Verifying security since 1999

Dataskydd och den nya standarden EN-SS-ISO/IEC 27701

Hans Hedbom

Delar av materialet är producerat av och används med tillåtelse av
Rose-Mharie Åhlfeldt, Högskolan i Skövde

Kort om mig

- Seniorkonsult på Veriscan.
- Tidigare forskare och universitetsadjunkt på Karlstads Universitet.
- Sysslat med datorer och datavetenskap sedan 1986.
  - Informationssäkerhet sedan 1996
  - Dataskydd och personlig integritet sedan 2007
- Arbetar tidvis som teknisk bedömare åt Swedac.
- Insyltad i standardisering sedan 2007.
- Medlem i TK318 och ordförande för TK318/AG51 sedan 2009.
- Starkt involverad i arbetet med ISO/IEC 27701 på nationell och internationell nivå.

Grunden för personlig integritet

Artikel 8 - Rätt till skydd för privat- och familjeliv

1. Var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens.
2. Offentlig myndighet får inte ingripa i denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.

- Europeiska konventionen om skydd för de mänskliga rättigheterna

Personlig integritet ?

"The right to be let alone"

(Judge Cooley (Cooley on Torts, 2d ed., p. 29.) Cited in (Warren & Brandeis "The Right To Privacy" 1890)

Personlig integritet?

"The common law secures to each individual the right of determining, ordinarily, **to what extent his thoughts, sentiments, and emotions shall be communicated to others** […] and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. **The existence of this right does not depend upon the particular method of expression adopted**.[…] Neither does the existence of the right depend upon the nature or value of the thought or emotions, nor upon the excellence of the means of expression.[…] In every such case the individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent." (Warren & Brandeis The Right To Privacy 1890)

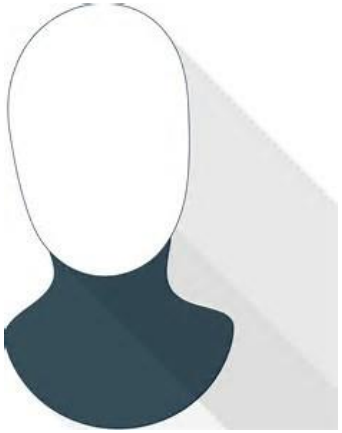
"The right to be let alone"

(Warren & Brandeis 1890)

Personlig integritet ?

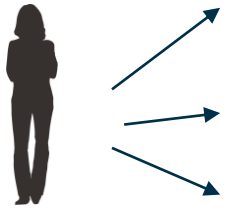
"Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others"

(Alan Westin 1967)

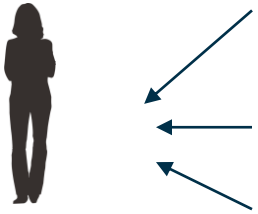


Personlig integritet : Dimensioner

- Informational self determination



- Spatial privacy



Dataskydd handlar främst om ISD.

VARFÖR BRY SIG OM INFORMATIONSSÄKERHET NÄR DET GÄLLER GDPR? ÄR DET INTE BARA JURIDIK?

•Mjaaaa, Personlig integritet ≠ Info Sec and Dataskydd ≠ Info Sec
MEN:

- Utan informationssäkerhet ingen möjlighet för "informational self determination" (dataskydd)
- Ett central byggblock i GDPR.
- Påverkar direkt eller indirect möjligheten att implementera och efterleva manga paragrafer (inte bara de som enbart relaterar till informationssäkerhet)
- De metoder, verktyg, processer och skyddsåtgärder som används har stora likheter.
- Ergo: Det är svårt att implementera GDPR på ett bra, stabilt och hållbart sätt utan kunskap om och förståelse för bade personlig integritet och informationssäkerhet eftersom de påverkar varandra.

