
- Informationsleverantörer
 - Säkerställa informationstjänster
- Informationskonsumenter
 - Säkerställa informationsanvändning

Ekosystemet – relationer / 1

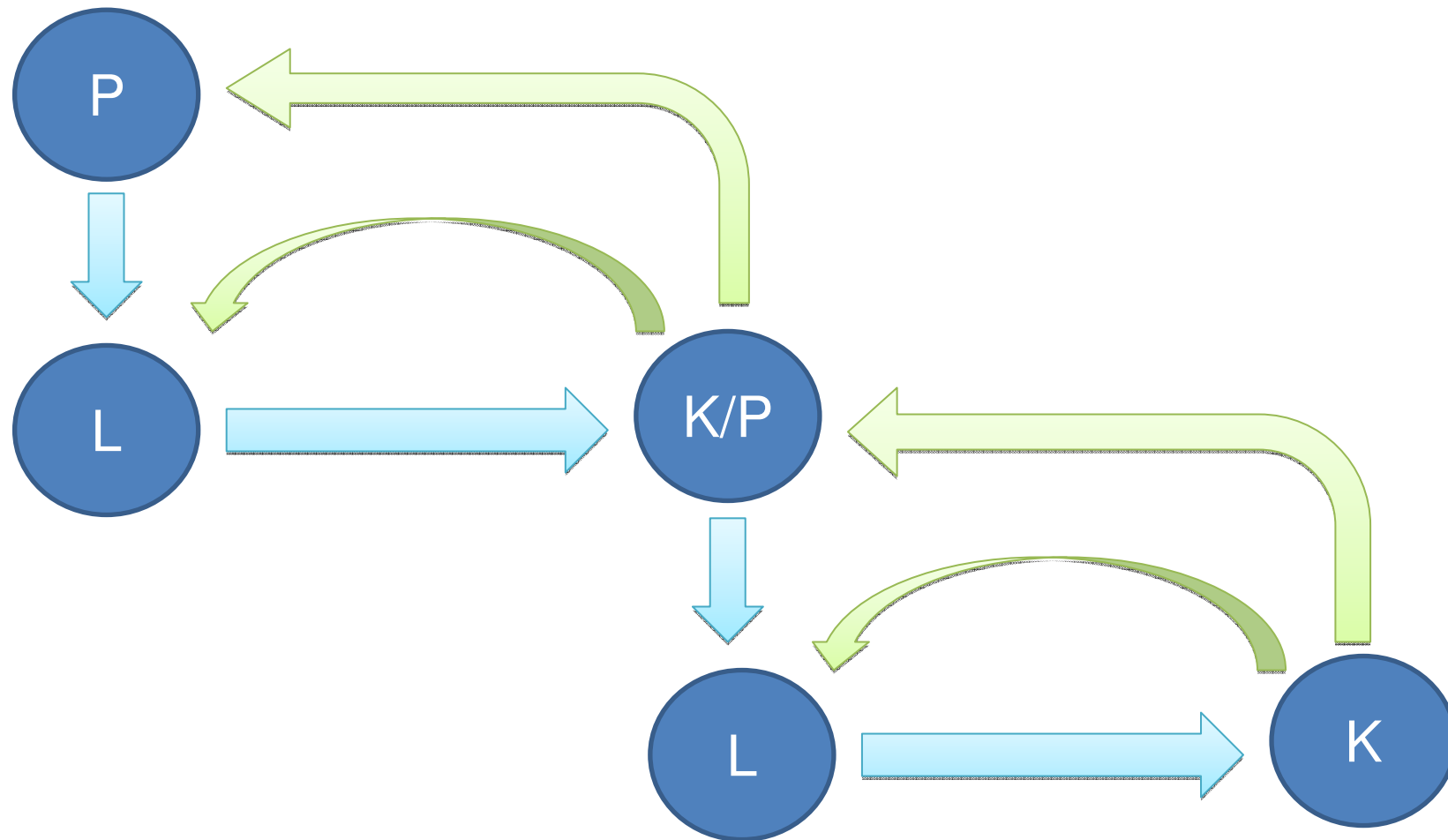
producent



Ekosystemet – relationer / 2



Återkoppling i ekosystemet



Informationssäkerhet – nu

Balansering mellan:

- Ramverk för säkerhet
- Verksamhetens kvalitets- och produktionskrav

Generellt: innefattar all verksamhetsdata

- Databaser, dokument, epost, wikis, IRC, etc.

