Göteborgs Stad

Dataskyddsförordningen
och
Stadens styrsystem

Jan A Svensson
Informationssäkerhetschef

Göteborgs Stads styrsystem

Analyseras
-Juridisk analys
-Informationssäkerhetsanalys
-IT-analys

Soluret symboliserar det ständigt pågående cykliska arbetet som drivs av utgångspunkterna samt understöds av förutsättningarna.

Våra utgångspunkter

- Lagar och övriga författningar är det vi har att rätta oss efter inom alla områden.
- Den politiska viljan är de beslut och mål som tar form i kommunfullmäktige, nämnder och styrelser.
- Våra invånare, brukare och kunder som genom dagliga kontakter med vår organisation påverkar oss och vår verksamhet.

Vår systematik

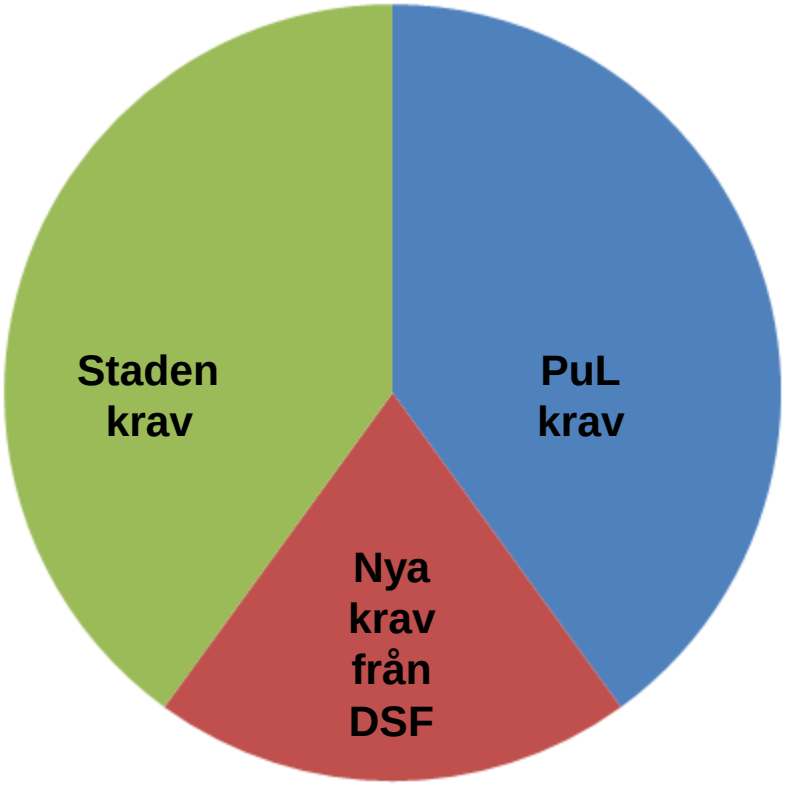
- Arbetsgången som styrningen ska följa: planering, genomförande, uppföljning och förbättring.

Våra förutsättningar

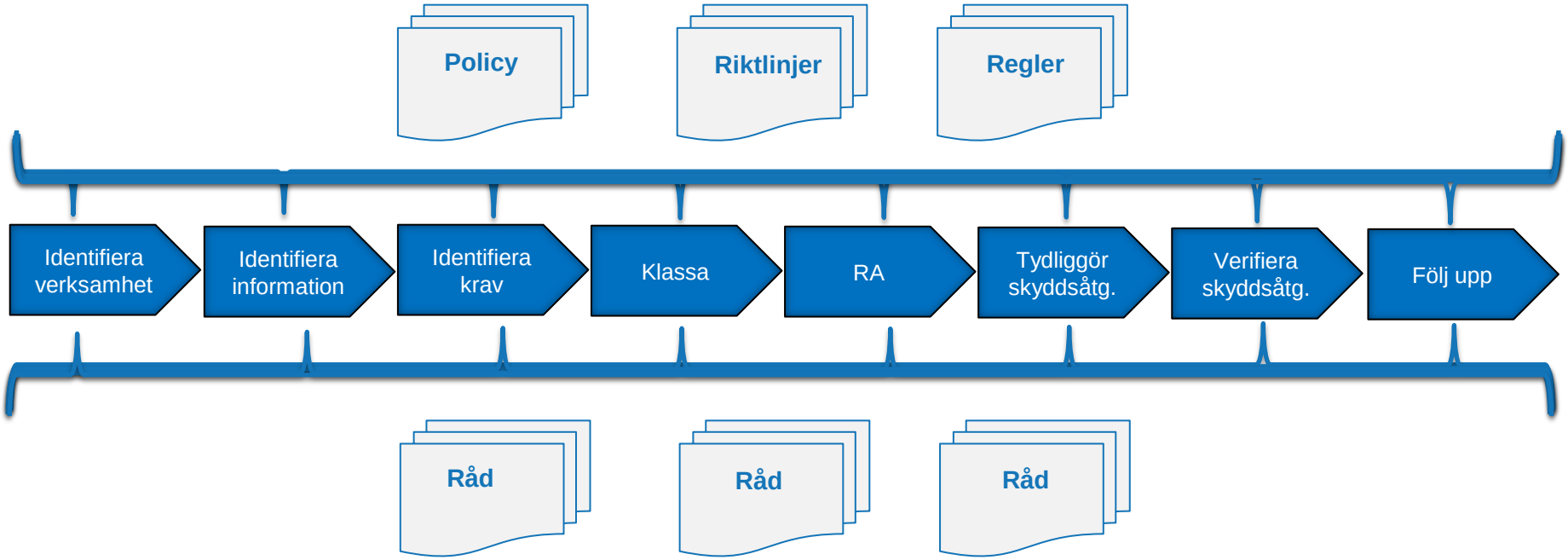
- Konkretisering av utgångspunkterna i styrande dokument och förhållningssätt för vägledning.
- Vi organiserar oss för att förverkliga intentionerna i de styrande dokumenten.
- Vi tydliggör roller och fördelar ansvar samt tillsätter resurser för att nå mål och utföra uppdrag.