SYSTEMATISKT INFORMATIONSSÄKERHETSARBETE –

LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET

Genom ett systematiskt arbete med informationssäkerhet kan organisationer öka kvaliteten på och förtroendet för sin verksamhet

SS-ISO/IEC 27001/2017 – LIS - Krav

- Organisationens förutsättningar
- Ledarskap
- Planering
- Stöd
- Verksamhet
- Utvärdering
- Förbättring

GEMENSAMMA PROCESSER OCH ASPEKTER

- Riskanalys
- Riskhantering
- Incidenthantering
- Internrevision
- Liknande krav på organisatoriska åtgärder.
- Kravställningsprocessen för informationssäkerhet och metoder för skydd är de samma.
- .....

Grunden till många av åtgärderna och processerna relaterade till DS finns redan I ISO 27001

Finns ej:

- DSO
- Ansvarig / Biträde
- Speciella krav vad gäller innehåll i register.
- Syfte
- Legal grund
- 3:e land
- Kommunikation till den registrerade och processer för att hantera detta:
  - "Notice and Consent"
  - Den registrerades rättigheter
  - Incidenter

Source: Versican Security AB

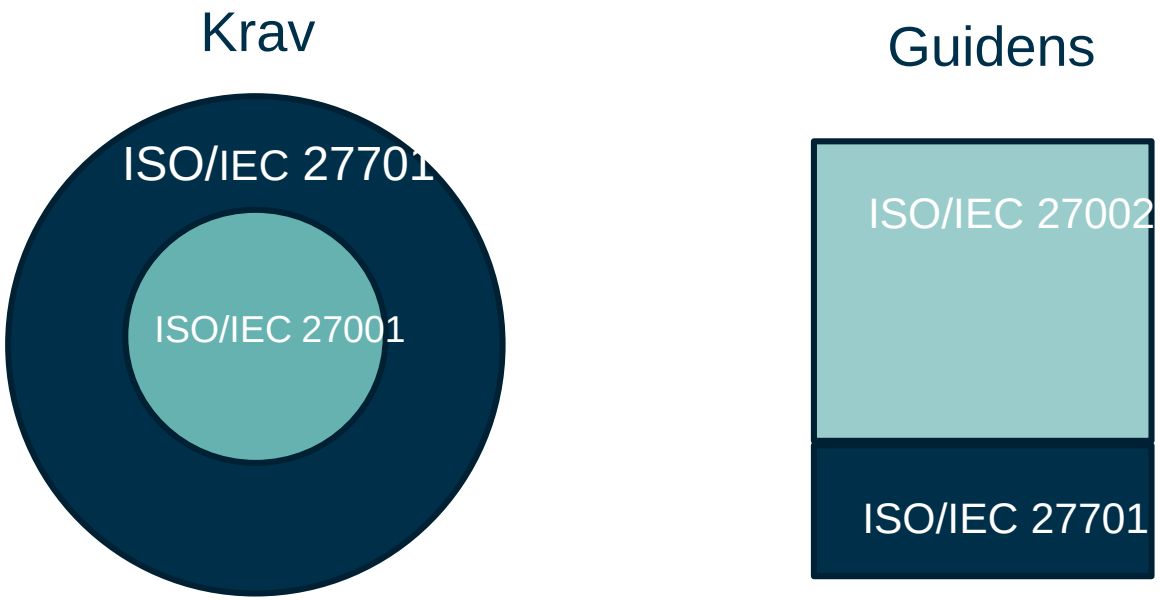
27001 och Annex A - LIS

- Roller för informationssäkerhet
- Medvetenhet och träning
- Identifiering av tillgångar och ägare – tillgångsregister.
- Klassning av persondata bade från företaget och den registrerades perspektiv.
- Säkerhetsåtgärder inclusive dtahanteringsrutiner.
- Metoder för kravhantering (Lägg bara till DS perspektivet)
- Metoder för utveckling/ förändring och upphandling av system (Lägg bara till DS perspektivet d.v.s data minimering och "privacy by design")
- Riskanalys och riskhantering (Lägg bara till DS perspektivet)
- Incidenthantering (nya typer och rapportrutiner)
- Outsourcing/Leverantörsavtal (Biträdesavtal)