Roll implicerar

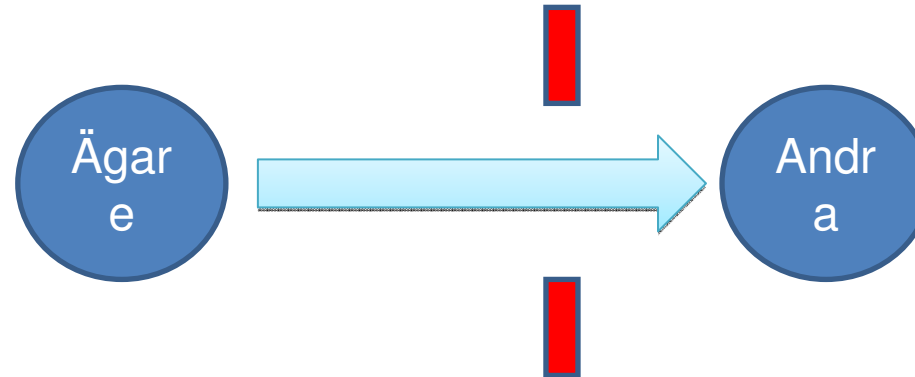
- Ansvarsområde
- Behov/önskningar/krav

Relationer implicerar

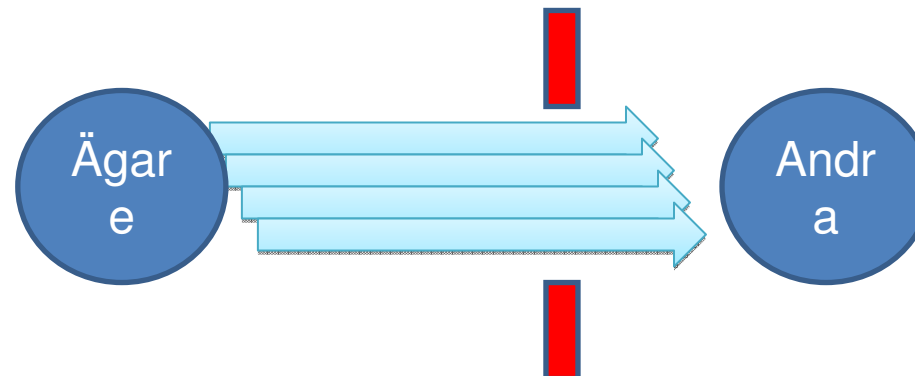
- Förväntningar

Leverantörsperspektiv / 1

- Ge tillgång till information

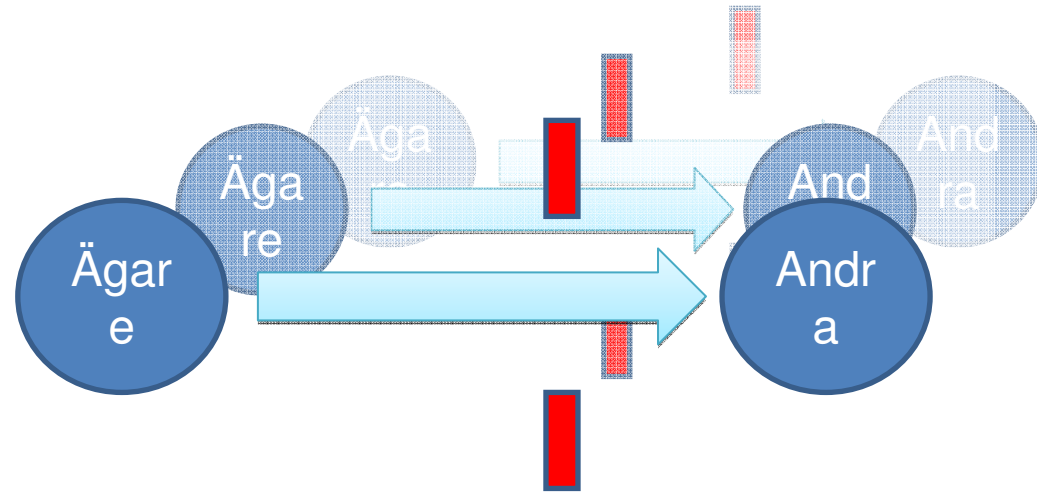


- Ge tillgång till all publicerad information

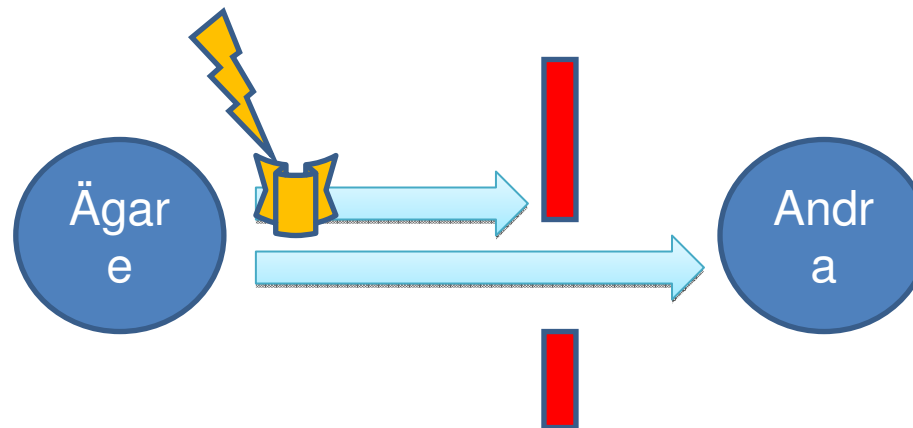


Leverantörsperspektiv / 2

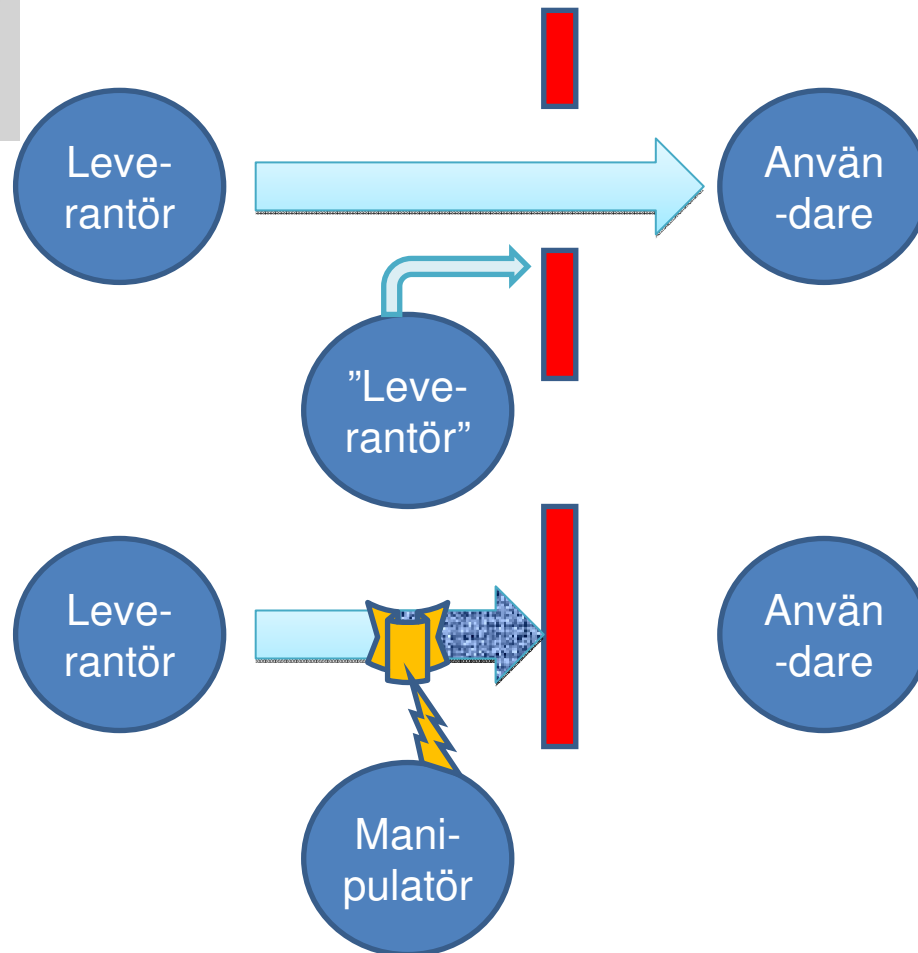
- Ge tillgång över tiden



- Ej ge tillgång till "osann" information



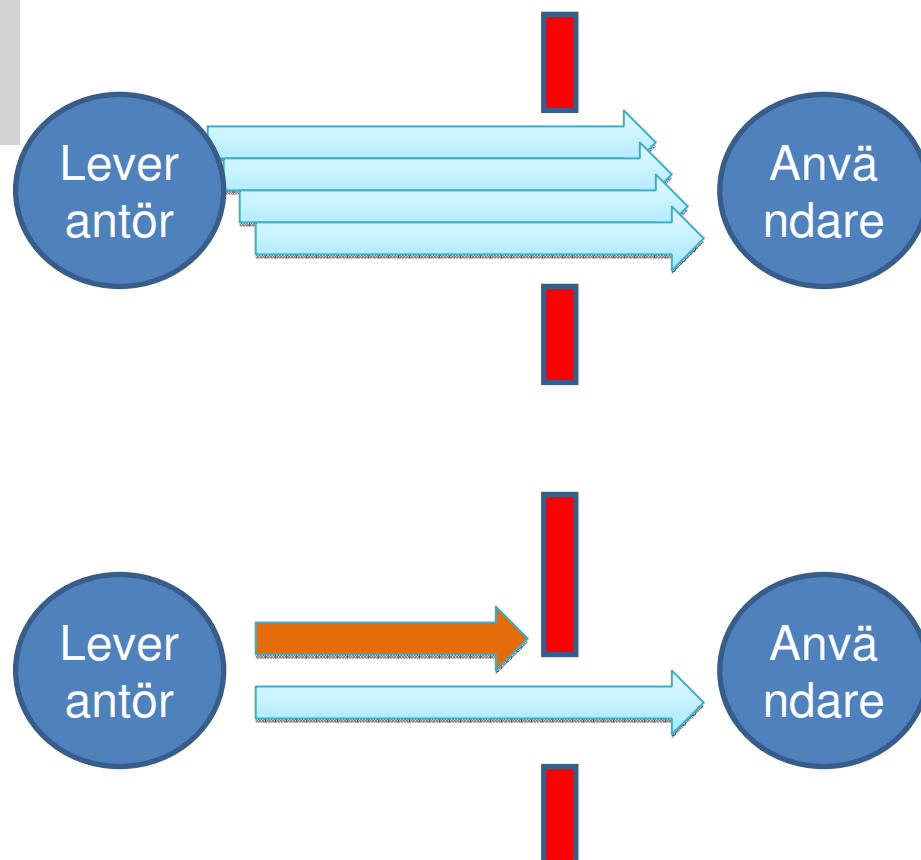
Konsumentperspektiv / 1



- Få oförfalskad information

- Ej få manipulerad information

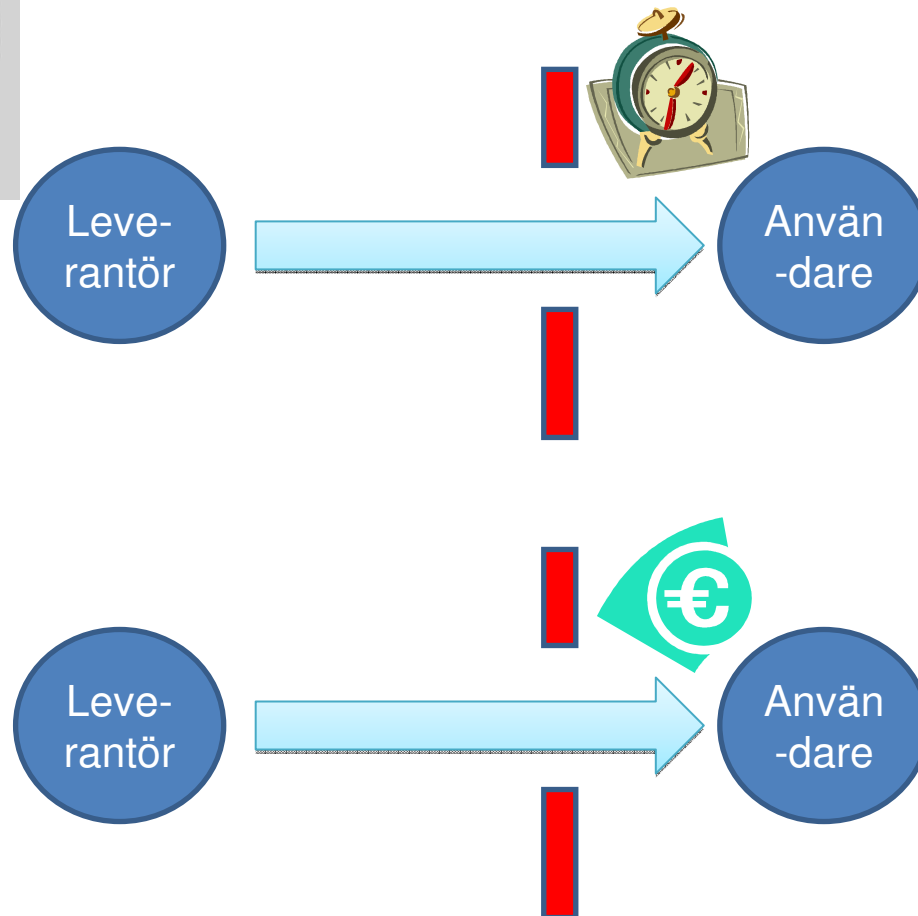
Konsumentperspektiv / 2



- Få all relevant information

- Ej få inaktuell information

Konsumentperspektiv / 3



- Få information när den behövs

- Få användbar information

Säkerhet: mål eller medel?

- Rättsinformation – ju mer användning desto bättre.
- Användbarhet är primär egenskap
 - ”Funktionell” egenskap
- Säkerhet är sekundär egenskap
 - ”Icke-funktionell” egenskap

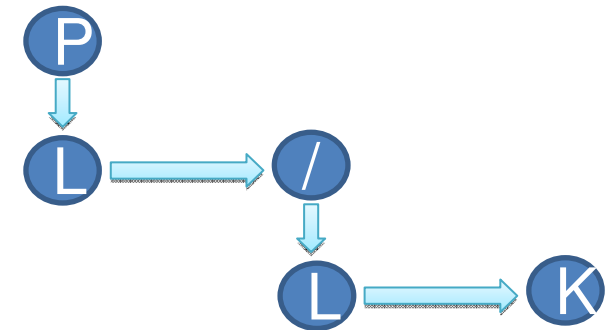
Säkerhetsaspekter - konsument

Integritet	Har data ändrats oönskat?
Tillgänglighet	Fås information inom rimlig tid?
Autentisering	Är informationen tillskriven rätt källa?
Åtkomlighet	Kan information åkommas inom rimlig tid?
Användbarhet	Kan informationen användas på avsett sätt?
Tillförlitlighet	Kan jag lita på dina mekanismer?
Säkerhetsgranskning	Är säkerheten väldefinierad och underbyggd?
Spårbarhet	Vem har gjort vad med data?
Icke-förnekelse	Hur visa vem som gett vad till vem?

Balans i försörjningskedjan

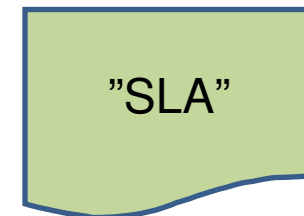
- Rättslig informationsförsörjning

- Producenter och konsumenter
- Kedjor av produktion och vidareförädling



- Balans i kedjan

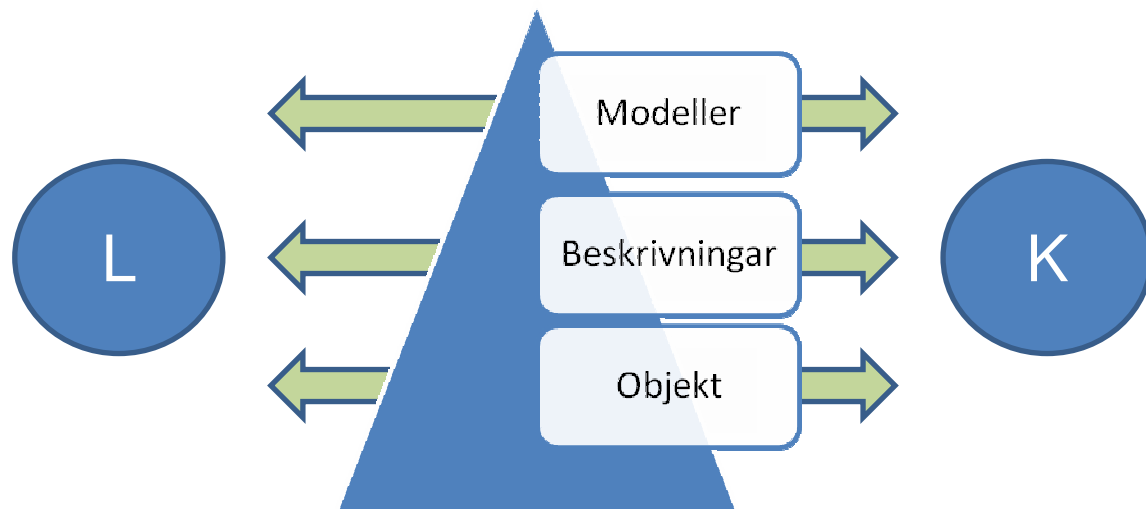
- Tydliga ömsesidiga förväntningar
- Underbyggda påståenden om att leva upp till förväntningar



