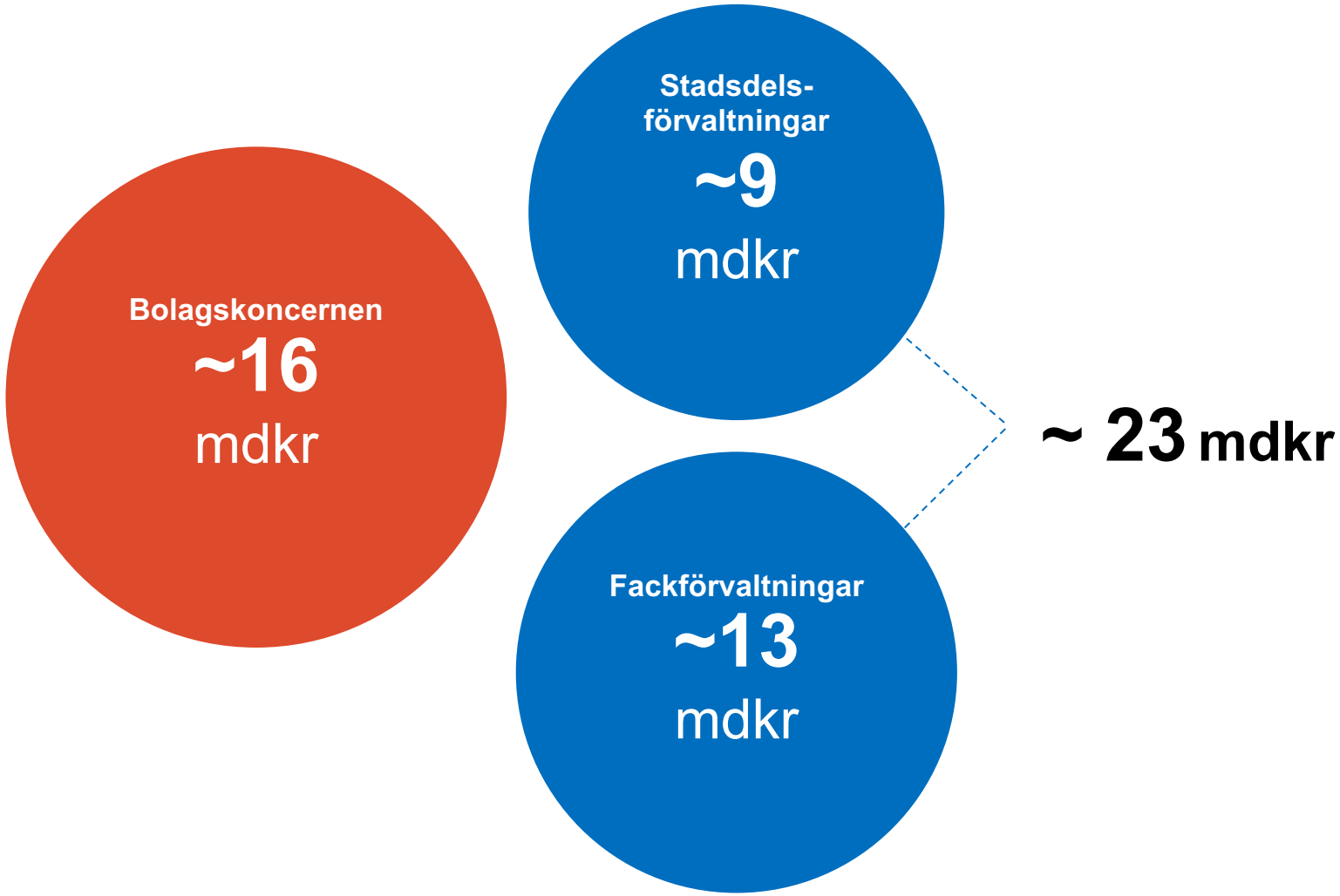
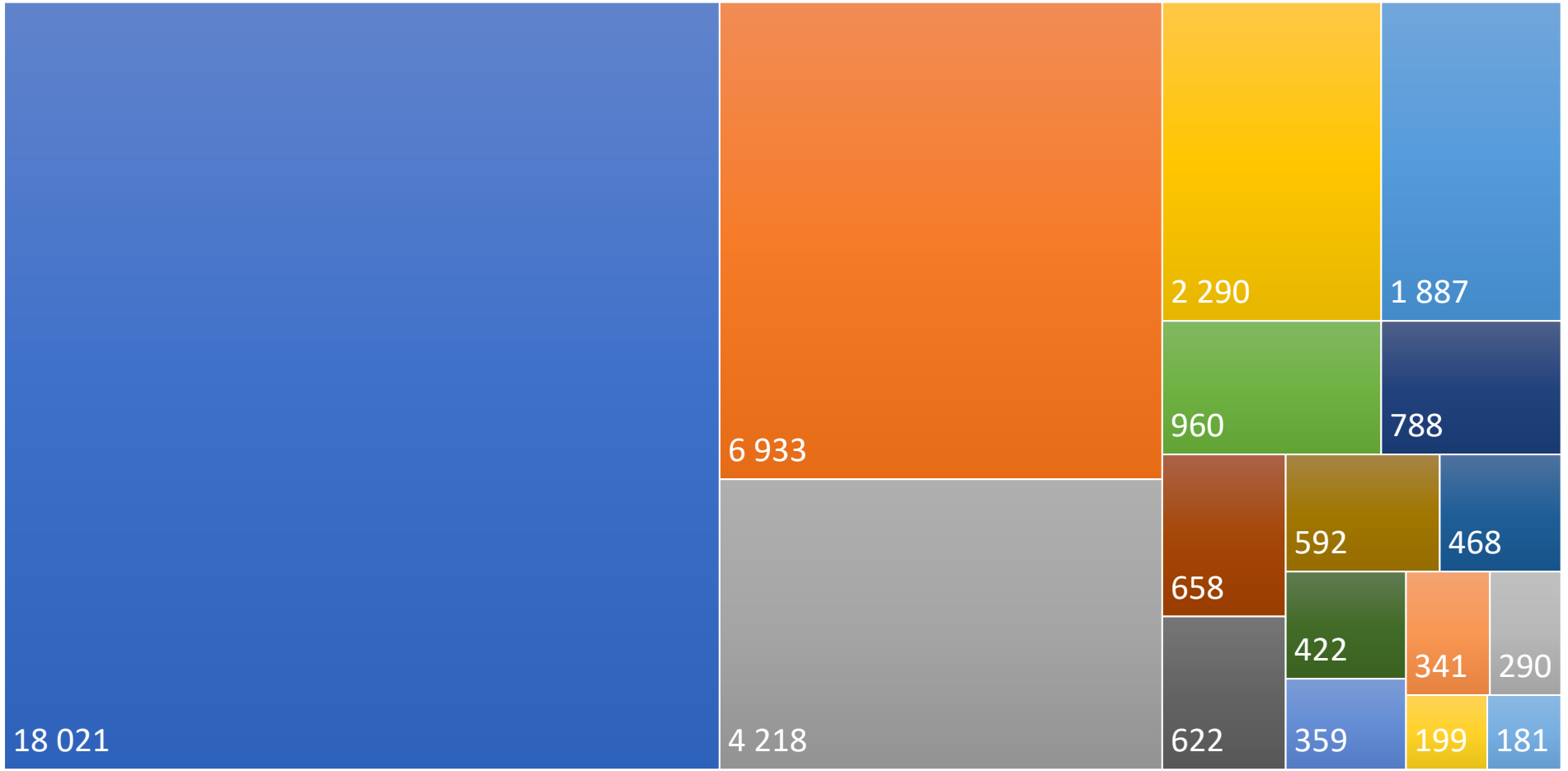
Tredjelandsöverföringar, Schrems II och krav vid upphandling