Förutsättningar för standardisering inom personlig integritet inom ISO/IEC JTC1/SC 27/WG5

- Scoopet på SC27 ger bara förutsättningar för standardisering inom det som EU kallar data protection (personuppgiftsskydd e.g. informational self determination).
- Vitt skilda lagar, ibland motsägelsefulla, i de olika länderna.
- Det bästa vi kan sträva efter är “best practice” utan att vi bryter mot någon lag. Vi kan aldrig garantera full lag teckning men vi kan stötta på vägen.
  - Dock har ISO/IEC 27701 i hög grad inspirerats av GDPR och den har kommenterats på via ”liaisons” av Art29 och EBDP.
- Inte vi som får eller kan uttala oss om huruvida en standard kan användas för att visa compliance mot något annat än standarden själv.
- Och till slut: Best practice är mer än bara laguppfyllnad ☺.

ISO/27701s struktur (har historiska skäl).



Adderade eller förtydligade krav

Generella

- Kraven ISO/IEC 27001:2013 som omnämner "informationssäkerhet" ska utvidgas till skyddet för den personliga integriteten som potentiellt påverkas av behandlingen av personuppgifter.
  - ANM. I praktiken gäller att där "informationssäkerhet" används i ISO/IEC 27001:2013 "informationssäkerhet och dataskydd" i stället (se bilaga F).

Adderade krav till ISO/IEC 27001 Kap 4

- Förtydliganden och tillägskrav till:
  - Att förstå organisationen och dess förutsättningar
  - Att förstå intressenters behov och förväntningar
  - Att bestämma ledningssystemets omfattning
  - Ledningssystem för informationssäkerhet

Veriscan

Adderade eller förtydligade krav

- Adderade krav till ISO/IEC 27001 Kap 5 (Ledarskap)
  - Inga utom den utökade tolkningen av “information security”
- Adderade krav till SO/IEC 27001 Kap 6 (Planering)
  - **6.1.2 c) och 6.1.2 d) är förtydligad så att riskanalys och riskhantering även skall ta in aspekter av personlig integritet.**
  - **6.1.3 c) och 6.1.3 d) är förtydligade så att hänsyn även skall tas för Annex A och B i ISO/IEC 27701 vid riskhantering och I SoA.**
- Adderade krav till ISO/IEC 27001 Kap 7 (Stöd)
  - Inga utom den utökade tolkningen av “information security”
- Adderade krav till ISO/IEC 27001 Kap 8 (Verksamhet)
  - Inga utom den utökade tolkningen av “information security”
- Adderade krav till ISO/IEC 27001 Kap 9 (Utvärdering av prestanda)
  - Inga utom den utökade tolkningen av “information security”
- Adderade krav till ISO/IEC 27001 Kap 10 (Förbättringar)
  - Inga utom den utökade tolkningen av “information security”

Nya Annex och tillägg till ISO/IEC 27002

- ISOIEC 27701 innehåller två nya normativa annex.
  - Annex A är tänkt för rollen som personuppgiftsansvarig med 31 säkerhetsåtgärder
  - och Annex B för rollen som personuppgiftsbiträde med 18 säkerhetsåtgärder..
- Några av implementations guiderna i ISO/IEC 27002 har fått tillägg och implementations anvisningar för de nya kontrollerna i Annex A och B finns i standarden (dessa ses som tillägg till ISO/IEC 27002)
- Dessutom finns ytterligare 4 informerande bilagor:
  - Annex C med korsreferenser till ISO/IEC 29100
  - Annex D med korsreferenser mot artiklar i GDPR
  - Annex E med korsreferenser mot ISO/IEC 27018 och ISO/IEC 29151
  - Annex F med exempel på hur ISO/IEC 27701 ska tillämpas på ISO/IEC 27001 och ISO/IEC 27002 .