Informationsförsörjningspusslet

	Dokument	Funktioner
Objekt	Innehåll	Beteende
Beskrivningar	.. av dokument ..av dokumentsamlingar	..av funktioner
Modeller	.. över beskrivningar	..över beskrivningar

Lägger grunden för
förväntningar och
åtaganden



Kvalitet i pusslet

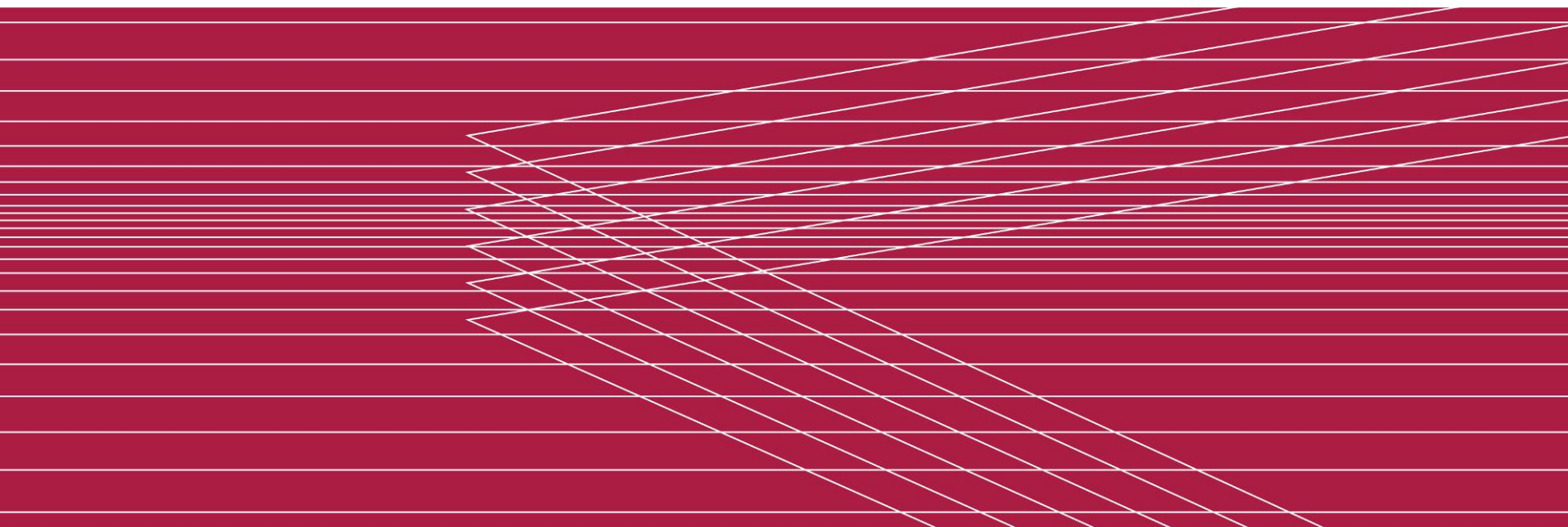
- Objekt, beskrivningar, modeller ...
 - ...måste alla kvalitetssäkras
 - Del i gränssnittet mellan aktörer i kedjan
- En föränderlig värld
 - Ökad samordning: harmoniserad hantering av bredare informationsbaser
 - Verksamhets- och rollutveckling: hantering av ständig förändringsprocess
- Kvalitet
 - inom definierade ramar
 - över förändring i tiden

Sammanfattning

- Säkerhet rör
 - Inte bara information *i form av data*
 - Även *informationstjänster*
 - Inte bara *producentens* krav
 - Egentligen mer om *konsumentens* krav
- Informationssäkerhet
 - Underbygger tillförlitlig informationsanvändning
 - Kräver definierade mål och processer

Tack för uppmärksamheten!

Statens åtagande



Hans Sundström, Verva
Konferens Rosenbad 2007-11-29

Bakgrunden för rättsinformationssystemet

- **Rättsinformationsförordning (1999:175)**
- 1 § I syfte att tillförsäkra den offentliga förvaltningen och enskilda tillgång till grundläggande rättsinformation i elektronisk form skall det finnas ett offentligt rättsinformationssystem.
- Innehållet i systemet skall vara tillgängligt på ett enhetligt sätt.

Det offentliga åtagandet över tiden

Hur har det offentliga åtagandet förändrats över tiden
när det gäller tillgång till offentlig rättsinfo

- **Tiden före systemstöd**
- **Förordning (1980:628) om rättsdatasystemet**
- **Rättsinformationsförordning (1999:175)**
- **Nationell vägdatabas i Rättsinformationssystemet**

Skrivelsen 2003/2004:168

- information och sökfunktioner presenteras på ett lättillgängligt, överskådligt och enhetligt sätt
- möjlighet att anpassa rättsinformationssystemet till användare med särskilda behov.
- exakta kopior av den tryckta versionen av samtliga författningar
- länkar mellan olika informationskällor
- informationen i systemet bör också kunna grupperas och presenteras på flera olika sätt

Vad är då statens åtagande

- rättsinformation skall finnas tillgängligt genom ett allmänt nätverk
- svara för en kontinuerlig grundservice av rättsinformation till allmänheten och den offentliga förvaltningen
- omfattar lagarnas förarbeten till domstolarnas och myndigheternas praxis och de statliga myndigheternas föreskrifter
- visst ansvar för att förädla rättsinformationen
- till största delen tillhandahållas utan avgifter.

Hur löser vi detta?

- Skapar en gemensamt system där all information om rättsinformationen finns samlad
- Pekar ut länkar mellan dokument, t.ex.
Kommittédirektiv -> Kommittébetänkande->Proposition
- Enhetlig modell för uppmärkning av dokument
- Kompletterande format till Pdf som kan ge stöd till personer med särskilda behov
- Regelverk för publicering i rättsinformationssystemet

Vad blir effekten av ett elektroniskt rättsinformationssystem?

- Kunna söka i all rättsinformation samtidigt
- Hitta dokument som står i relation till varandra och kunna navigera mellan dessa
- Uppfylla kraven i PSI-direktivet
- Skapa tjänster för personer med särskilda behov
- Säkra att rättsinformationen finns tillgänglig även efter förändringar bland myndigheterna

Vilka är vinnarna?

- Medborgare och företag
- myndigheter
- intresseorganisationer m.fl.

genom en förbättrad tillgång till rättsinformation med bättre sökbarhet

- Marknaden genom kvalitetssäkrad tillgång till rättsinformation där alla har samma tillgång till informationen

Vilka svårigheter finns i statens åtagande?

- Uppmärkning av äldre redan publicerad och kungjord rättsinformation
- Märkning som syftar till att stödja personer med särskilda behov
- Användandet av sökord

Kontaktuppgifter Rättsinformationsprojektet

<http://rinfo.lagrummet.se>

**Rättsinformationsprojektets
informationsblogg**

Projektledare Anders Carlsson, tel 0734-27 58 83

anders.carlsson@verva.se

Datakvalitet

Elektroniskt kungörande av vissa trafikföreskrifter

Jenny Forkman

Elektroniskt kungörande av vissa trafikföreskrifter

- Bakgrund
- Kort presentation av förordningen
- Ansvarsfördelningen
- Vad händer om något går snett?

Bakgrund

- Regeringens skrivelse Ett nytt offentligt rättsinformationssystem (skr. 1998/99:17)
- Trafikföreskriftsutredningens betänkande Rikstäckande Databas för Trafikföreskrifter (SOU 2003:119)
- Regeringens proposition Kungörande av vissa trafikföreskrifter (prop. 2004/05:87)
- Förordning (2007:231) om elektroniskt kungörande av vissa trafikföreskrifter
- Utredningen om elektroniskt kungörande av författningar (Ju 2007:11)
- Varför just trafikföreskrifter?

Kort presentation av förordningen

- Föreskrifter ska kungöras elektroniskt på en särskild webbplats (1 §).
- Webbplatsen ska vara tillgänglig utan avgifter för var och en (1 §).
- Beslutsmyndigheten ansvarar för att föreskriften är riktig och förs på ett säkert sätt i elektronisk form till Vägverket (3 §).
- Vägverket ansvarar för webbplatsen (9 §).
- Vägverket får, efter samråd med Verva, meddela verkställighetsföreskrifter (12 §).

Ansvarsfördelningen

Observera! De data som finns om föreskriften i databasen utgör föreskriftens autentiska version.

Ansvarsfördelningen

Beslutsmyndigheten ansvarar för att

- uppgifterna är riktiga
- uppgifterna lämnas på säkert sätt i elektronisk form
- föreskriften tilldelas löpnummer
- "trycklov"

Vägverket ansvarar för

- webbplatsen
- det system som behövs för databasens funktion
- säkerheten i systemet

Observera...

**Vägverket ska inte kontrollera
beslutsmyndig-heternas föreskrifter**

Vägverkets stödjande roll

- Informationsbrev till samtliga kommuner
- Information på hemsidan
- Handböcker
- Användarstöd per telefon
- Utbildning

Vad händer om något går snett?

- Ändringsföreskrift
- Rättelse
- ”Datateknisk rensning”

Integritetsskydd vid publicering av rättsinformation på nätet

Hans-Olof Lindblom
Datainspektionen

Integritetsskydd för personuppgifter

- Personuppgiftslagen
(1998:204)

Direkta personuppgifter:
namn, personnummer

Indirekta personuppgifter:
diarienumr, målnr etc.



Integritetsskyddet i PuL för personuppgifter

Vilka uppgifter är nödvändiga, adekvata och relevanta för ändamålet?



Integritetsskyddet i PuL för personuppgifter

Rättsligt stöd för att behandla uppgifterna?

- Känsliga personuppgifter (13-19 §§ PuL)
- Uppgifter om lagöverträdelser (21 § PuL)



Avidentifiering?

”...även uppgifter som vid en bakvägsidentifikation kan knytas till en viss person , t.ex. genom att målnummer och domstol anges, måste tas bort”.