SOI: s årskonferens 2021-11-10

Staden köper varor och tjänster för totalt ~39 miljarder kr under år 2019[1]



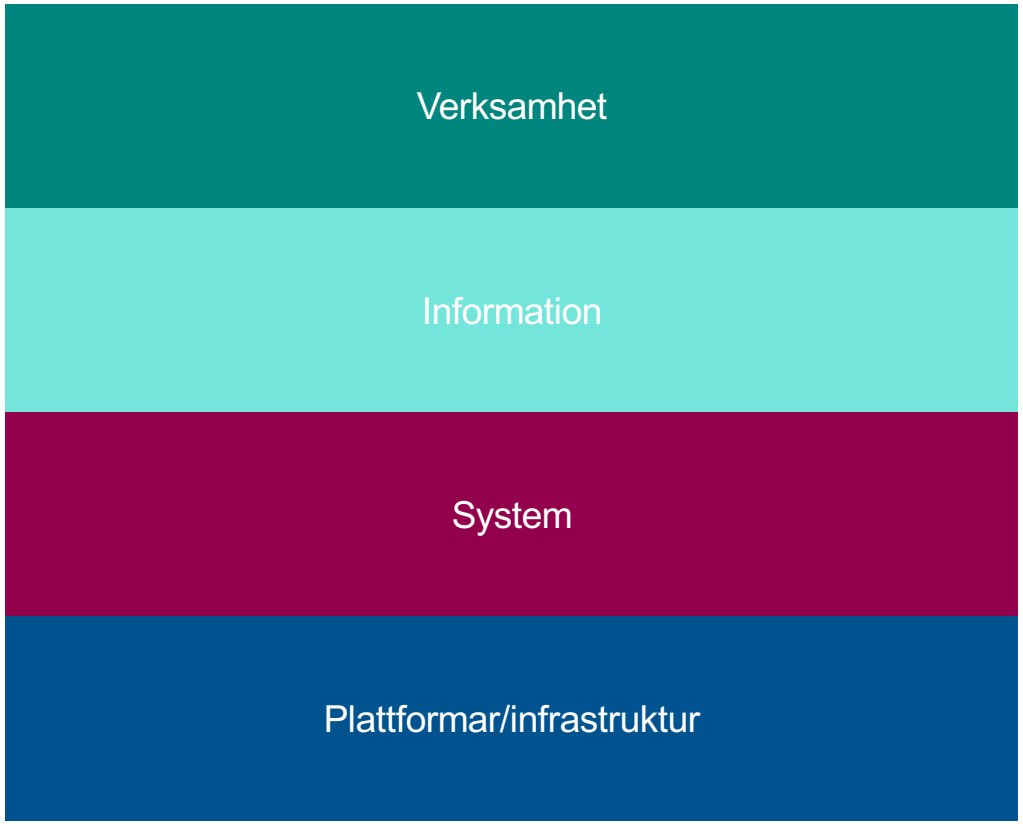
Kategorifamiljer 2020 i Mnkr



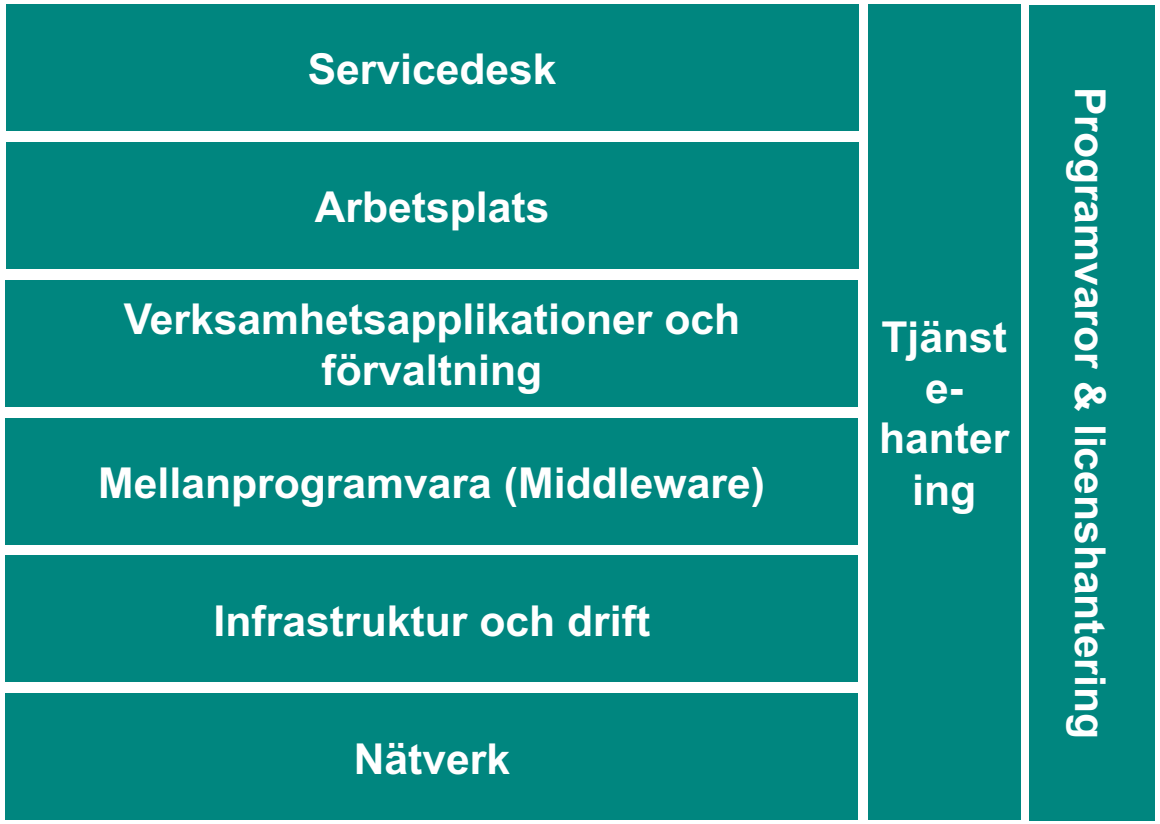
- Anläggning Bygg och Mark
- Vård och omsorg
- Lokal och FM
- IT och Kommunikation
- Drift och Underhåll
- Externa tjänster
- Avfall och Sanering
- Måltider och livsmedel
- HR
- Anläggningsmateriel
- Förbrukningsmateriel
- Resa och Konferens
- Logistik
- Kommunikation
- Maskiner och Fordon
- Medborgarutveckling
- Litteratur