Veriscan

Avsnitt i ISO/IEC 27002:2017	Titel	Underavsnitt i detta dokument	Kommentar
5	Informationssäkerhetspolicy	6.2	Ytterligare vägledning
6	Organisation av informationssäkerhetsarbetet	6.3	Ytterligare vägledning
7	Personalsäkerhet	6.4	Ytterligare vägledning
8	Hantering av tillgångar	6.5	Ytterligare vägledning
9	Styrning av åtkomst	6.6	Ytterligare vägledning
10	Kryptering	6.7	Ytterligare vägledning
11	Fysisk och miljörelaterad säkerhet	6.8	Ytterligare vägledning
12	Driftsäkerhet	6.9	Ytterligare vägledning
13	Kommunikationssäkerhet	6.10	Ytterligare vägledning
14	Anskaffning, utveckling och underhåll av system	6.11	Ytterligare vägledning
15	Leverantörsrelationer	6.12	Ytterligare vägledning
16	Hantering av informationssäkerhetsincidenter	6.13	Ytterligare vägledning
17	Informationssäkerhetsaspekter avseende hantering av verksamhetens kontinuitet.	6.14	Ingen LISD-specifik vägledning
18	Efterlevnad	6.15	Ytterligare vägledning

Veriscan

A.7.2 Villkor för insamling och behandling

Mål: Att fastställa och dokumentera att behandlingen är laglig, med rättslig grund enligt tillämpliga jurisdiktioner, och med tydligt definierade och legitima ändamål.

- Identifiera och dokumentera ändamål
- Identifiera rättslig grund
- Fastställ när och hur samtycke ska inhämtas
- Inhämta och dokumentera samtycke
- Bedömning av konsekvenser för den personliga integriteten
- Avtal med personuppgiftsbiträden
- Gemensam personuppgiftsansvarig
- Dokumenterad information relaterad till behandling av personuppgifter

A.7.3 Förpliktelser gentemot de registrerade

Mål: Att säkerställa att de registrerade förses med lämplig information om behandlingen av deras personuppgifter och att uppfylla andra eventuella tillämpliga förpliktelser gentemot de registrerade i relation till behandlingen av deras personuppgifter.

- Fastställa och uppfylla förpliktelser gentemot de registrerade
- Fastställa information till de registrerade
- Tillhandahålla information till de registrerade
- Tillhandahålla en mekanism för att ändra eller återkalla samtycke
- Tillhandahålla en mekanism för att invända mot personuppgifts behandling
- Åtkomst, korrigering och/eller radering
- Personuppgiftsansvarigas skyldighet att informera tredje part
- Tillhandahålla en kopia av behandlade personuppgifter
- Hantera begäran från de registrerade
- Automatiserat beslutsfattande

Veriscan

A.7.4 Inbyggt dataskydd och dataskydd som norm

Mål: Att säkerställa att processer och system är utformade så att inhämtande och behandling (inklusive användning, utlämnande, bevarande, överföring och destruktion) begränsas till det som är nödvändigt för det identifierade ändamålet.

- Begränsa insamling
- Begränsa behandling
- Riktighet och kvalitet
- Mål för personuppgiftsminimering
- Avidentifiering och destruktion av personuppgifter vid slutet av behandlingen
- Tillfälliga filer
- Bevarande
- Destruktion
- Säkerhetsåtgärder för överföring av personuppgifter