Ostrukturerad behandling - missbruksregeln

5 a § PuL

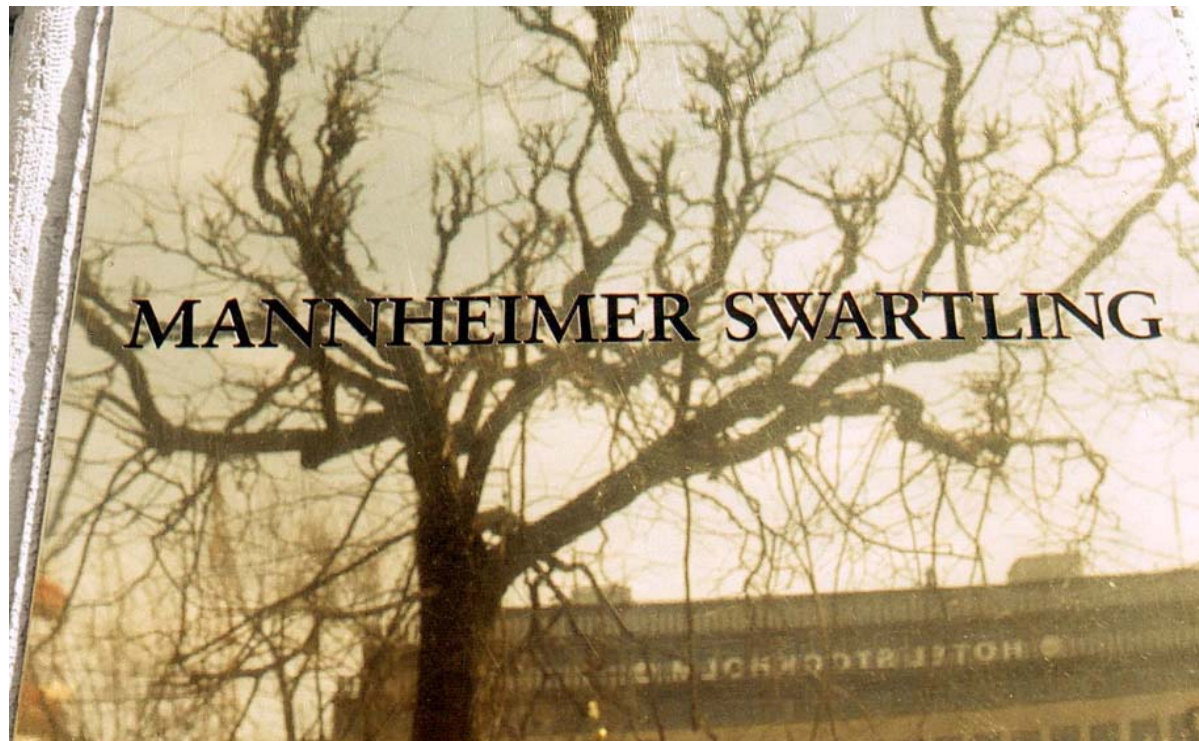
DI: Publicering av
rättsinformation som lever upp
till de villkor som är angivna i
rättsinformationsförordningen
(1999:175) kan normalt sett
inte anses kränkande.

Rättsinformations- förordningen

- Huvudregeln: Inte uppgifter som direkt kan hänföras till en fysisk person
- Aldrig personnummer

Risk för kränkning trots ”anonymisering” ?

Dom hämtad från
rättsinformationssystemet
publicerad i annat
sammenhang.



www.mannheimerswartling.se

MANNHEIMER SWARTLING

Etiska överväganden och funktionell användning av digital kommersiell rättsinformation



David Eriksson, jur kand/MSc
System development lawyer/Associate

www.mannheimerswartling.se

MANNHEIMER SWARTLING

AGENDA



1. Rättsinformation på en affärsjuridisk advokatbyrå
2. System för rättsinformation
3. Framtiden och etiska överväganden

www.mannheimerswartling.se

MANNHEIMER SWARTLING

AGENDA



- 1. Rättsinformation på en affärsjuridisk advokatbyrå**
2. System för rättsinformation
3. Framtiden och etiska överväganden

www.mannheimerswartling.se

MANNHEIMER SWARTLING

VAD ÄR
RÄTTSSINFORMATION
PÅ EN ADVOKATBYRÅ?



- Affärsjuristen rådgivande konsult i vid bemärkelse
- Information/kunskap relevant för ärendet
- Rättsinformation i vid bemärkelse

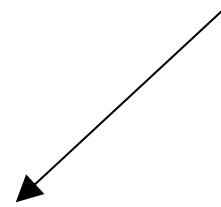
www.mannheimerswartling.se

MANNHEIMER SWARTLING

KUNSKAP PÅ EN ADVOKATBYRÅ -informationstyper



Affärsjuristens
rättskällelära



- Kunskap om juridiken/sedvanor
 - Kunskap om klienter och deras branscher
 - Metodologi och processer
 - Finansiell/affärsinformation
 - Marknadsinformation
 - Kunskap om tredje part
-
- Informationen konsumeras i hög grad digitalt

www.mannheimerswartling.se

MANNHEIMER SWARTLING

KUNSKAP/INFORMATION HOS MSA



- Interna kunskapsdatabaser
 - Kunskapsbanken, Expertsystem - Know Who, Dokumenthantering - Worksite, Bibliotekssystem, Ekonomisystem - Axapta, Intranät, mm
- Externa kunskapsdatabaser (betaltjänster ca 40-50 st + publika)
- Ett av Sverige största bibliotek
- Fysiska kunskapsbanker
- Externa/interna nyhetsbrev
- Professional development programs / Utbildning
- Mannheimer Swartling Academy
- Debriefings
- Databas med information om vänbyråer
- Strukturerade personliga möten etc
- mm mm

www.mannheimerswartling.se

MANNHEIMER SWARTLING

AGENDA



1. Rättsinformation på en affärsjuridisk advokatbyrå
- 2. System för rättsinformation**
3. Framtiden och etiska överväganden

www.mannheimerswartling.se

MANNHEIMER SWARTLING

TRENDER ADVOKATBYRÅSYSTEM



- Ärendehanteringssystem (Dokhantering, ekonomi, jäv, tidreg, CRM, KM)
- Dokumenthanteringssystem
- Portaler
- Sökmotorer
- Integration, internt och externt
- KM Outsourcing

www.mannheimerswartling.se

MANNHEIMER SWARTLING

SYSTEMEN GENERERAR ALLT MER INFORMATION



- Vi blir bättre på att tillgängliggöra information
- Vi investerar mer i att strukturera den

www.mannheimerswartling.se

MANNHEIMER SWARTLING

SYSTEMEN GENERERAR ALLT MER INFORMATION



- Vi blir bättre på att tillgängliggöra information
- Vi investerar mer i att strukturera den

IT systemen blir en del av en slags metodlära för affärsjuridiska rättskällor

www.mannheimerswartling.se

MANNHEIMER SWARTLING

http://www.mofo.com - Introduction to Answer Base - Microsoft Internet Explorer

Morrison & Foerster | AnswerBase - Microsoft Internet Explorer provided by Morrison & Foerster LLP

File Edit View Favorites Tools Help Back Forward Stop Home Search Favorites Media Print

MORRISON FOERSTER answerbase beta Advanced Search Help

DOCUMENTS PEOPLE MATTERS

NEW SEARCH

22,634 Documents

Back 1-20 Next Sort Relevance Preview ACTIONS

Search = motion to compel arbitration

Refine results by

- Document Type
- Application
- Author
- Related People
- Client
- Matter
- Portal

[USBK] Motion to Compel Arbitration .doc SF - 21072107 v.3

Simmons, Carol J. edited last on March 24, 2006
Egan, Kathleen V. authored on January 15, 2006
Client/Matter U.S. BANK NA > CHIODO, BARBARA (255-)
Type of Law Class Action - Financial Services Document Type Pleadings, Complaints, Petitions, Motions, Answers, Demurrer

Jonathan M c Seigle (SBN 186) Christopher R. c Speed (SBN 175) william e. french (SBN 287) jseigle@mofo.com ... U.S.'s Motion to Compel Arbitration ("Herman Decl.") ... U.S.'s Motion to Compel Arbitration ("Speed Decl.") ... party opposing the motion to compel arbitration must have suffered prejudice."). ... MBNA's Motion to Compel Arbitration US's Motion to Compel Arbitration

CRG - Reply brief ISO motion to compel arbitration .doc SF - 19811981 v.1

Stambaugh, Susan edited last on December 4, 2005
Stambaugh, Susan authored on May 17, 2005
Client/Matter HIGHCAMP RESEARCH GROUP, INC. > COMPEL ARBITRATION (580-1)
Document Type Pleadings, Complaints, Petitions, Motions, Answers, Demurrer
Type of Law Securities - Private Litigation

David B. Cohen (BAR NO. 235) Susan Stambaugh (BAR NO. 605) Morrison & Foerster LLP 425 Market Street San Francisco, CA 94105-2482 Telephone: (415) 268- ... Inc.'s Reply Memorandum in Support of Motion to Compel Arbitration ... support of its motion to compel arbitration ("Petition" or "Pet. to ... for the site.com's motion to

Klar Internet

http://www.mofo.com - Introduction to Answer Base - Microsoft Internet Explorer

Morrison & Foerster | AnswerBase - Microsoft Internet Explorer provided by Morrison & Foerster LLP

File Edit View Favorites Tools Help Back Forward Stop Home Search Favorites Media Print

MORRISON FOERSTER answerbase^{beta} Advanced Search Help

DOCUMENTS PEOPLE MATTERS

NEW SEARCH

100 People

Search = motion to compel arbitration

Back 1-20 Next Sort Relevance Preview ACTIONS

Refine results by

- Department
- Group
- Role
- Title
- Office
- Bar Admission
- Law School
- Notary State
- CPR
- Worked On
- Language
- HR Information



Jonathan Speed, Partner
Litigation > Bay Area Litigation
San Francisco, Floor 29
[8 or 3] + 73 + 6200; +1 (415) 268-6200; JSpeed@mofo.com
Secretary: Linda Lowery ([8 or 3] + 73 + 6500, +1 (415) 288-6500, LLowery@mofo.com)
Jonathan Speed is a litigation partner in the San Francisco office of Morrison & Foerster LLP. His practice focuses on general commercial litigation, including securities and financial services matters in federal and state courts. ...



Charles A. Bellfield, Associate
Technology Transactions > Bay Area
San Francisco, Floor 30
[8 or 3] + 73 + 6000; +1 (415) 268-6000; CBellfield@mofo.com
Secretary: Rachel M. Lu ([8 or 3] + 73 + 1000, +1 (415) 268-1000, RLu@mofo.com)
Mr. Bellfield is an associate in the Technology Transactions group in Palo Alto, CA. In 1983, he received his A.B. degree with high honors from the University of California, Berkeley, where he was a member of Phi Beta Kappa and a state finalist ...



