

# Välkommen till Delphi Tech Day

Advokatfirman Delphi

21 september 2023

**Delphi**

# Delphi Tech Day

21 september 2023

# Välkomna till Advokatfirman Delphi och Delphi Tech Day



John Neway Herrman

Delphi



# Delphi Tech Day

21 september 2023

## IT-avtalet

Tips för en bra avtalsprocess



Agne Lindberg

Delphi



**Delphi**

# Tips för en bra avtalsprocess och ett effektivt avtal!

Agne Lindberg, Advokatfirman Delphi

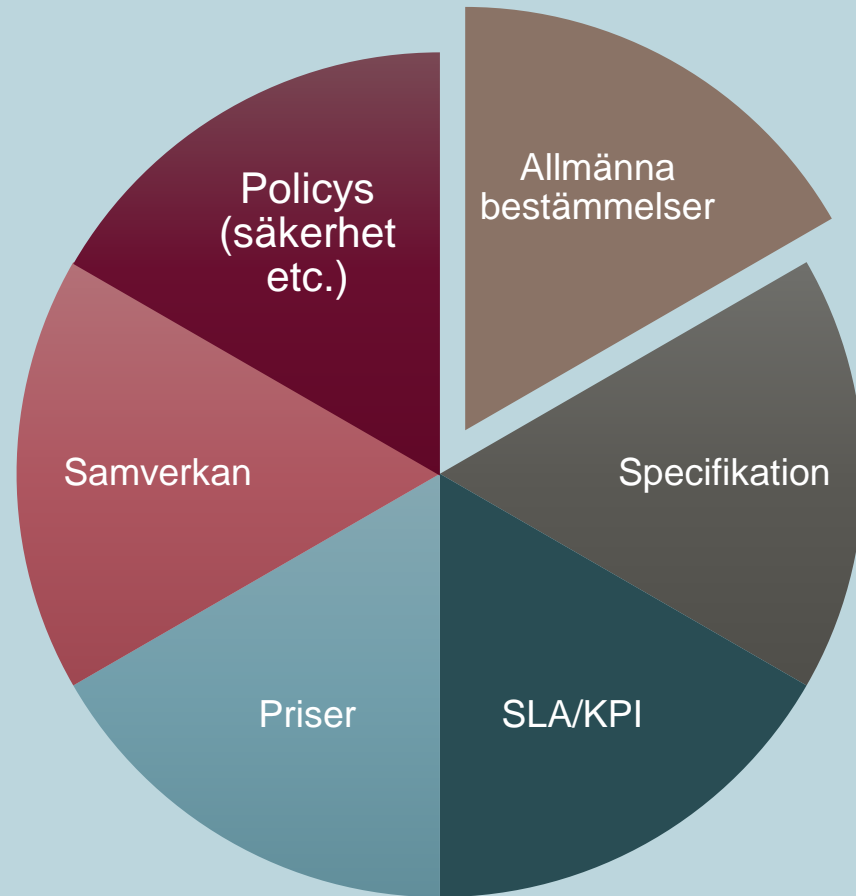
# Topplista för utmaningar i IT-avtal!

- No 1 – Scope / omfattning: Ingår / Ingår inte. Även kopplat till prismodell.
- No 2 – Inlåsnings till leverantör / teknik
  - Exit
- No 3 – Flexibilitet och innovation – utveckling eller förvaltande leverans?
- Viktiga lärdomar – använd dessa i kravställande, kontraktutformning och ev förhandling samt förvaltning av avtalet!