Analysresultat

- Grundprinciperna i DSF rörande informationssäkerhet är i stort i linje med Stadens styrsystem
- De delar som har tillkommit och även preciserats jämfört med PuL har Staden i stort redan täckt in



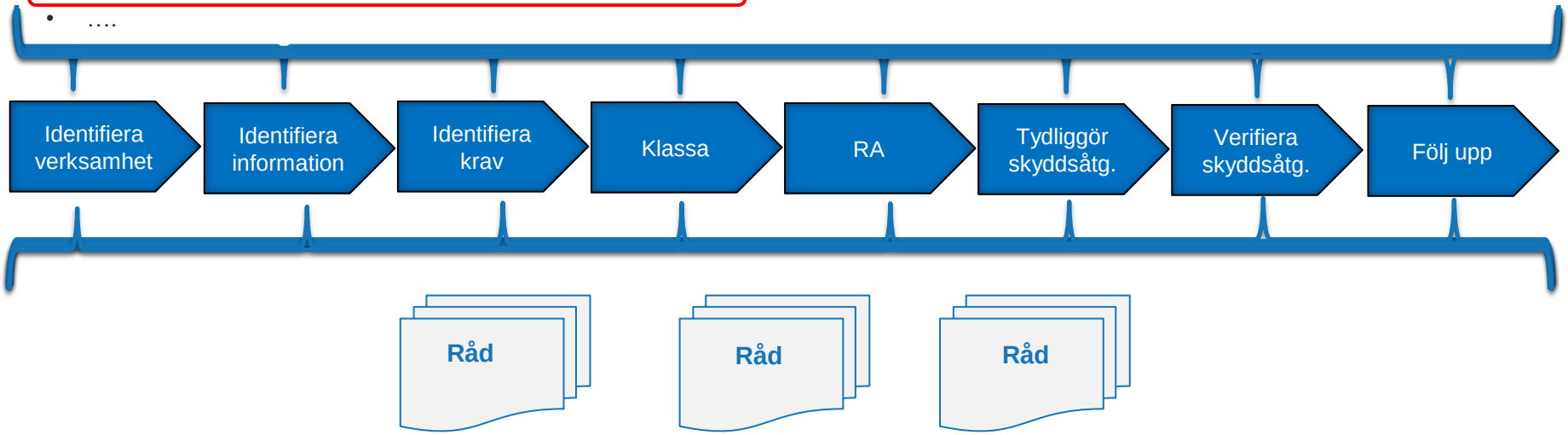
Stadens metod för säker informationshantering (del av styrsystemet)



Styr- och stöddokument (urval)

- ….
- Säkerhetspolicy
- Riktlinje för hantering av säkerhetsrisker
- Riktlinje för informationssäkerhet
- Riktlinjer för användning av informationsteknik
- Riktlinjer för intern kontroll
- Regler för kommungemensamma interna tjänster generellt
- Regler gällande informationssäkerhetsansvar för chefer
- Policy och riktlinjer för tillämpning av personuppgiftslagen
- ….