Erec Glogowski, Associate
Litigation > New York Litigation

Internet

http://www.mofo.com - Introduction to Answer Base - Microsoft Internet Explorer

Morrison & Foerster | AnswerBase - Microsoft Internet Explorer provided by Morrison & Foerster LLP

File Edit View Favorites Tools Help Back Forward Stop Home Search Favorites Media Print

is no cognizable claim in ... Second Cause of Action Declaratory Relief Re Arbitration) [See Request for ... parties are mandated to pursue disputes through private mediation and arbitration .

Lupine- Arbitration Agmt/Isomata .doc NY - 15801580 v.1
Bosso, John M. edited last on April 12, 2005
Speed, Jonathan authored on April 10, 2005
Client/Matter TIEHACK USA, INC. > GENERAL CORPORATE (533-1)
Type of Law General Corporate **Document Type** Agreements, Contracts, Leases

tiehack arbitration AGREEMENT ... as specifically provided herein, any arbitration proceeding shall be conducted in ... of Employment Disputes of the American Arbitration Association (the AAA Rules"). Claims subject to arbitration shall include, without limitation: contract ... A neutral and impartial arbitrator shall be chosen by mutual agreement of the parties; however, if the parties are unable to agree upon an arbitrator within a reasonable period of time, then a neutral and impartial arbitrator shall be appointed in ... action in court to compel arbitration under this Agreement and to ... the parties. The arbitration provisions of this Arbitration Agreement shall be ...

Relevant Matters

Display all 19 Relevant Documents | Show all Documents for this Person

RELEVANT MATTERS ☒ display time notes

PORTOLA FINANCIAL, INC. > GENERAL LICENSING (23456-23000)

June 8, 2005	1.25 hrs	Telephone conference with A. Ross; follow up on Assignment
June 1, 2005	1.00 hrs	Review motion to compel for client
May 13, 2005	.5 hrs	Review draft agreement w/ Neff
April 11, 2001	2.50 hrs	Prepare application for motion.

METAMORPHOSIS US, INC. > DUE DILIGENCE (76767-14000)

Internet



XMLAW Enterprise Portal System Search Results

Actions

- [Advanced Search](#)
- [Search Preferences](#)
- [Add to My Links](#)
- [Alert Me](#)

Sort By

- [Author](#)
- [Date](#)
- [Relevance](#)
- [Size](#)
- [Title](#)
- [Matter](#)

Group By

- [Area](#)
- [Author](#)
- [Date](#)
- [None](#)
- [Size](#)
- [Status](#)
- [Matter](#)
- [Client](#)

[Intranet](#) [People](#)

intel

All sources

11 Results, showing items 1 - 11

[Prev](#) [Next](#)

[Refine search](#)

WorkSite - Client Library

Intel Client Folder [Marlee Olsen](#)
Matter workspaces (automatically created when a matter is opened)
and all client relationship documents and communications are in this folder.
[View Contents](#)

Proposal 632495 [Tim Schaefer](#) [6/22/2005](#)
Proposal to Intel that we hire a local survey agent in Tampa to inspect
the facility which is the target of an EPA investigation (532 KB)
[View Document](#) | [Check Out](#) | [View Profile](#) | [Print](#)

Intel 2004 Tax Strategies [Tim Schaefer](#) [4/15/2005](#)
us to act as their representative
1000 North Dearborn Street, Chicago. (425 KB)
[View Profile](#) | [Print](#)

Show Hits

Open

Edit Profile

Check In

Alert Me

Add to My Links

Details

Authors (3)

- [Joe Attorney](#) (4)
- [Andrew Jones](#) (1)
- [Edward M. Roberts](#) (1)

Matter (2)

- [6371 - Lease Renegotiation...](#) (2)
- [29393 - 2004 Tax strategi...](#) (1)

Client (2)

- [100 - Intel Corporation](#) (6)
- [Dummy](#) (0)

ACTIONS

stock option agreement

SEARCH

☐ Exact match only

4,144 Results

Refine results by

Author

Author Group

Author Office

Client

Client Industry

Technology (807)

Services (625)

Financial (400)

Healthcare (203)

Consumer Cyclical (182)

Capital Goods (155)

Transportation (81)

Consumer/Non-Cyclical (78)

Energy (70)

Utilities (39)

☒ Preview

Sort by: Relevance

Sort order: Descending

Back 1-10 Next

1. **Stock Option Agreement - Websense Inc. 6725**

Author: David Baudemont

Office: Washington D.C.

Client: Websense Inc.

... WEBSense, INC.

STOCK OPTION AGREEMENT

RECITALS ... by reason of any stock split, stock dividend, recapitalization, combination of ... pursuant to that certain option (the "Option") granted to me under ... AGREEMENT shall mean this Stock Option Agreement. B. BOARD shall ... Notice of Grant of Stock Option accompanying the Agreement, pursuant to ...

Group: Corporate

Industry: Technology > Software & Programming

2. **Stock Option Agreement - China Broadband Corp. 545**

Author: Caroline Adderson

Office: Tokyo

Client: China Broadband Corp.

... PLAN

STOCK OPTION AGREEMENT

is otherwise ... defined meanings in this Stock Option Agreement. I. NOTICE OF ... Type of Option: ... Incentive Stock Option

statutory ...

as an Incentive Stock Option ("ISO"), this Option is intended ... PLAN") and the Stock Option Agreement dated ..., (the "OPTION AGREEMENT"). ...

Group: Corporate

Industry: Services > Communications Services

3. **Stock Option Agreement - Sohu.com Inc. 5766**

Author: Paul McAulay on Dec 5, 1999

Office: Berlin

Client: Sohu.com Inc.

... INC.

In-Qualified Stock Option Stock Option Agreement dated as of ... time for stock splits, reverse stock splits, stock dividends and

specifications ... hereby elect to exercise the stock option granted to me on ..., ... I understand that the stock option that I

electing ... not qualified as an "incentive stock option" under Section 422 of ...

Group: Finance

Industry: Technology > Computer Services

4. **1998 Stock Option Plan - Stock Option Agreement - eGroups Inc. 1312**

Author: David Homel

Office: New York

Client: eGroups Inc.

... INC.

1998 STOCK OPTION PLAN

STOCK OPTION AGREEMENT

1. GRANT ... If designated an Incentive Stock Option, this Option is intended to ... a) EXERCISE OF INCENTIVE STOCK OPTION. If this Option qualifies as ... b) EXERCISE OF NONSTATUTORY STOCK OPTION. If this Option does not ...

Group: Legal

5. **1995 Stock Option Plan 1150**

Author: Caroline Lawrence on May 19, 1995

Office: Berlin

Client: Exodus Communications Inc.

... INC.

... of a written stock option exercise agreement (the "Exercise Agreement") ... The Plan and the Stock Option Exercise Agreement

attached as ... the Plan and the Stock Option Exercise Agreement constitute the entire ...

Group: Legal

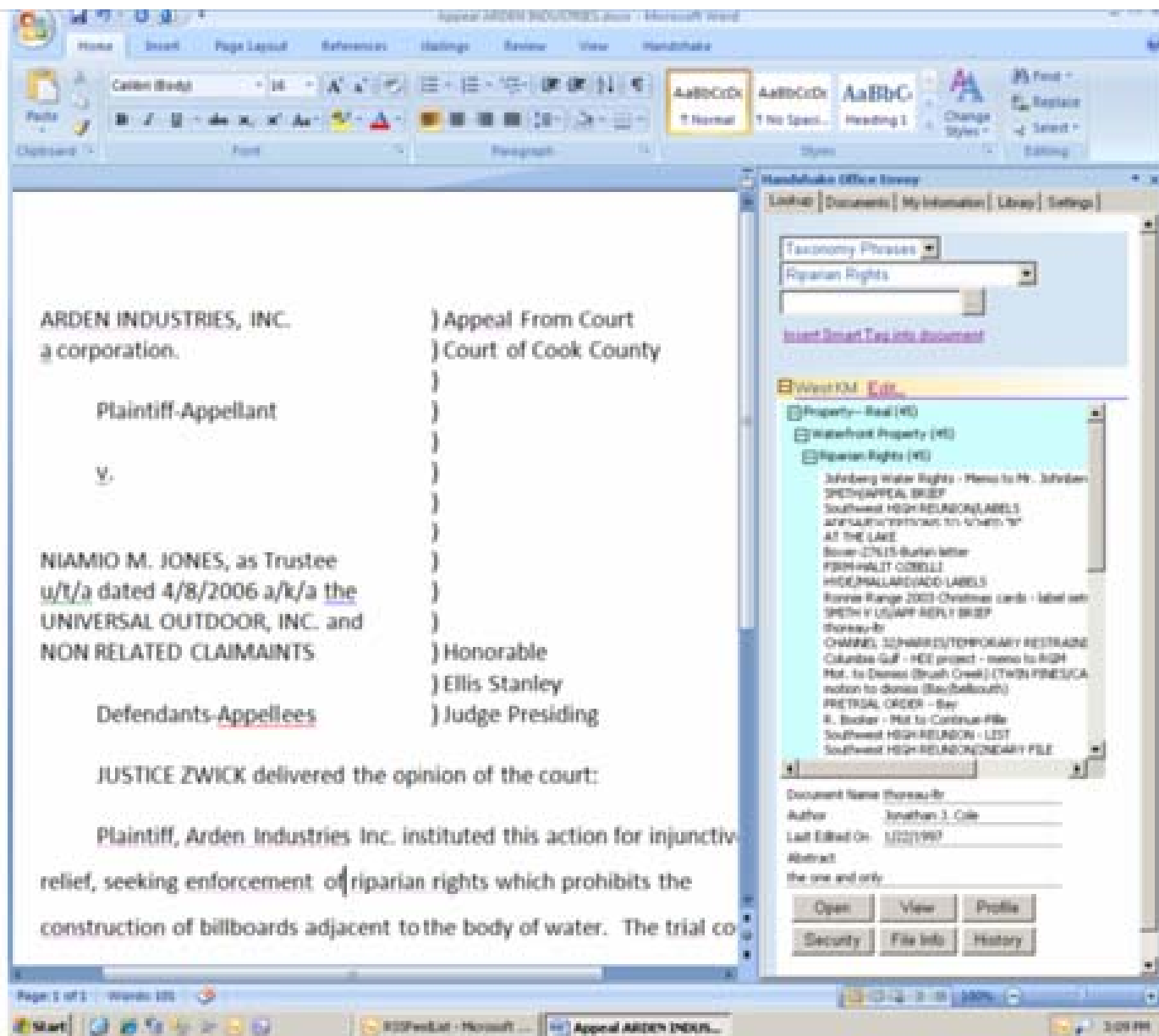
Industry: Services > Communications Services

COMMUNICATIONS, INC.

STOCK OPTION EXERCISE AGREEMENT

This Exercise

MANNHEIMER SWARTLING



Handshake Office Envoy recognizes terms as they are entered in the document and matches them against taxonomy categories in West KM™. Users then have the option to explore documents which fall into these categories.