Stockholms stad

Stockholms stads it-verksamhet



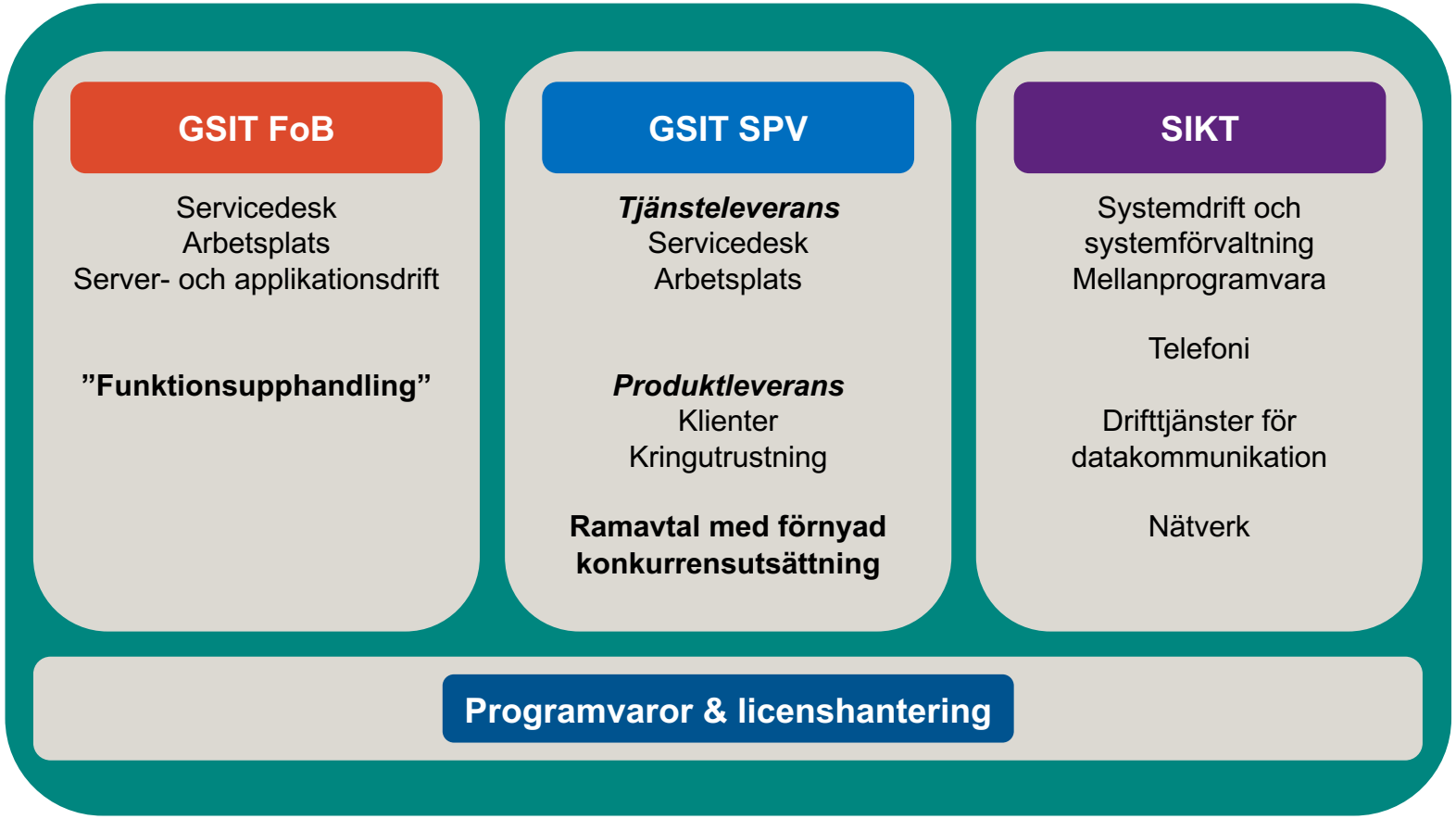
Standardiserad modell för paketering av it



Stockholms stad

Avtal inom it-området – inköpsenhetens uppdrag

Majoriteten av stadens centrala it-leverans är utlagd på entreprenad och köps som tjänst fördelat på flera olika avtal och leverantörer.



Tredjelandsöverföringar

Vad är problemet med molntjänster? Och viktiga begrepp.