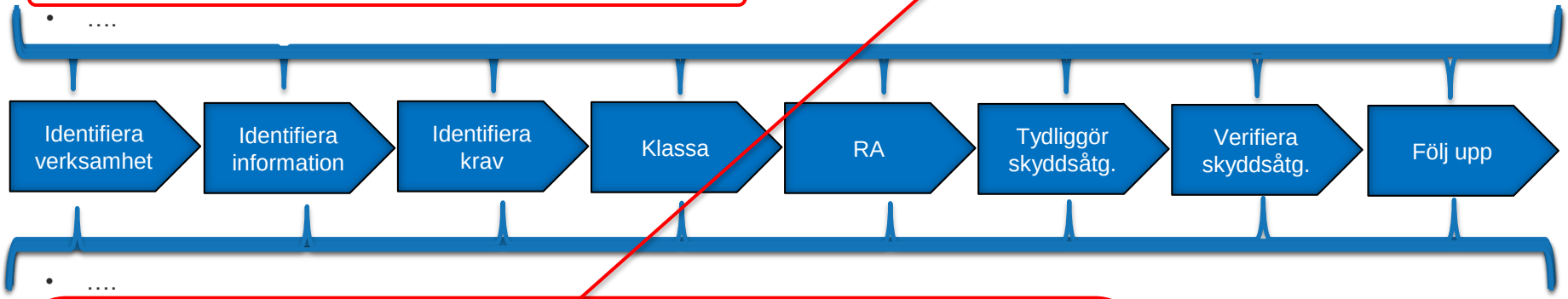
Ändringsbehov utifrån DSF-analyser!



Styr- och stöddokument (urval)

- ….
- Säkerhetspolicy
- Riktlinje för hantering av säkerhetsrisker
- Riktlinje för informationssäkerhet
- Riktlinjer för användning av informationsteknik
- Riktlinjer för intern kontroll
- Regler för kommungemensamma interna tjänster generellt
- Regler gällande informationssäkerhetsansvar för chefer
- Policy och riktlinjer för tillämpning av personuppgiftslagen
- ….

Ändringsbehov utifrån DSF-analyser!



- ….
- Råd för säker informationshantering
- Råd - exempel på informationsklassning
- Råd för riskanalys avseende informationssäkerhet
- Råd IT-säkerhetskontroller
- Råd – säkerställande av appar
- Råd - uppföljning och analys incidenter i informationssystem
- Råd för hur man i verksamheten bör agera för att säkerställa nyttjandet av molntjänster
- Råd – Förslag på lokala anvisningar/bestämmelser för informationshantering och IT-användning
- ….

Ändringar utifrån förändrad policy/riktlinje

Ändringsbehov i ”Policy och riktlinjer för tillämpning av personuppgiftslagen”

Göteborgs Stad

- Tydliggöra de grundläggande principerna för behandling av pu i Staden
- Tydliggöra krav på tillsättande av Dataskyddsombud
- Tydliggöra att Dataskyddsombudet ska rådfrågas och övervaka konsekvensbedömning (= riskanalys)
- Tydliggöra att det krävs samråd med tillsynsmyndigheten om man i sin riskhantering inte klarar av att minska en hög risk
- Tydliggöra att synpunkter från de registrerade ska inhämtas i samband med riskanalysen när det är lämpligt
- Tydliggöra att pseudonymisering eller kryptering är riskminimeringsåtgärder som bör användas (nivå 1)
- Tydliggöra krav gällande ”inbyggt dataskydd” och ”dataskydd som standard”
- Tydliggöra krav på att säkerställandet av personuppgiftshanteringen ska finnas med redan från den initiala planeringen och täcka såväl tekniska som organisatoriska åtgärder (riskanalys)
- Tydliggöra krav på att kunna visa, kontinuerligt testa, undersöka och utvärdera effektiviteten av införda säkerhetsåtgärder
- Tydliggöra krav på incidentanmälan till tillsynsmyndigheten
- Tydliggöra krav på spridning av incidentinformation till registrerade som drabbats
- Tydliggöra kraven som ställs på PUB-avtal
- Tydliggöra kraven på PUB att kunna visa att säkerhetskraven uppfylls, att det finns beskrivningar över hur kraven uppfylls och att säkerheten ska vara verifierad och verifieras regelbundet

Dataskyddsombud (DSO)

1 av 2

Göteborgs Stad

Huvudsaklig uppgift

- Vara kontaktpunkt för intressenter (tillsynsmyndighet, registrerade, medarbetare m fl)
- Informera och ge råd till PUA och medarbetare bl a om skydd och skyldigheter enligt DSF samt vid riskanalysen
- Övervaka efterlevnad av förordningen avseende fungerande rutiner och åtgärder, ansvarstilldelning, information, utbildning och granskning
- Samarbeta med tillsynsmyndigheten