Exempel sökning i advokatbyrås dokumentsystem/kunskapsbaser



- A handlägger ärende 1: Leasing av fritöser och spisar för McDonalds
- B handlägger ärende 2: Leasing av läskmaskiner hos MAX
- B söker med “leasing”, “läsk” och “restaurang”
- Även om ordet “restaurang” inte finns i McDonalds-avtalen ges ändå träff

...MEN VAD FÖRSÖKER DU
SÄGA MED DETTA?



www.mannheimerswartling.se

MANNHEIMER SWARTLING

...MEN VAD FÖRSÖKER DU
SÄGA MED DETTA?



- information relevant för våra ärenden kan komma/existera i många former och behöver struktureras och tillgängliggöras med hjälp av IT-system

www.mannheimerswartling.se

MANNHEIMER SWARTLING

...MEN VAD FÖRSÖKER DU
SÄGA MED DETTA?



- information relevant för våra ärenden kan komma/existera i många former och behöver struktureras och tillgängliggöras med hjälp av IT-system
- IT-systemen måste också bli smartare. Läras upp.

www.mannheimerswartling.se

MANNHEIMER SWARTLING

...MEN VAD FÖRSÖKER DU
SÄGA MED DETTA?



- information relevant för våra ärenden kan komma/existera i många former och behöver struktureras och tillgängliggöras med hjälp av IT-system
- IT-systemen måste också bli smartare. Läras upp.
- Rättsinformatiken och juridiska metodläran måste hjälpa till

www.mannheimerswartling.se

MANNHEIMER SWARTLING

...MEN VAD FÖRSÖKER DU
SÄGA MED DETTA?



- information relevant för våra ärenden kan komma/existera i många former och behöver struktureras och tillgängliggöras med hjälp av IT-system
- IT systemen måste också bli smartare. Läras upp.
- Rättsinformatiken och juridiska metodläran måste hjälpa till
- Vem skriver algoritmerna? Vem skapar tekniken och gör den smart?

www.mannheimerswartling.se

MANNHEIMER SWARTLING

Juridisk-semantic algoritmer?



- Immaterialrättsligt verk
- Statligt verk
- Livsverk
- Träningsvärk

Juridisk-semantiska algoritmer?



- Immaterialrättsligt verk
 - Statligt verk
 - Livsverk
 - Träningsvärk
-
- Juridisk-semantiska algoritmernas användning i sökmotorer och IT-system

AGENDA



1. Rättsinformation på en affärsjuridisk advokatbyrå
2. System för rättsinformation
- 3. Framtiden och etiska överväganden**

www.mannheimerswartling.se

MANNHEIMER SWARTLING

FRAMTID OCH ÖVERVÄGANDEN



- Hur ser framtiden ut för advokatbyråernas (rätts)informationssystem och vilka (etiska) överväganden finns?

www.mannheimerswartling.se

MANNHEIMER SWARTLING

FRAMTID



- Informationsanalysverktyg
- IT-systemen del av rättskälleläran
- Integration
- Nya produkter/marknader
- Nya roller
- Juridiska informationsalgoritmer
- Öppenhet och informationsdelning viktig
- Standarder

www.mannheimerswartling.se

MANNHEIMER SWARTLING

ÖVERVÄGANDEN



- Informationsdelning
- IT-systemen del av rättskälleläran, därför måste de utvecklas enligt dess principer
- Säkerhet och datakvalitet
- Tillgänglighet
- Sekretess
- Snokande
- Spårbarhet
- Intressekonflikter
- Chinese Walls



www.mannheimerswartling.se
MANNHEIMER SWARTLING

Spårbarhet (i rettsinformationsforsörjningen) – presentasjon for Föreningen Rättsinformation, Stockholm 29. november 2007

*Rolf Riisnæs, advokat dr. juris, advokatfirmaet Wikborg Rein (Oslo)*¹

1. Definisjon og problemstilling

Jeg er invitert til å si noen ord om sporbarhet. Med sporbarhet mener jeg i denne sammenheng muligheten for å fastlegge for eksempel:

- *hvem* som har opprettet en tekst eller utstedt et dokument, eller
- på hvilket *tidspunkt* eller
- i hvilken *sammenheng* et dokument er opprettet.

Spørsmålet er:

- *hvilke* krav som stilles til sporbarhet for normerende rettslige tekster,
- *hvor* eller hvordan slike krav er *forankret* og
- *hvordan* de eventuelt kan oppfylles.

Eksemplene jeg benytter er hentet fra norsk rett, men prinsippene er nok allmenne.

2. Om normerende tekster

De normerende tekster kan grovt sett deles i to: generelle og individuelle. Vi kjenner skillet typisk i forholdet mellom lov/forskrift på den ene siden og enkeltvedtak/dom på den annen side.

Det som preger begge grupper, er at de er underlagt *særlige form- og kompetanseregler*, både når det gjelder:

- deres *tilblivelse*, og når det gjelder
- *hvordan resultatet skal formidles* til, eller gjøres tilgjengelig for, de det angår.

¹ Wikborg Rein er blant Norges største advokatfirmaer og sysselsetter i dag ca 170 advokater. Rolf Riisnæs arbeider særlig med spørsmål knyttet til elektronisk forvaltning, informasjonssikkerhet, personvern og IKT-kontrakter. Han ble dr. juris i 2006 på sin avhandling *Digitale sertifikater og sertifikattjenester – roller, oppgaver og ansvar*, Fagbokforlaget 2007, ISBN 978-82-450-0589-9. E-post: rri@wr.no. (Referanser til flere publikasjoner på siste side.)

Dette er typisk regler om *hvem* som kan treffe vedtak eller fastlegge generelle regler av en spesiell type og *hvordan* man skal gå frem i forbindelse med at vedtak skal treffes eller regler skal fastsettes. I tillegg vil det gjerne finnes krav til *distribusjon* av vedtaket eller til *publisering* og tilgjengeliggjøring av reglene.

Vi har for eksempel Grunnlovens bestemmelser om hvordan det norske Storting går frem når de gir lover, og om Kongens sanksjon. Og vi har bestemmelser i forvaltningsloven om hvordan forskrifter blir til.

2.1 Generelle regler

Generelle regler publiseres typisk i en dertil egnet offentlig trykksak. I Norge i Norsk Lovtidend. Dette er bestemt ved egen lov. Det samme er for forskrifter bestemt i forvaltningsloven. Og forskriftene kan ikke påberopes overfor dem den før den er publisert.

Lovtidend trykkes på grunnlag av den elektroniske databasen hos stiftelsen Lovdata. Slik har man nå sikret at det som er fritt tilgjengelig elektronisk er identisk med det som er trykket i den offisielle publikasjonen.

Disse rammer omkring tilblivelse og tilgjengeliggjøring av normerende tekster skaper tradisjonelt forholdsvis stor grad av både forutberegnelighet og sporbarhet knyttet til tekstens grunnlag og innhold.

2.2 Individuelle vedtak

Individuelle vedtak følger naturligvis en annen rute. Individuelle vedtak formidles tradisjonelt til den det gjelder i form av *papirdokument* som etter sitt eget innhold, for eksempel fordi det er benyttet et lett gjenkjennelig brevark, tydelig stammer fra vedkommende offentlige myndighet. Og det fremsendes til den det gjelder ved hjelp av postvesenet som kan bidra til å skape sannsynlighet for den tidsmessige sammenhengen mellom tidspunktet da vedtaket ble truffet, eller i alle fall formidlet, og det tidspunkt da det ble mottatt.

Vanligvis vil det derfor være mulig, uten for store problemer, å fastlegge entydig hvilke normerende tekster som er vedtatt, av hvem de er vedtatt og på hvilket tidspunkt de kan gjøres gjeldende.

3. Publisering i elektronisk form

Utfordringene blir større når tekstene gjøres tilgjengelige i elektronisk form og spres ved hjelp av elektronisk kommunikasjon. Jeg vil belyse noen av de utfordringer dette reiser med noen eksempler på hvordan vi har håndtert dette i Norge.

Utfordringene gjelder, slik jeg ser det, særlig for individuelt normerende tekster, eller enkeltvedtak som det kalles i Norge. Det vil si avgjørelser som er bestemmende for enkeltpersoners rettigheter eller plikter. Jeg kommer straks tilbake til det.

Men også for generelle vedtak, reiser kommunikasjonsformen visse nye utfordringer.

For eksempel vil muligheten for publisering på de enkelte forvaltningsorganers egne nettsteder skape et press mot troverdigheten til materialet, i forhold til om de enkelte kopier er oppdaterte. Har man funnet siste versjon av den aktuelle teksten? Er det kommet endringer eller relevante tillegg som ikke fremgår her?

Et praktisk og meget uheldig eksempel er den norske eForvaltningsforskriften. Forskrift om elektronisk kommunikasjon med og i offentlig forvaltning. Forskriften nedfeller rammebetingelsene for *forvaltningens bruk av elektronisk kommunikasjon med borgerne og med hverandre*, også i forbindelse med prosesser som ender i normerende vedtak.

Forskriften forvaltes av Fornyings- og administrasjonsdepartementet, tidligere Moderniseringsdepartementet. Forskriften var tilgjengelig i fulltekst på departementets nettsider.

Forskriften, som først ble vedtatt i 2002, hadde en såkalt solnedgangsbestemmelse, som innebar at den ville opphøre å gjelde etter to år dersom den ikke ble fornyet. Som følge av dette ble forskriften grundig evaluert i god tid før den utløp. Det ble konstatert at forskriften var lite kjent og at den var til dels vanskelig å forstå, men at den innholdsmessig måtte videreføres. En revidert forskrift

ble derfor utarbeidet og den trådte i kraft 1. juli 2004, den dagen den opprinnelige forskriften etter sin ordlyd opphørte.

I oktober 2004, fire måneder etter at den nye forskriften ble vedtatt, var det fortsatt den gamle forskriften som lå ute på det ansvarlige departementets hjemmesider. Jeg oppdaget det ved en tilfeldighet, fordi jeg fant en utskrift av den gamle forskriften i skriveren på universitetet. Jeg gjorde vedkommende som hadde skrevet den ut oppmerksom på at det var kommet en ny forskrift, og han uttrykte bestyrtet at: ”Jammen, jeg har jo skrevet den ut fra departementets hjemmeside!” Dette er nok et tegn på at forskriften på det aktuelle tidspunkt var lite kjent. Men at departementet med ansvar for it-politikken ikke var i stand til å holde oppdatert sine egne regler om bruk av elektronisk kommunikasjon er et grelt eksempel.

Eksempelet synliggjør utfordringen med oppdatering av distribuerte tekster. I dette tilfellet var problemet forsterket ved at det var regelverksforvalter selv som ikke var oppdatert. Hadde det vært et underordnet organ, eller en annen nettside, ville en bruker hatt større foranledning til å kontrollere om det var skjedd endringer siden dokumentet ble publisert. Men når *kilden* var selve dokumentets utsteder, eier, forvalter, er det mindre nærliggende å utføre videre kontroller.