- USA: s lagstiftningar Cloud act och Foreign Intelligence Surveillance Act (FISA), avsnitt 702.
- Grundläggande rättigheter i EU-stadgan
- GDPR
- Schrems II – privacy shield inte adekvat skydd
- EU – kommissionen
- Europeiska dataskyddsstyrelsen (EDPB)
  - Vägledning
  - Standardavtalsklausulerna

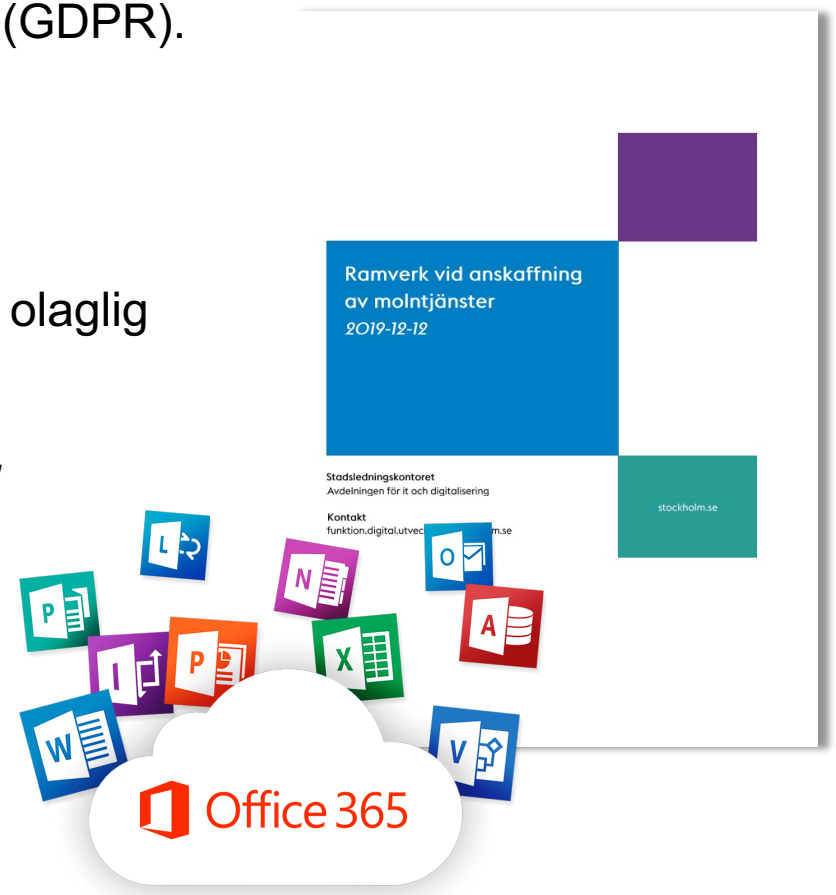
Stockholms stad

Först…

Vi pratar egentligen inte om ”moln” här, vi pratar om tredjelandsöverföringar av sekretessbelagd information (OSL) och (framför allt) personuppgifter (GDPR).

Hur långt måste vi gå? Är t.ex. en IP-adress en personuppgift och en olaglig överföring? Vissa tolkningar av lagen ger i praktiken orimliga effekter.

”Är vår användning av Android och iPhone i vår verksamhet olaglig?”



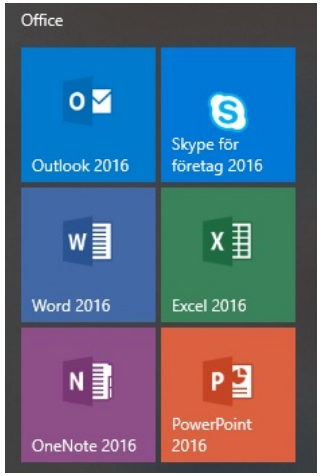
Stockholms stad

Läget i Stockholms stad (mycket förenklat beskrivet)

- Pedagogisk verksamhet

Vill behålla

- Övriga förvaltningar och bolag



Vill ha!!!

Stockholms stad

Max Schrems och Non Of Your Business

None of your business (NOYB) är en privacy-organisation som drivs av den österrikiske advokaten Max Schrems.

Har lett till Schems I och Schrems II (EU-domstolen C-311/18)

At its core, this case is about a conflict of law between US surveillance laws which demand surveillance and EU data protection laws that require privacy.

Citat från NOYB:
”While it is politically clear that there will be no new ”Privacy Shield” or ”Safe Harbor” in the near future, many companies seem to continue to bury their heads in the sand.”