Kompetensområden

- Hög kompetens på DSF och dess praxis
- God kunskap i nationell lagstiftning som påverkar personuppgiftshantering
- God verksamhetskompetens, speciellt på de processer och organisationsdelar där behandling sker
- God förståelse för riskhantering, informations- och IT-säkerhet
- God kommunikationsförmåga
- God samarbetsförmåga
- Hög integritet

Resurser/förutsättningar

- Ledningens stöd med rapportering direkt till PUA/högsta förvaltningsnivå
- Officiella och tydliga kontaktvägar för alla intressenter
- Tillräcklig tid att för utföra/uppfylla sina skyldigheter
- Tillgång till administrativt stöd, finansiella resurser, teknik, utrustning, personal etc. efter behov
- Ha rätt/möjlighet att samla information för att identifiera personuppgiftsbehandling
- Ha rätt/möjlighet att analysera och kontrollera efterlevnaden av behandlingen
- Ha rätt/möjlighet att informera, ge råd och utfärda rekommendationer till PUA, PUB och andra intressenter
- Ha rätt/möjlighet att upprätthålla sakkunskap
- DSO får inte bli bli föremål för sanktioner eller avsättas på grund av utförande av uppdrag

Oberoende

- PUA /PUB får ej ge instruktioner till DSO angående sitt utövande
- DSO får ej riskera att hamna i intressekonflikt p.g.a. andra uppgifter och skyldigheter
- DSO kan ej bestämma ändamålen och medlen för pu-behandlingen

Dataskyddsombud (DSO) 2 av 2

- DSO för varje PUA (myndigheter *och bolag*)
- Olika behov för olika verksamheter – samma krav på DSO
- Önskemål från verksamheten om en central samordning
- Förslag - en ny kommungemensam intern tjänst
  - Ett antal DSO utgör en egen organisation inom förvaltningen som ansvarar för kommungemensamma interna tjänster
  - Verksamheterna delas in i grupper med närliggande typer av pu och pu-behandlingar
  - Varje grupp får en ansvarig DSO som tecknar uppdragsavtal med respektive verksamhet
  - Främjar kostnadseffektivitet, kompetens, samarbete, effektivitet och utveckling samt DSO:ns integritet och självständighet gentemot PUA

Konsekvensbedömning (= Riskanalys)

- DSF använder begreppet ”konsekvensbedömning” för det som i PuL beskrivs som ”beaktande av särskilda risker”.
  Bägge skrivningarna innebär i praktiken att man måste sätta säkerhetsåtgärderna i förhållande till riskerna med en pu-behandling
- Vissa skrivningar i DSF ger uttryck för att denna typ av bedömning/analys ska genomföras om man misstänker en hög risk, andra skrivningar tydliggör att säkerhetsåtgärderna alltid ska sättas i relation till riskerna
- Oavsett så innebär skrivningarna i praktiken att en riskanalys alltid behöver genomföras för att säkerställa pu-behandlingen vilket ligger i linje med Stadens styrsystem att säkerhetsarbetet ska utgå från riskanalyser
- Riskanalysen ska utgå från verksamhetsnivån (process) där pu hanteras (inte IT-system eller annan ”delmängd”)
- Dataskyddsombudet ska rådfrågas och övervaka analysen
- Det är PUA som ansvarar för att utföra analysen