I dag lenker de fleste offentlige nettsteder, i alle fall de statlige organer, direkte til forskriftsdatabasen i Lovdata, som inneholder de til enhver tid gjeldende tekster. Alle norske bestemmelser på lov og forskriftsnivå skal nå via Lovdata for publisering.

Det innebærer at hvis en forskrift er opphevet uten at lenken til Lovdata er oppdatert vil brukeren bli oppmerksom på det. Det er også mulig å knytte lenken til hjemmelsbestemmelsen, slik at eventuelle nye forskrifter med hjemmel i samme lov fanges opp automatisk.

Når det gjelder individuelle vedtak er utfordringene større.

De alminnelige regler vi har om formidling av individuelle avgjørelser, enkeltvedtak, bygger på en del ikke uttalte forutsetninger om hvordan formidling skjer.

Forvaltningsloven stiller krav om at underretning om enkeltvedtak skal skje skriftlig til den vedtaket gjelder. Skriftlighetskravet i

forvaltningsloven fra 1967 ble nok opprinnelig oppfattet som *motsetningen til muntlighet*. Og det *praktiske* alternativet for et skriftlig vedtak var i form av et papirdokument.

Når kravet var begrenset til skriftlighet bygde det ganske sikkert også på noen andre forutsetninger – som ikke var uttalt i loven. Blant annet en forutsetning om at vi har et rimelig velfungerende postvesen, som faktisk bringer de fleste brev frem til adressaten innen rimelig tid. Og en forutsetning om at *i alle fall de fleste* personer faktisk sjekker postkassen sin jevnlig, og at de stort sett leser brev de mottar fra det offentlige. Slike forutsetninger kan vi ikke uten videre operere med, i alle fall ikke foreløpig, når det benyttes elektronisk kommunikasjon.

Dette kan utløse krav til sporbarhet, bl.a. i forhold til om en handling (vedtak) har kommet frem til rette vedkommende, og i forhold til hvordan en handling kan dokumenteres over tid, eller overfor tredjepart.

I det følgende vil jeg knytte enkelte merknader til noen av de utfordringer og løsninger vi har knyttet til:

- Formidling av vedtak
- Herunder bruk av virksomhetssertifikater
- Oppbevaring av elektronisk signert materiale
- Innsyn i og utlevering av elektronisk signert materiale

Alle disse forhold er behandlet i den norske eForvaltningsforskriften.²

4. Formidling av vedtak

For formidling av vedtak gjelder som nevnt et skriftlighetskrav. Skriftlighetskravet i forvaltningsloven er nå definert slik at det også omfatter bruk av ”elektronisk melding når informasjonen i denne er tilgjengelig også for ettertiden”. Det er også åpnet for at formidling av vedtak kan skje i elektronisk form dersom den vedtaket retter seg mot *uttrykkelig har godtatt dette* og oppgitt den elektroniske adressen som varsel om vedtak skal sendes til (forvaltningsloven § 27).³

² Se <http://www.lovdata.no/for/sf/fa/fa-20040625-0988.html>

³ Se <http://www.lovdata.no/all/tl-19670210-000-005.html#27>

eForvaltningsforskriften (§ 8) inneholder mer detaljerte regler om hvordan formidling av vedtak skal foregå. Stikkordsmessig er det særlig tre forhold forskriften dekker. Det er krav til:

- 1) at bare rette vedkommende får tilgang til vedtaket,
- 2) at rette vedkommende har reelle muligheter til å gjøre seg kjent med vedtaket, og
- 3) at vedkommende har mulighet for å sikre seg at det faktisk er forvaltningsorganet som står bak vedtaket.

Bakgrunnen er at forvaltningens vedtak forutsetningsvis har betydning for våre rettigheter og plikter, og at det derfor ikke er likegyldig om vi blir kjent med dem eller ikke. Forskriften har derfor bygget inn mekanismer, bl.a. krav til sporbarhet, som skal sikre at ingen lider rettstap som følge av at vedtak ikke kommer frem, eller at den det gjelder av en eller annen grunn ikke blir oppmerksom på vedtaket eller ikke er i stand til å få tak i det.

4.1 Mulighet til å skaffe seg tilgang

Den første hovedtypen av utfordringer er altså knyttet til at rette vedkommende faktisk har *reell mulighet* til å skaffe seg kunnskap om vedtaket, og at det finnes reserveløsninger som sikrer at ikke vedkommende lider rettstap som følge av at han ikke blir kjent med det, som følge av omstendigheter han ikke selv rår over.

Den norske ordningen er derfor at underretning om vedtak kan skje i elektronisk form hvis den vedtaket retter seg mot uttrykkelig har godtatt det og oppgitt den elektroniske adressen som varsel om vedtaket skal sendes til. Dette kan være en e-postadresse, et mobiltelefonnummer for mottak av SMS, eller i prinsippet en nettbankkonto eller en personlig hjemmeside på en offentlig portal, det som i Norge går under navnet Min Side.

Poenget er at vedkommende varsles om at vedtak er fattet på en måte han selv har valgt, på en adresse vedkommende vanligvis benytter. Varsel skal inneholde opplysninger om hvordan mottakeren kan skaffe seg tilgang til vedtaket. Vanligvis i form av en lenke til en offentlig portal der vedtaket er lagt ut, og gjøres tilgjengelig for mottakeren når mottakeren autentiserer seg overfor portalen.

På denne måten sikres at bare rette vedkommende får tilgang til vedtaket.

4.2 Taushetsplikt

Forvaltningens vedtak vil i mange tilfeller være underlagt taushetsplikt, eller være knyttet til behandling av personopplysninger. Forskriften stiller derfor krav om at forvaltningsorganet skal sikre at bare rette vedkommende kan skaffe seg tilgang til vedtaket, og lagre data som dokumenterer at det var rette vedkommende som skaffet seg tilgang til vedtaket.

4.3 Reserveløsning

Men ordningen har også en annen hovedfunksjon. Forvaltningsorganet skal nemlig innrette seg slik at de kan kontrollere og dokumentere at mottakeren har skaffet seg tilgang til vedtaket, og om så ikke har skjedd innen en frist på syv dager, sende ut vedtaket på tradisjonell måte som om det ikke var gitt samtykke til bruk av elektronisk kommunikasjon.

På denne måten, ved å registrere opplysninger om tilgang (sporing), forsøker man å ivareta interessene til den som *har* samtykket i underretning i elektronisk form, men som av en eller annen grunn ikke kan eller vil benytte de aktuelle tjenestene.

4.4 Autentisering av forvaltningsorganet

Det andre spørsmålet er hvorledes den vedtaket retter seg mot skal kunne vite at det er forvaltningsorganet som er avsender eller som står bak vedtaket.

Det er tradisjon for å sende ut vedtak skriftlig, på forvaltningsorganets brevark, i konvolutter som identifiserer forvaltningsorganet. Og en bemyndiget person vil gjerne ha underskrevet vedtaket. Mottakeren vil imidlertid sjelden kunne verifisere underskriften, eller at det er rette person som har underskrevet. I praksis må mottakeren stole på at når vedtaket ser ut til å komme fra forvaltningsorganet, så gjør det det, og stole på at

forvaltningsorganet har rutiner som sikrer at rette vedkommende har undertegnet og ekspedert vedtaket.

Det mottakeren i praksis har behov for å få bekreftet er at forvaltningsorganet står bak vedtaket, ikke den enkelte saksbehandler. Ettersom det siste er noe mottakeren uansett ikke kan få verifisert, må han sette sin lit til at de interne rutinene sikrer at prosedyrene er fulgt.

Derfor stiller eForvaltningsforskriften ingen krav om at saksbehandler eller bemyndiget skal signere vedtak elektronisk. Derimot forutsetter forskriften at det benyttes virksomhetssertifikater i forbindelse med underretning om vedtak i elektronisk form (eForvaltningsforskriften § 14).

4.5 Virksomhetssertifikater

Et virksomhetssertifikat er et sertifikat som identifiserer en virksomhet, i dette tilfellet et forvaltningsorgan, som inneholder av sertifikatet, i stedet for en fysisk person. Personen ville i så fall vært kalt undertegner i esignatordirektivets terminologi.

Virksomhetssertifikater kan benyttes enten for signering av vedtak på vegne av forvaltningsorganet. Eller om man vil, påføring av et digitalt stempel på vegne av organet. Jeg mener terminologien er underordnet her. Poenget er at det benyttes prosesser som etablerer en kopling mellom den *tekst* som representerer vedtaket og det *forvaltningsorgan* som står bak vedtaket. Alternativt kan virksomhetssertifikatet benyttes for å autentisere forvaltningsorganet som kilde i forbindelse med at den vedtaket retter seg mot laster det ned, eller på annen måte skaffer seg tilgang til det fra forvaltningsorganets nettsted. Typisk i form av et serversertifikat som autentiserer forvaltningsorganet som inneholder at det nettstedet vedtaket gjøres tilgjengelig fra. Dette kan gjøres uten at man benytter signeringsteknologi knyttet til selve vedtaket.

5. Oppbevaring og utlevering av vedtak

I forlengelsen av elektronisk formidling av vedtak får forvaltningen også en annen oppgave. Nemlig å holde relevante opplysninger og dokumenter tilgjengelig også for partene over tid (eForvaltningsforskriften §§ 10 og 26).

Vi har tradisjon for både alminnelig innsynsrett og partsinnsyn, men perspektivet er i eforvaltningsforskriften utvidet til at forvaltningsorganet skal oppbevare materiale også på vegne av den vedtaket gjelder. På en måte kan vi snakke om at forvaltningsorganet også skal tilby å forvalte partenes private arkiv.

Dette skyldes bl.a. at det er de færreste av oss som er i stand til, på en forsvarlig måte, å forvalte elektroniske dokumenter over lang tid. Hvor mange av oss har for eksempel full oversikt over egen e-post og elektroniske dokumenter mer enn et par år tilbake.

Og det er ikke alle elektroniske dokumenter som lar seg skrive ut hvis de på en troverdig måte skal kunne formidles videre.

Dette siste har foranlediget et krav om at forvaltningsorganet, på begjæring, skal kunne utlevere signerte dokumenter sammen med de sertifikater og andre opplysninger som er nødvendige for å verifisere dem, eller på annen måte kunne tilby en bekreftet kopi av det aktuelle dokumentet.

Dette kan være aktuelt dersom den dokumentet direkte gjelder har behov for å påberope det overfor en tredjepart, for eksempel en domstol, eller overfor en nabo eller et annet forvaltningsorgan.

I denne sammenheng sikres sporbarhet ved at dokumentene hele tiden gjøres tilgjengelig fra forvaltningens eget system, og ved at forvaltningen må vedlikeholde verifiserbarheten av elektroniske signaturer, eller på annen måte tilby en bekreftet kopi av dokumentet.