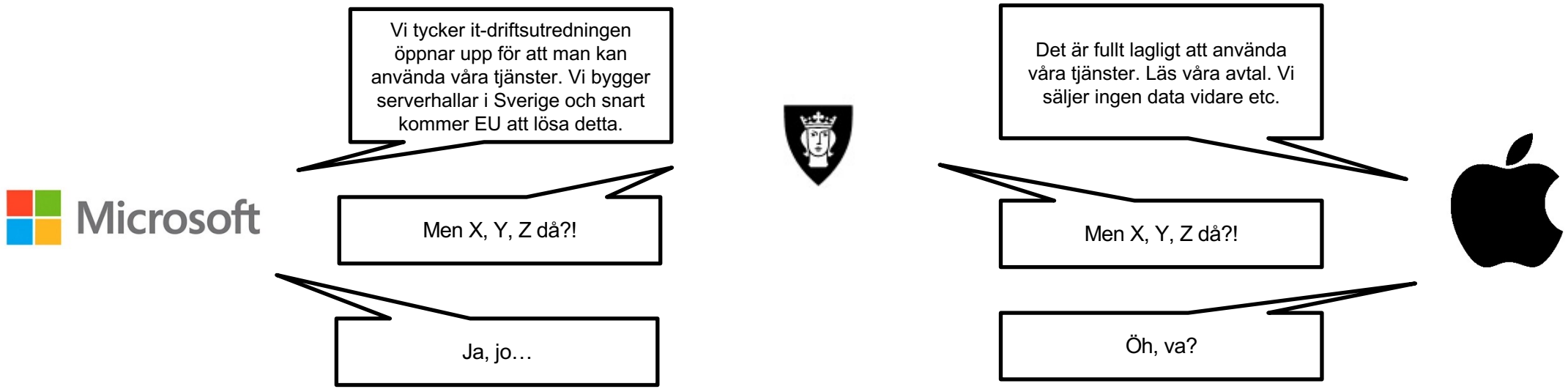
”Even many lawyers and ”experts” ignore the clear statements of the CJEU and claim that everything is fine as long as one enters into Standard Contractual Clauses (”SCCs”) with the data recepient – a complete misjudgement of the situation, which can cost companies dearly.”

Hur ska varje offentlig aktör kunna säkerställa att allt görs rätt?

- Offentlig sektor i stort famlar i mörkret…
  - Hur ska vi ta oss ur detta (vilken är vägen framåt i vårt digitaliseringsarbete)?
  - Hur säkerställer vi efterlevnad av GDPR?
  - Förstår vi ens var problemen finns?
  - Hur ska vi hantera våra leverantörer?
  - Hur ska vi kravställa i våra upphandlingar?

Stockholms stad

Leverantörsmarknaden



Stockholms stad

Vägen framåt?

En av fem saker kan/måste hända (eller?)….

1. EU ändrar sin lagstiftning
2. USA ändrar sin lagstiftning
3. Leverantörerna ändrar sina företag och/eller leveransmodeller
4. Vi väljer konkurrerande tjänster och/eller utvecklar i egen regi
5. Vi slutar digitalisera offentlig sektor på detta sätt

Just nu befinner vi (offentlig sektor) oss i ett slags limbo i väntan på att ”något ska hända”.

Stockholms stad

Vad har hänt efter Schrems II?

Europeiska Dataskyddsstyrelsen
Lämnat rekommendationer avseende bedömningen av överföring till tredje land. Slutlig version (2.0) fastställd 18 juni 2021.

EU-kommissionen
Nya standardavtalsklausuler (som i vissa fall kan användas vid överföring till tredje land) antagna 4 juni 2021

Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1)
Delbetänkande från It-driftsutredningen, 15 januari 2021.
Två skarpa lagförslag som föreslås träda i kraft den 1 januari 2022.

Skatteverket/Kronofogdemyndigheten – Beslut och PM (2021-05-03)
Avstår att använda Teams

IMY:s förhandssamråd om Azure AD och Teams – Stockholms stad (2021-06-02)
Råd: Inför inte tjänsterna Azure AD och Teams

Tredjelandsöverföring av personuppgifter – hur ska vi kravställa?

Juridiska och praktiska utmaningar vid upphandling

Problemställningen eller rättare sagt problemställningarna

Dataskyddsförordningen (GDPR)
Som personuppgiftsansvarig ansvarar varje verksamhet för att varje behandling av personuppgifter är laglig.

Utgångspunkt är att överföring av personuppgifter till tredje land är otillåtna (dvs. utanför EU/EES).

Undantag medges t.ex. när jurisdiktionen där mottagaren är belägen anses erbjuda en adekvat skyddsnivå, uppgifterna omfattas av ett lämpligt instrument för överföringen eller ett uttryckligt undantag är tillämpligt.

Offentlighets- och sekretesslagen (OSL)
Innan verksamheten gör sekretessreglerade uppgifter tillgängliga för en leverantör, måste Staden bl.a. analysera om detta innebär ett **röjande** av uppgifter i den mening som avses i offentlighets- och sekretesslagen.

Överföring av personuppgifter till tredje land (GDPR)

Vad omfattas i begreppet överföring?

Lagring/faktisk överföring till tredje land.

Uppgifterna blir tillgängliga för någon i tredje land.

Även **risken** för att den som behandlar personuppgifter kan behöva tillhandahålla uppgifterna till ett tredje lands stat, myndighet eller motsvarande behöver beaktas. Det kan t.ex. gälla om en leverantör/personuppgiftsunderbiträde ägs av bolag med säte i tredje land.

