

En konsults perspektiv på

Informationssäkerhet och författningskrav i verksamheter

Dr Fredrik Björck

e-Stockholm '08 Legal Conference



Agenda

- I. Bakgrund och verksamhet
- II. Författningskrav som drivkraft
- III. Att hantera författningskrav
- IV. En iakttagelse om utvecklingen
- V. Frågor och svar

Del I

MIN BAKGRUND OCH VERKSAMHET

Bakgrund

DJ, Radio &
TV-producent

Studerar
Ekonomi

IT-revision

Informations-
säkerhet



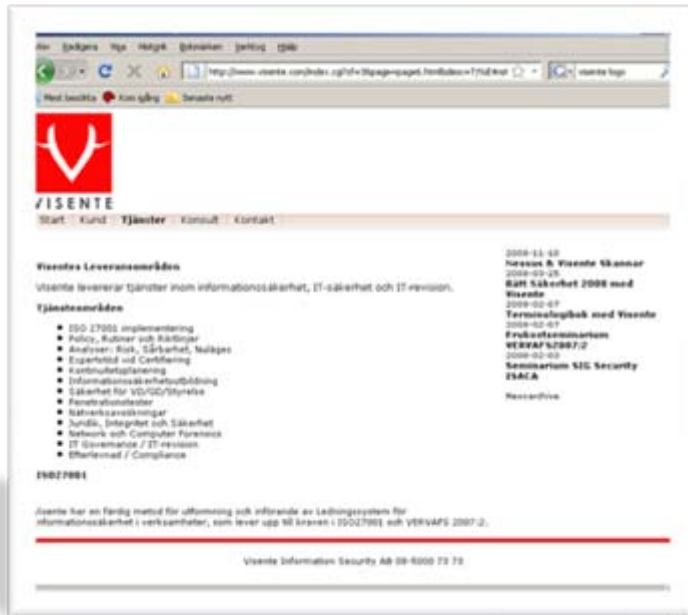
Radio Växjö 102.4



DJ Freddie



Verksamhet



www.visente.com

Visente levererar rådgivningstjänster inom informationssäkerhet.

Kunder är företag och myndigheter.

Typiska uppdrag är analys, utveckling och implementering av systematiskt informationssäkerhetsarbete:

- Analyser: Nuläge, risk, verksamheten
- Informationssäkerhetspolicy
- Riktlinjer inom informationssäkerhet
- Utbildning av medarbetare
- Tekniska granskningar och revision.

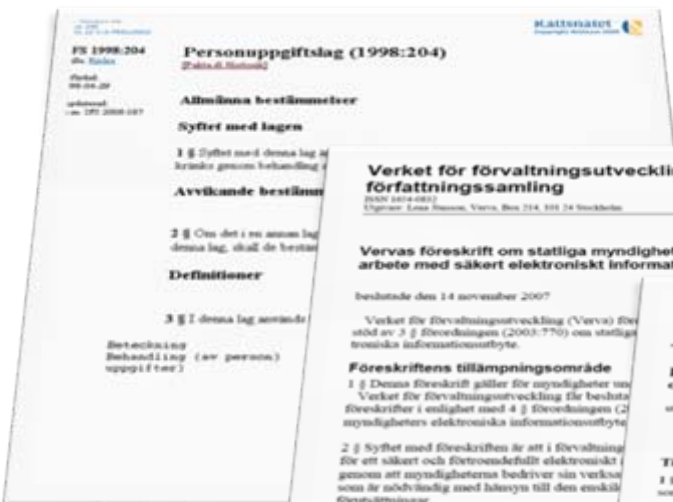
Del II

FÖRFATTNINGSKRAV SOM DRIVKRAFT

Kravkällor Informationssäkerhet



Författningskrav som drivkraft



Personuppgiftslag



Vervas föreskrift:
Säkert elektroniskt informationsutbyte



Förordning:
Intern styrning och kontroll

Det är ofta författningskrav som får kunderna att besluta sig för att satsa på informationssäkerhet

Vad finns det då för författningskrav på informationssäkerhet?

- Generella
 - föreskrifter (ex. Vervafs 2007:2)
 - Lagar (ex. Personuppgiftslagen)
- Branschspecifika
 - föreskrifter (ex. inom hälso- och sjukvårdssektorn)
 - Lagar (ex. personuppgifter vid riksdagsval)
- (Med flera)

Exempel: Informationssäkerhetspolicy

3 Mål

Införandet av ledningssystemet för informationssäkerhet syftar till att uppfylla följande mål:

- *Allmänhetens förtroende:* Att genom god informationssäkerhet medverka till att bevara och öka tilltron till allmänna val och folkomröstningar.
- *Författningars efterlevande:* Att leva upp till de krav som ställs på informationssäkerheten i följande standarder och författningar:
 - Informationssäkerhetsstandard SS-ISO/IEC 27001,
 - Vervas föreskrift (2007:2) om statliga myndigheters arbete med säkert elektroniskt informationsutbyte,
 - Säkerhetsskyddslagen (1996:627),
 - Personuppgiftslagen (1998:204),
 - Förordning (2006:942) om krisberedskap och höjd beredskap,
 - Förordning (1995:1300) om statliga myndigheters riskhantering, samt
 - Lag (2001:183) om behandling av personuppgifter i verksamhet med val och folkomröstningar
- ~~God informationssäkerhet:~~ Att lägga grunden till ett systematiskt arbete med informationssäkerhet som resulterar i en för verksamheten kontinuerligt anpassad nivå och uppbyggnad.