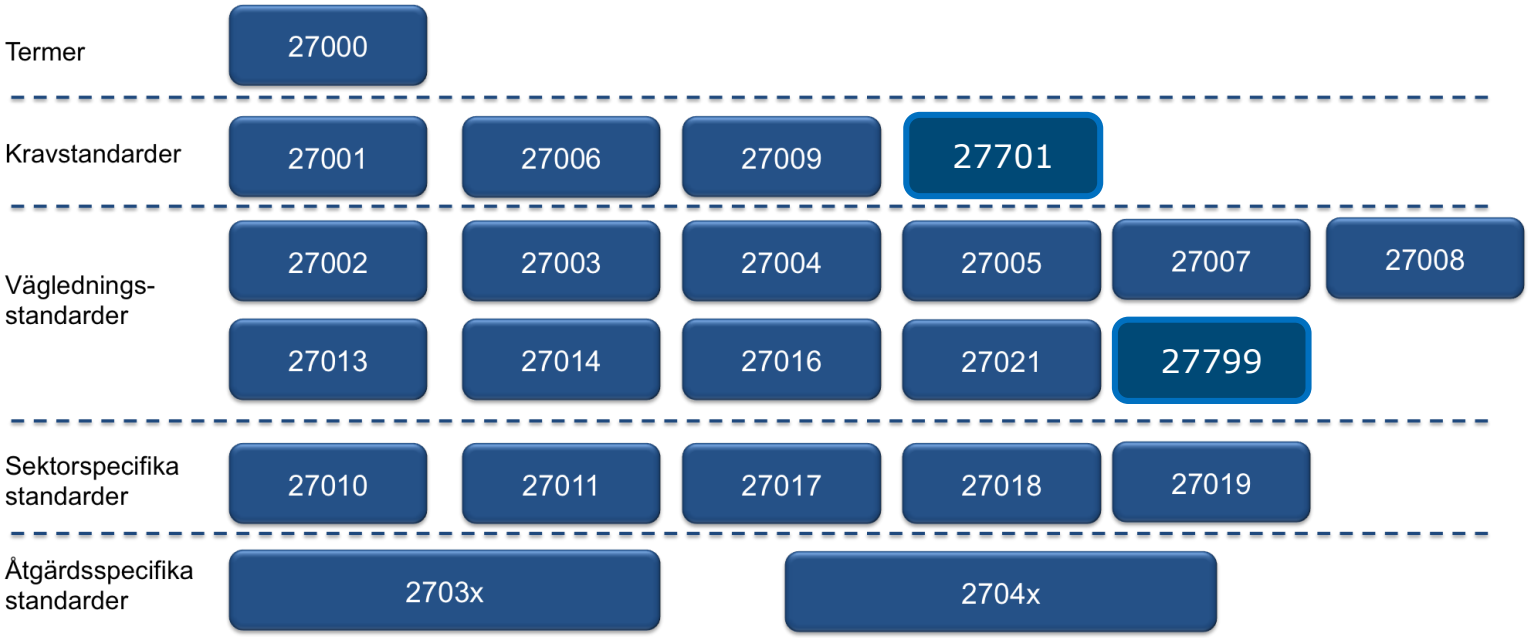
A.7.5 Delning, överföring och utlämnande av personuppgifter.

Mål: Att fastställa om och dokumentera när personuppgifter delas, överförs till andra jurisdiktioner eller tredjeparter och/eller utlämnas i enlighet med tillämpliga förpliktelser.

- Identifiera grunden för personuppgiftsöverföring mellan jurisdiktioner
- Länder och internationella organisationer som personuppgifter kan överföras till
- Dokumenterad information vid överföring av personuppgifter
- Dokumenterad information om utlämnande av personuppgifter till tredje part

Veriscan

Hur hänger de ihop.



Veriscan

Om certifiering och ackreditering.

- Certifiering
  - Bygger på utomstående parts granskning.
  - Sker mot ett förutbestämt schema
  - Bygger oftast på krav baserade på antingen standarder, lagar eller andra typer av regelverk.
  - Kan tas fram av vem som helst.
  - I GDPR kan ackrediterade certifieringsorgan och tillsynsmyndigheten certifiera.

- Ackreditering
  - Styrt i förordningar, avtal och lagar
  - Sköts som regel av en ackrediteringsorganisation per land (i Sverige Swedac)
  - Opartisk granskning av certifieringsorgan.
  - Granskningen sker ofta mot någon av standarderna 17020,17021,17025 och 17065 med tillägg eller utökningar (27006).
  - I GDPR kan en ackrediteringsorganisation eller tillsynsmyndigheten ackreditera.

Vilka kan man certifiera mot och varför.