Överföring av personuppgifter till tredje land (GDPR)

Adekvat skyddsnivå – Bestäms av EU-kommissionen

Länder som idag anses ha adekvat skyddsnivå:

Andorra	Argentina
Bailiwick of Guernsey	Färöarna
Isle of Man	Israel
Japan	Jersey
Nya Zeeland	Schweiz
Uruguay	Storbritannien

Kanada, om deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling.

Standardklausuler (Standard Contractual Clauses, SCC)

- Nya standardavtalsklausuler antagna 4 juni 2021 av EU-kommissionen
- Tillägg till personuppgiftsbiträdesavtal och instruktioner.
- Klausulerna får inte ändras, men tillägg kan göras.

- **Problem**: Binder endast avtalsparterna och inte ett lands myndigheter.
  - Klausulerna måste i det enskilda fallet ge en skyddsnivå som ger en ”väsentligen likvärdig skyddsnivå” för registrerade som den som finns i unionen. Andra lämpliga åtgärder kan vara nödvändiga

Stockholms stad

Överföring av personuppgifter till tredje land (GDPR)

Vad kan göras?

Europeiska Dataskyddsstyrelsen (EDPR) har kommit med rekommendationer:

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
- Innehåller 6 steg

Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
- Innehåller 4 principer

Stockholms stad

EDPBs 6-stegsprocess

1. Ta kontroll över tredjelandsöverföringarna, kartlägg och förteckna
2. Identifiera vilka verktyg som används. Ex. beslut från EU-kommissionen om ”adekvat skyddsnivå” eller standardavtalsklausuler?
3. Bedöm om mekanismen ger ett väsentligen likvärdigt skydd som det som garanteras inom EU
4. Kompletterande skyddsåtgärder bedöms och fastställs. [Avtalsmässiga, organisatoriska och tekniska]
5. Vidta alla steg som behövs för att implementera effektiva kompletterande åtgärder
6. Utvärdera med jämna mellanrum utvecklingen i det tredje landet till vilket persondata har överförts

Överföring av personuppgifter till tredje land (GDPR)

De 4 principerna

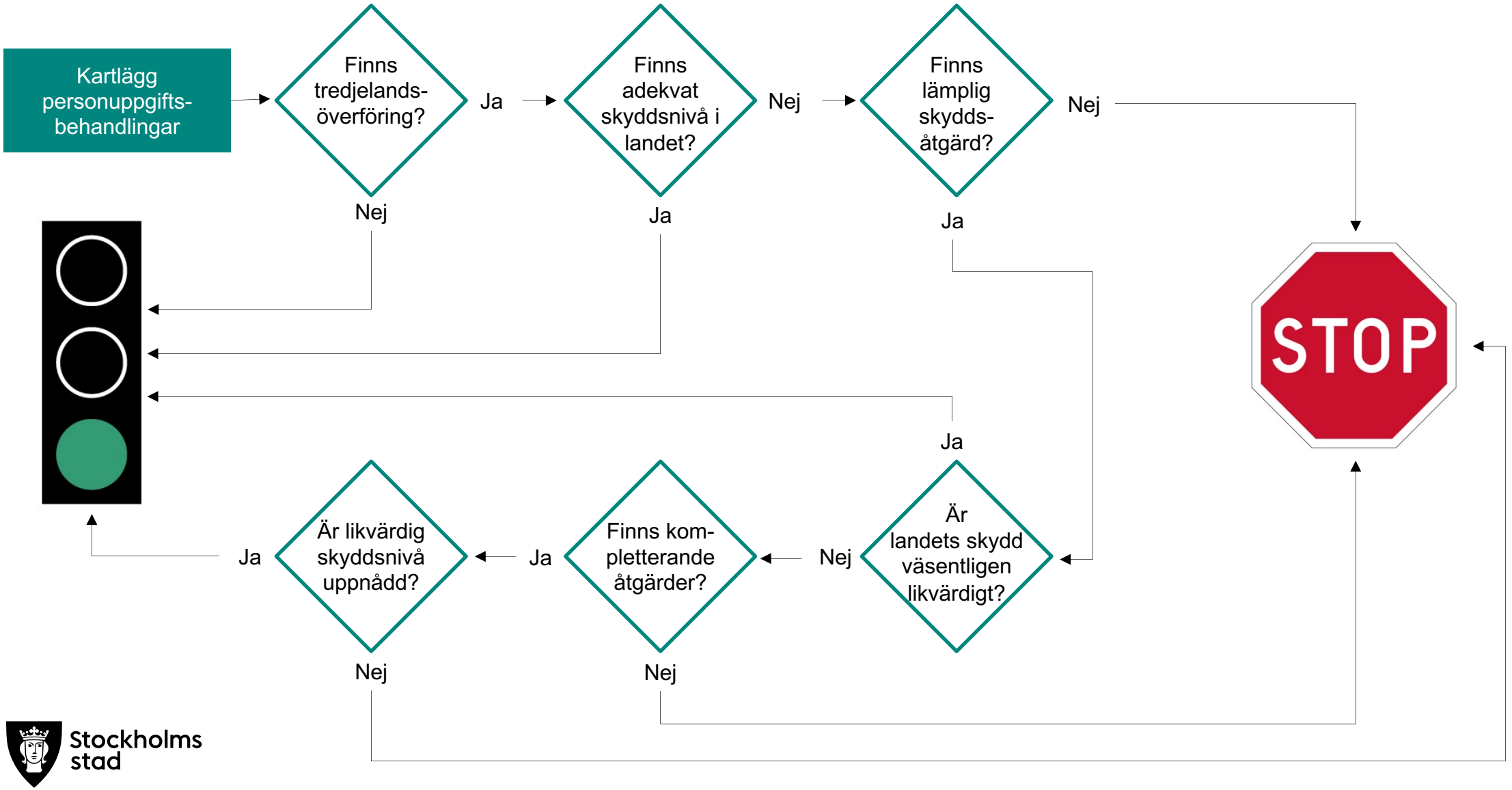
A. Processing should be based on clear, precise and accessible rules.