6. Arkiv

Kravene henger sammen med krav til forvaltningens egen oppbevaring av dokumenter som er signert med elektronisk signatur.

Det er betydelige utfordringer knyttet til oppbevaring av elektronisk signert materiale over tid.

eForvaltningsforskriften (§ 26) stiller derfor krav om at dokumentet skal lagres sammen med signaturen og de øvrige opplysninger som er nødvendig for senere å kunne verifisere signaturen, typisk relevante sertifikater og opplysninger om sertifikatets status på signerings eller verifiseringstidspunktet.

I mange tilfeller vil det imidlertid være behov for å konvertere dokumentet til et annet format i forbindelse med lagring. Da kan den elektroniske signaturen ikke lenger verifiseres. I disse tilfellene må arkivet i henhold til forskriften overta ansvaret for sporbarheten ved å verifisere signaturen i forbindelse med arkivering, og lagre den sammen med relevante opplysninger fra sertifikatet på en måte som sikrer meldingens integritet over tid.

Og det er naturligvis en sammenheng med reglene om utlevering av dokumenter som jeg nettopp snakket om. Arkivet må innrettes slik at forvaltningsorganet er i stand til å oppfylle sine plikter til utlevering av verifiserbare signaturer eller på annen måte bekrefte kopier som er egnet som dokumentasjon overfor tredjepart.

7. Rekonstruksjon av hendelsesforløp – hva som ligger bak et signert dokument når det er resultatet av en prosess

En av de store utfordringer vi står overfor når det gjelder elektronisk samhandling, er at den dokumentasjon vi ender opp med, og som arkiveres, ofte er resultatet av en prosess, der en person gjennom dialog med et informasjonssystem har tilegnet seg informasjon, bearbeidet informasjon og avgitt informasjon, vanligvis i form av svar på spørsmål systemet har stilt i løpet av prosessen. Typisk at brukeren ledes gjennom et antall sider som dels orienterer, dels samler inn opplysninger. Arbeidsflytverktøy styrer denne prosessen, og kan tilrettelegge den for den enkelte bruker. Dette kan for

eksempel føre til at ulike brukere får ulik informasjon og valg fordi de har svart ulikt på innledende spørsmål.

Vi opplever i mange sammenhenger at det er veldig fokus på det signerte dokumentet som arkiveres som resultat av en slik prosess, og verdien av signaturen som dokumentasjon for de faktiske forhold. Men like viktig som signaturen og innholdet i det signerte dokumentet, er å kunne dokumentere den *prosessen* brukeren gikk igjennom, og som ledet frem til det signerte dokumentet som kanskje skal legges til grunn for et normerende vedtak.

I tradisjonell, papirbasert samhandling, vil de rettslige virkningene av den disposisjon personen har foretatt i mange tilfelle kunne knyttes direkte til innholdet i et dokument, typisk en papirblankett (eller et skjema). Ved gå gjennom det utfylte skjemaet får man et inntrykk av hva parten har svart på og hvordan det er svart.

I systemer for elektronisk samhandling vil det i mange tilfeller ikke være noen slik kopling mellom det brukeren opplevde i systemdialogen, og den måte resultatet av arbeidsprosessen er oppsummert i et signert dokument. Det signerte materiale vil typisk representere et uttrekk av de data som har vært involvert. (Det er altså ikke skjemapresentasjonen/skjermbildene slik brukeren opplevde det som er signert.)

Det skal i denne sammenheng legges til at signeringsoperasjonen ofte styres av saksbehandlingssystemet og er i realiteten utenfor brukerens kontroll. I interaktive systemer er det ikke slik at brukeren på sin lokale maskin fremstiller et dokument som han så signerer og sender.

Det vil nok snarere være slik at saksbehandlingssystemet, som en del av prosessen, tilrettelegger de data som skal signeres og oversender hashverdien av disse til brukerens klient for signering.

Brukeren er i disse tilfellene helt ute av stand til å kontrollere hva som faktisk går til signering, og tilliten til sporbarheten i systemløsningen blir derfor avgjørende for troverdigheten til det signerte materialet.

Av det signerte materiale kan man for eksempel konstatere om vedkommende svarte ja eller nei på et spørsmål, hvilke tall vedkommende oppga i et felt for inntekt mv. Men for å kunne gjøre

seg opp en mening om hva personen faktisk forstod, eller burde forstå, må vi også vurdere de spørsmålene eller ledetekstene som svarene relaterer seg til. Og vi må kanskje ta stilling til hele den prosessen brukeren ble ledet gjennom, og vurdere hvorledes det inntrykk prosessen var egnet til å etterlate hos brukeren kunne påvirke vedkommendes oppfatning av spørsmålene underveis.

Vi har eksempler på moderne saksbehandlingssystemer som signerer felter som brukeren aldri har blitt konfrontert med pga sporvalg, datoer som forekommer (skjult) flere steder mv. Dette er opplysninger som, når de settes inn i rette sammenheng, selvfølgelig ikke er til skade for brukeren, men bare tanken på at det faktisk signeres uttrekk av felter som brukeren aldri har sett kan innebære et press mot troverdigheten til systemløsningen.

Dette innebærer at verdien av det signerte materiale ikke kan måles uavhengig av de tiltak som er etablert med hensyn til sporbarhet mellom det signerte materialet som er resultatet av en arbeidsprosess, og dokumentasjonen for hvorledes selve prosessen forløp.

Det betyr at bl.a. opplysninger om gjeldende versjon av skjemadefinisjoner, arbeidsflyt og regelhåndteringsverktøy må kunne identifiseres med referanse fra det signerte materialet eller med kopling til det tidspunkt prosessen ble registrert gjennomført.

Dette kan antakelig håndteres enten ved hjelp av signerte attributter, definert innenfor rammen av en veldefinert signaturpolicy eller som lagrede revisjonsspor i tilknytning til den signerte melding, i begge tilfeller med referanse til systematisk og dokumentert lagring av alle relevante versjoner av skjemaer, arbeidsflyt og regelhåndteringsverktøy med angivelse av tidsmessig tilknytning.

Vi har ikke eksplisitte rettslige krav om lagring av slik sporingsinformasjon Norge, men det er antakelig helt nødvendig for å kunne føre fyllestgjørende og troverdig bevis for et hendelsesforløp.

Følgelig bør det antakelig anses som et grunnleggende krav til forsvarlig innretning av denne type systemer, selv om det ikke har kommet til uttrykk i noen skrevet regel.

Rolf Riisnæs har innenfor emnet publisert blant annet:

- *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar*, Fagbokforlaget (2007)
- *Regelverksutvikling og brukerdeltakelse i eForvaltningen*, i Dag Wiese Schartum (red.), Elektronisk forvaltning i Norden, Fagbokforlaget (2007)
- *Sikker elektronisk samhandling med og i forvaltningen (eForvaltningsforskriften)*, i Arild Jansen og Dag Wiese Schartum (red.), Informasjonssikkerhet - Rettslige krav til sikker bruk av IKT, Fagbokforlaget (2005)
- *Digital Certificates and Certification Services*, i Peter Wahlgren (ed), IT Law, Scandinavian Studies in Law Volume 47, Stockholm Institute for Scandinavian Law (2004)

Frågeställningar

- Har statliga myndigheter en skyldighet att lägga ut rättslig information på nätet?
- Vilket ansvar har staten för denna information?
- Vad kan bli följderna om denna information är felaktig?
- Vilka övervägande bör respektive myndighet göra innan de publicerar rättslig information på sin hemsida?

Har statliga myndigheter en skyldighet att lägga ut rättslig information på nätet?

Förvaltningslagen (1986:223)

4 § första stycket

Varje myndighet skall lämna upplysningar, vägledning, råd och annan sådan hjälp till enskilda i frågor som rör myndighetens verksamhetsområde. Hjälpens skall lämnas i den utsträckning som är lämplig med hänsyn till frågans art, den enskildes behov av hjälp och myndighetens verksamhet.

5 § andra stycket

Myndigheterna skall också se till att det är möjligt för enskilda att kontakta dem med hjälp av telefax och elektronisk post och att svar kan lämnas på samma sätt.

Verksförrordningen (1995:1322)

7 § andra stycket 5

Myndighetens chef skall

”se till att allmänhetens och andras kontakter med myndigheten underlättas genom en god service och tillgänglighet, genom information och genom ett klart och begripligt språk i myndigheternas skrivelser och beslut,”

Vad kan bli följderna om myndighetens information är felaktig?

1. Skadestånd

3 kap. 2 § 1 Skadeståndslagen (1972:207)

Staten eller en kommun skall ersätta

1. personskada, sakskada eller ren förmögenhetsskada, som vållas genom fel eller försummelse vid myndighetsutövning i verksamhet för vars fullgörande staten eller kommunen svarar, och

3 kap. 3 § Skadeståndslagen

Staten eller en kommun skall ersätta ren förmögenhetsskada som vållas av att en myndighet genom fel eller försummelse lämnar felaktiga upplysningar eller råd, om det med hänsyn till omständigheterna finns särskilda skäl. Därvid skall särskilt beaktas upplysningarnas eller rådets art, deras samband med myndighetens verksamhetsområde och omständigheterna när de lämnades.

Regeringsrättens avgörande (RÅ 2004 ref 8)

"En av Livsmedelsverket offentliggjord skrivelse, kompletterad med ett pressmeddelande jämte vissa ytterligare uppgifter på verkets hemsida, har - trots att den rubricerats som information - ansetts utgöra ett överklagbart beslut, vilket undanröjts såsom innefattande ett kompetensöverskridande."

2. "Förtroendeförlust"

Vilka övervägande bör respektive myndighet göra innan de publicerar rättslig information på sin hemsida?

- Överväger fördelarna nackdelarna med att publicera informationen?
- Vilka risker finns med att publicera informationen?
 - ju mer som läggs ut desto större risk för fel i informationen + svårt att överblicka och kontrollera
 - konflikt/dåligt samarbete mellan olika yrkesgrupper och vad de vill åstadkomma med publiceringen
 - ledningen för myndigheten är inte införstådd med riskerna att publicera rättslig information
 - vilka rutiner finns för att kontrollera den information som publiceras?
 - vilka rutiner finns för att kontrollera när information behöver uppdateras eller tas bort?
 - finns det någon på myndigheten som är ansvarig för informationen?

Checklista

- Myndighetens ledning bör verka för ett nära samarbete mellan jurister och informatörer samt se till att det finns rutiner för hur rättslig information publiceras på myndighetens hemsida
- Implementera rutiner;
 - för att kontrollera att rättslig information som ska publiceras är korrekt
 - för att kontrollera att rättslig information är uppdaterad
 - för att avlägsna inaktuell eller felaktig information
- Utse en ansvarig enhet/person som ser till att rutinerna följs