- Man kan bara certifiera sig mot kravstandarder
  - I detta fall ISO/IEC 27001 och ISO/IEC 27701, den sistnämnda kommer troligtvis aldrig stå ensam.
- Man kan inte certifiera sig (ackrediterat) mot vägledningsstandarder.
  - Dessa innehåller inga krav ”shall” utan bara bör ”should” och har därför inga krav man kan certifiera sig mot.
- Kan jag certifiera mig under ISO/IEC 27017 och ISO/IEC 27018?
  - Nej, det går inte att få ett ackrediterat certifikat för dessa standarder och kommer aldrig bli möjligt.
  - De är inte kravstandarder.

GDPR och Certifiering

- Nedanstående är tolkningar av ENISA och Art29
- Bygger på 17065 och därför bara produkt, tjänst eller process.
  - Produkt osannolikt eftersom behandling berör hela kedjan.
  - Bara behandlingen inom processen eller tjänsten certifieras.
  - Troligtvis mål snarare än process relaterad certifiering (både vad och hur snarare än bara vad.)
- Standarder godkända av dataskyddsmyndigheten kan användas för att visa på kravuppfyllnad i vissa paragrafer i GDPR (25,28 32 och 46)
- Kommer troligtvis aldrig gå att certifiera eller på annat sätt visa ”compliance” mot GDPR (I betydelsen ansvarsfrihet gent emot GDPR).

Så vad är nyttan då !

- Förutom att visa att man jobbar enligt standarden.
  - Ett bra hjälpmedel för hantering av informationssäkerhet och personuppgifter.
  - Få en verifiering av oberoende part.
  - Visa att organisationen bryr sig och har ett strukturerat arbetssätt.
  - Få ett ökat focus, engagemang och medvetenhet i informationssäkerhetsfrågor.
  - Ett incitament för att verkligen ta tag i uppgiften och ta den på alvar.
  - Ökad trygghet vid handel och avtal.
  - Ett “sanitetskrav” att använda vid upphandlingar.

Så vad är nyttan då?

- Kan jag certifiera mig nu?
  - 27001 ja definitivt.
  - 27701 Nej, inte under internationellt erkänd ackreditering ännu.

- Vad saknas för ackrediterade certifikat?
  - Måste fram en certifieringsschema för ISO/IEC 27701.
  - Detta är precis klart för publicering och heter TS 27006-2.

Vägledningsstandarder för hjälp inom dataskydd (publicerade).

- **ISO/IEC 31000** – Riskmanagement – Guidelines
  - innehåller riktlinjer för att hantera de risker som en organisation ställs inför.
- **ISO/IEC 27005** – Riskhantering för informationssäkerhet
  - Relevant att lägga in DPIA i riskhanteringsprocessen och i de fall en full DPIA inte behövs behöver man i alla fall göra en riskanalys för att bedöma skyddskraven.
- **ISO/IEC 29134** – Privacy impact assessment – Guidelines
  - Stöd i riskhanterings- och riskbedömningsprocessen

Vägledningsstandarder för hjälp inom dataskydd (publicerade).

- **ISO/IEC 29100** – Privacy framework
  - En vägledningsstandard som beskriver och förklarar principer, terminologi och aktörer inom området personlig integritet.
  - Kan användas för att förstå begrepp, roller och frågeställningar
  - Ingen kravstandard och kan inte användas för att visa efterlevnad av GDPR.

- **ISO/IEC TR 27550** ” Privacy engineering for system life cycle processes”
  - är en teknisk rapport som bland annat diskuterar , ”privacy-by-design”.

- **ISO/IEC 20889** ”Privacy enhancing data de-identification terminology and classification of techniques”
  - är en vägledningsstandard som diskuterar olika tekniker och metoder för avidentifiering.

Vägledningsstandarder inom dataskydd .

- ISO/IEC 29184 Online privacy notices and consent.
  - Ger vägledning gällande information till registrerade och samtycke.

- ISO/IEC 27555 Guidelines on personally identifiable information deletion (om ca 1 år)
  - Vägledning om radering av personuppgifter.

Frågor