Kravkällor Informationssäkerhet



Del III

ATT HANTERA FÖRFATTNINGSKRAV

Hur kan man hantera legala krav inom ramen för informationssäkerhetsarbetet?

- Det beror på lite var i arbetet man är:
 - Ska man fastställa lagkraven generellt för verksamheten och försöka se ifall de är uppfyllda
 - Håller man på med en analys av kraven på en enskild informationsresurs eller IT-system?
- Det finns verktyg för att analyseras kraven, exempelvis RISA av Helena Andersson.

Kärnan i metodik för att identifiera författningskrav inom informationssäkerhet

- Utgå från en bruttolista på tänkbara lagrum som kan komma ifråga.
- Gå igenom lagrummens lydelse och avgör ifall de alls är tillämpliga på analysobjektet (ex. ett IT-system).
- Markera lagrum som är tillämpliga.
- Undersök, bedöm och beskriv hur och ifall de aktuella kraven kan anses vara uppfyllda (eller kan riskera att inte uppfyllas)
- Koppla in juristerna vid behov!

Exempel: Tillvägagångssätt

2. Analyser

2.1 Författningskrav

Information: Författningskrav kan finnas både för verksamheten i stort såväl som för den analyserade informationstillgången specifikt. Målet med denna analys är att identifiera alla de författningskrav som måste uppfyllas av myndigheten och som relaterar till tillgångens informationssäkerhet.

Steg för att analysera författningskrav

- 1) Läs igenom lagrummets innehåll och betydelse. Man kan ta del av författningarna i helhet genom att klicka på respektive lags namn (samtidigt som `[ctrl]` hålls ned).
- 2) Bedöm och markera med ett kryss om lagrummet är tillämpligt för informationstillgången. Innehåller författningen sådant som ställer krav på tillgångens säkerhet?
- 3) Bedöm och markera med ett kryss om lagrummet är uppfyllt eller ej.
- 4) Skriv eventuellt en kommentar. Vad baseras bedömningen på? Varför är lagrummet inte uppfyllt?

Exempel: Lista på författningar

Lagrum	Innehåll
Järnvägslag (2004:519)	Lag som reglerar den verksamhet vi bedriver
Järnvägsinspektionens föreskrifter (BV-FS 2000:4)	Om hälsoundersökning och hälsotillstånd för personal med arbetsuppgifter av betydelse för trafiksäkerheten avser krav på personal som ska planeras.
Järnvägsinspektionens föreskrifter (BV-FS 2000:3)	Om utbildning för personal med arbetsuppgifter av betydelse för trafiksäkerheten avser krav på personal som ska planeras.
Personuppgiftslag (1998:204)	Ställer krav på vilken information som får finnas i systemet, dess riktighet samt hur den hanteras.

Exempel: Bedömning

Analys av författningskrav

Lag	Tillämplig	Uppfylld	Kommentar
Jämvägslag (2004:519)	<input type="checkbox"/>	<input type="checkbox"/>	
Jämvägsinspektionens föreskrifter (BV-FS 2000:4)	<input type="checkbox"/>	<input type="checkbox"/>	
Jämvägsinspektionens föreskrifter (BV-FS 2000:3)	JA	<input type="checkbox"/>	
Personuppgiftslag (1998:204)	<input type="checkbox"/>	<input type="checkbox"/>	Om tillämplig, fyll i uppgifter om behandlingen på nästa sida.