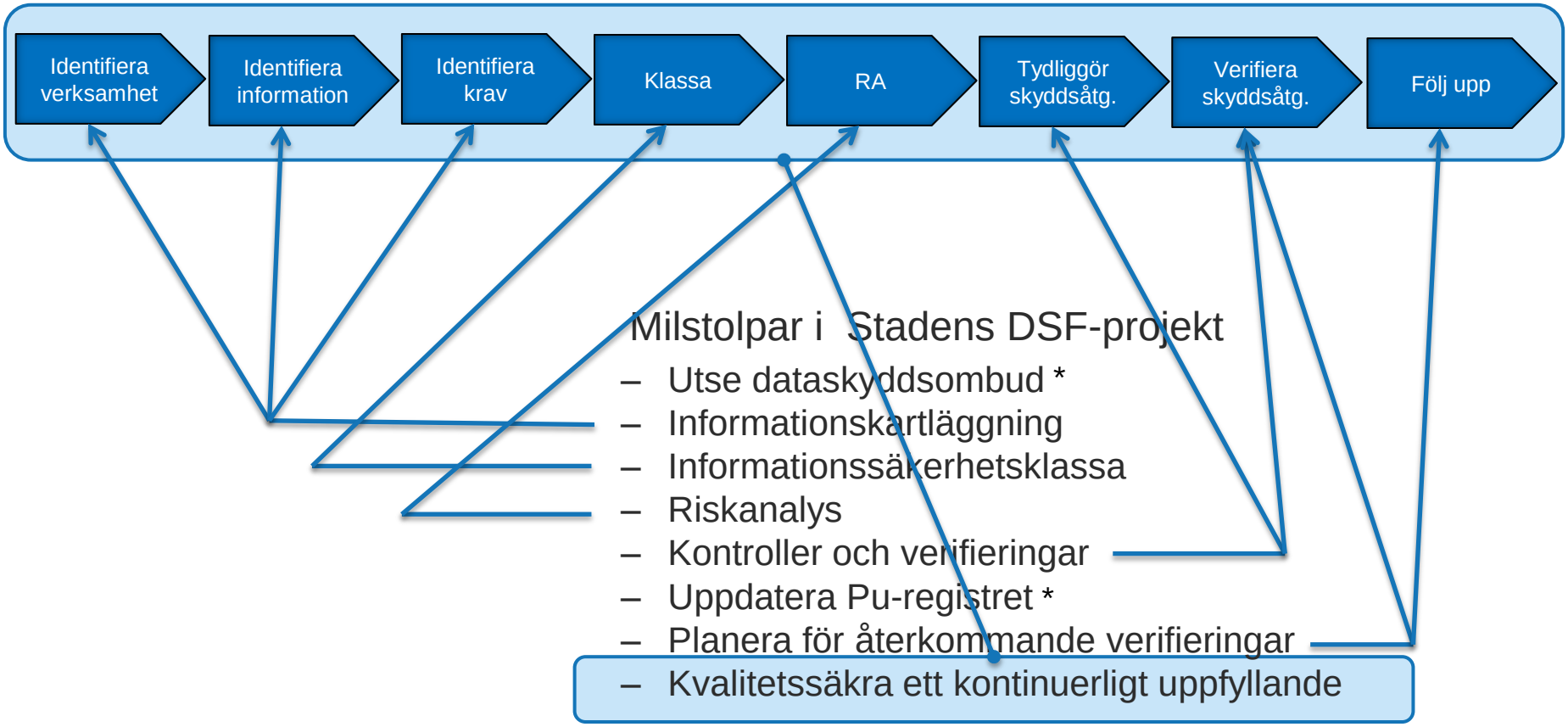
Inbyggt dataskydd/Dataskydd som standard

Privacy by design / Privacy by default

Stadens förhållningssätt *(del av ny policy/riktlinje)*

- Säkerheten (=dataskyddet) baseras på genomförda informationssäkerhetsklassningar och riskanalyser för att på så sätt finnas med redan från den initiala planeringen och täcka såväl tekniska som organisatoriska åtgärder
- Stadens grundsäkerhetsnivå för informationssäkerhet (nivå 1) gäller för pu-behandling generellt och nivå 2 för känsliga/särskild pu avseende konfidentialitet och riktighet
- Uppgiftsminimering, lagringsminimering, fritextfältsmimimering och åtkomstbegränsning är grundläggande krav för all pu-behandling
- Om möjligt alltid använda pseudonymisering, anonymisering eller kryptering även på nivå 1

Skapa följsamhet mot DSF



= Tillämpa Stadens styrsystem

* enligt policy & riktlinje

Stadsövergripande DSF-projekt

- Projekt för att stödja och underlätta för Stadens verksamheter att anpassa sig till DSF
  - Analysera och redovisa behovet av ändringar i Stadens styrsystem
  - Identifiera de nya krav som DSF kommer att medföra för verksamheten
  - Utarbeta stadenövergripande beslutsunderlag
  - Ta fram stadengemensamma stöddokument och checklistor
  - Erbjuda informationsmöten och tillhandahålla utbildning till nyckelpersoner
  - Ej genomförande – respektive verksamhet ansvarar för genomförandet för att uppnå följsamhet mot DSF
- Styrgruppsrepresentanter från bolag, förvaltningar och stiftelser
- I respektive verksamhet finns det en utsedd *Ansvarig genomförare* för den operativa realiseringen (projektets primära målgrupp)
- > 500 operativa projektdeltagare utbildade till dags dato

Göteborgs Stad

Tack för visat intresse!

Jan.A.Svensson@stadshuset.goteborg.se