B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.

C. An independent oversight mechanism should exist.

D. Effective remedies need to be available to the individual.

Personuppgiftsbehandling i tredjeland

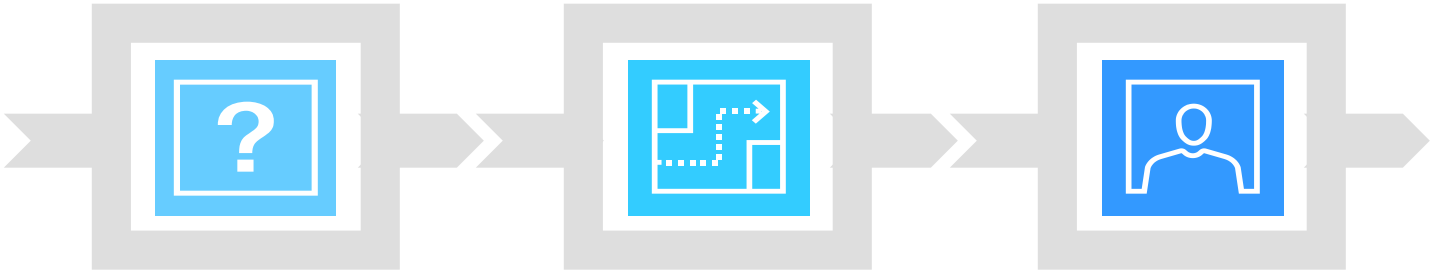


Stockholms stad

Arbetsgång Särskild Prövning

Motsvarar relevanta steg enligt EDPB *”Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”*, vilket även Stadens egen rekommenderade process baseras på.

Dokumentera



Analys Inhämtad info (Kravspecifikation)

Ställda frågor till huvudleverantör:

- Sker, eller finns risk för att det kommer att ske, överföring av personuppgifter till tredje land?
- Nyttjas ev. underbiträden? Vilka juridiska personer? Deras juridiska hemvist (land)?
- Kommer personuppgifter att någon gång, i något sammanhang, för någon individ finnas tillgängligt i klartext?
- Om överföring sker, vilka skyddsmekansismer använder leverantören (kontraktuellt, tekniskt, organisatoriskt)?
- På vilket sätt anses skyddsmekanismerna utgöra en nivå som motsvarar GDPR (adekvat dataskydd)?

Analysera (Utvärdera anbud)

- Beskrivna tekniska, organisatoriska och kontraktuella åtgärder
- Huvudleverantörens och underbiträdens nationella lagstiftning (kan ev. påverka dataskyddsnivån i förhållande till GDPR); **extern juridisk kompetens**

Gap nationell lagstiftning / GDPR

Värdera och riskbedöm (TIA)

- Personuppgifternas klassning (inkl. ev. känsliga, OSL, etc.)
- Tillfällig/löpande överföring
- Finns avtal med EU om adekvat säkerhetsnivå?
- Om avtal inte finns, kan SCCs tillämpas?
- Utgör de tänkta tekniska och organisatoriska skyddsåtgärderna tillsammans med SCC adekvat skyddsnivå?
- Om inte, vilka andra kontraktuella, tekniska och organisatoriska åtgärder föreslås och kan de anses uppnå adekvat skyddsnivå?
- Kvarvarande risk?

Ta fram förslag till rekom-mendation

- Diskussion av analysunderlag och utkast till rekommendation (iterationer).
- Överlämna rekommendation till Operativ Styrgrupp.


Stockholms stad
Tack!