Exempel: Personuppgifter

Förteckning enligt 39 § Personuppgiftslagen

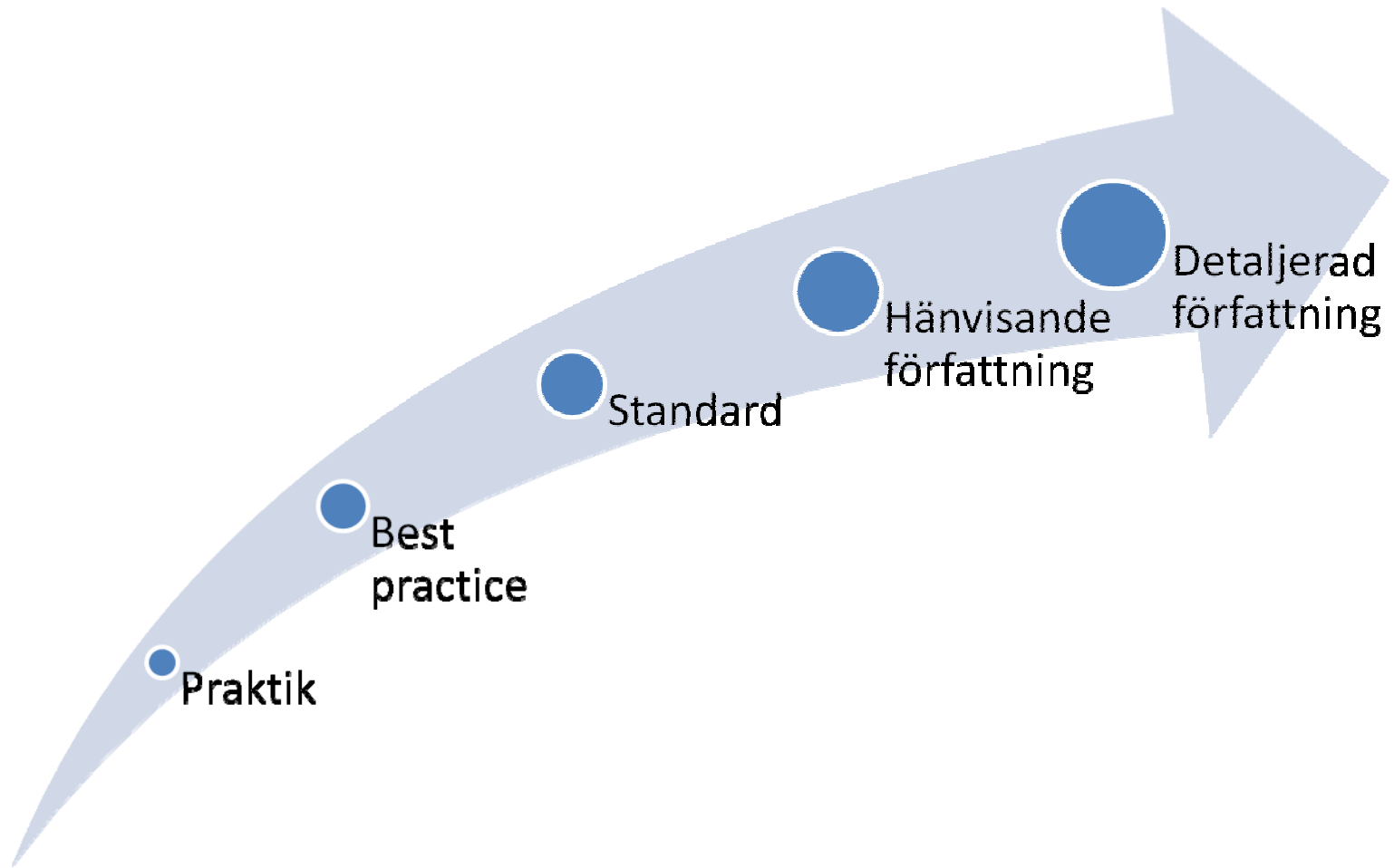
Information: Denna förteckning ska enligt lag upprättas och arkiveras hos myndigheten för varje informationstillgång som innehåller personuppgifter (uppgifter som direkt eller indirekt kan hänföras till en fysisk person). Ifylls endast om informationstillgången innefattar personuppgifter.

Personuppgifts-ansvarig	Namn: XXX		Organisationsnummer: XXXXXX-XXX
	Postutdelningsadress:		
	Postnummer: 100 00	Ortnamn: Stockholm	Telefonnummer: 08-12345678
Registret och behandlingen	Uppgifterna nedan är: <input type="checkbox"/> Uppgifter om ny <u>behandling</u> <input type="checkbox"/> Ändring av eller tillägg till tidigare anmälan <input type="checkbox"/> Avanmälan		
	Registrets/behandlingens namn: <u>X-Systemet</u>		
	Ändamålet/ändamålen med behandlingen:		
	Den/de kategorier (grupper) av personer som berörs av behandlingen:		

Del IV

EN IAKTTAGELSE OM UTVECKLINGEN

Vägen till författningskrav



Trender

- Bättre och mer heltäckande lagar
 - Hål täpps till (ex. BrB om dataintrång)
 - ”Skyddsobjekt” ändras
 - Lagar harmoniseras inom EU
- Allt mer detaljerad författning kring informationssäkerhet
- Flera liknande författningar kring just riskhantering som relaterar till informationssäkerhet skapar frågor.

Utmaningen

- Inom juridik och informationssäkerhet står vi idag inför en pedagogisk utmaning.
- Det gäller att alla som ska lyda författningen ges möjlighet att först ta till sig den och förstå dess innebörd.
- Inte minst på myndighetssidan finns det risk att brist på att förklara olika riskhanteringskrav och informationssäkerhetskrav och hur de förhåller sig till varandra gör att det blir svårt att navigera rätt.

fredrik . bjorck @ visente . com

08 50007373

Del IV

FRÅGOR OCH SVAR!