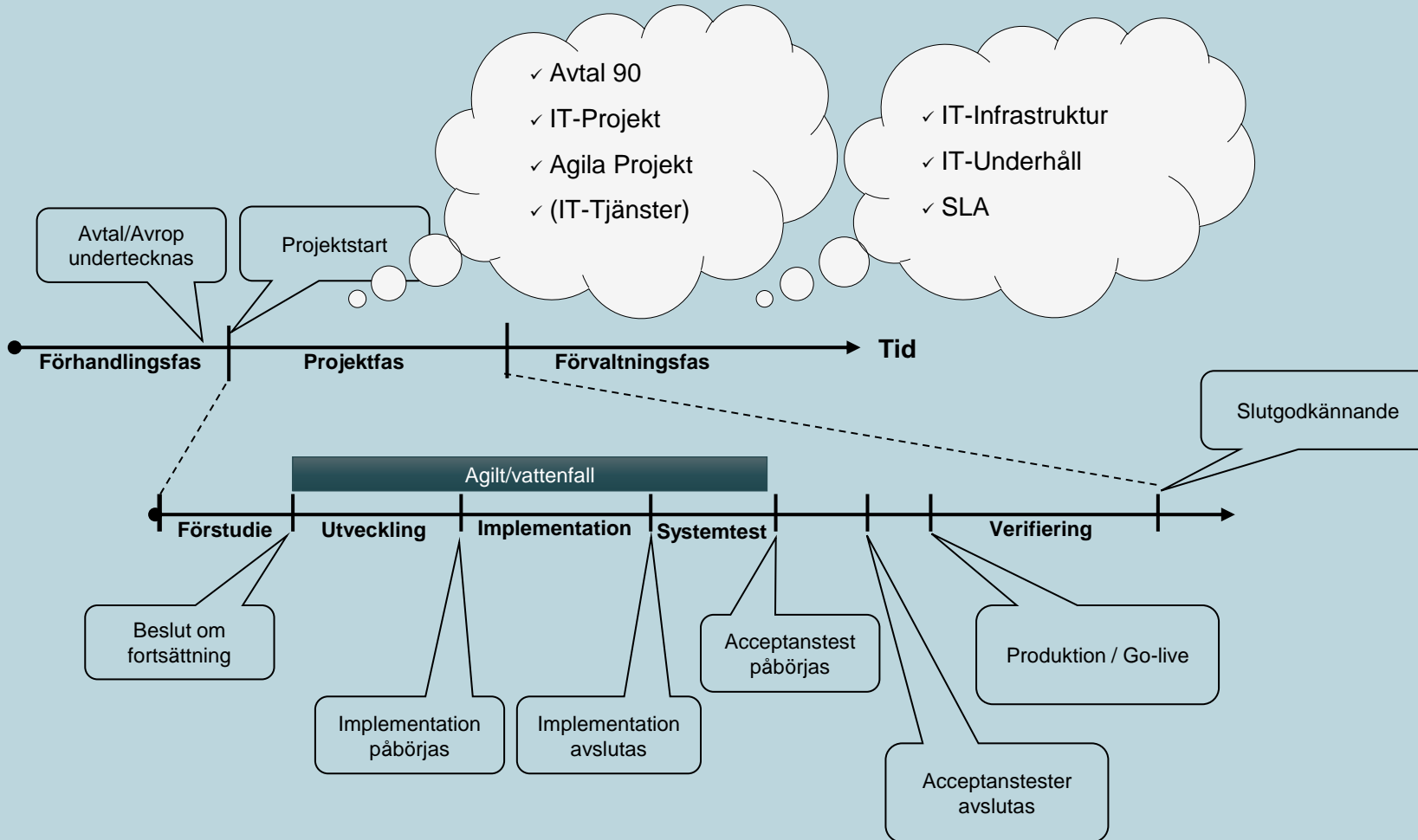


# IT-avtalets beståndsdelar



- Benchmarking
- Exit
- Övertagande
- Finansiella garantier
- Specifika villkor
- Ändringshantering
- UAT-kriterier

# IT-avtalen ur ett projektperspektiv



# Avtalstyp 1 - LEVERANSAVTAL: Projekt vs Resurser

- Grundläggande: Leveransen avgränsad i tid och innehåll.
- Projekt: Leverantören tar ett ansvar för leverabel, projekt och tidplan (Jfr Resursuppdrag)
- Vad är viktigt att reglera:
  - Kravbild på vad som ska levereras
  - När?
  - Verifiering av rätt leverans
  - Dröjsmålsansvar – rätt tid
  - Garantiansvar
  - IP reglering
  - Prismodell – Fast – Budget - löpande



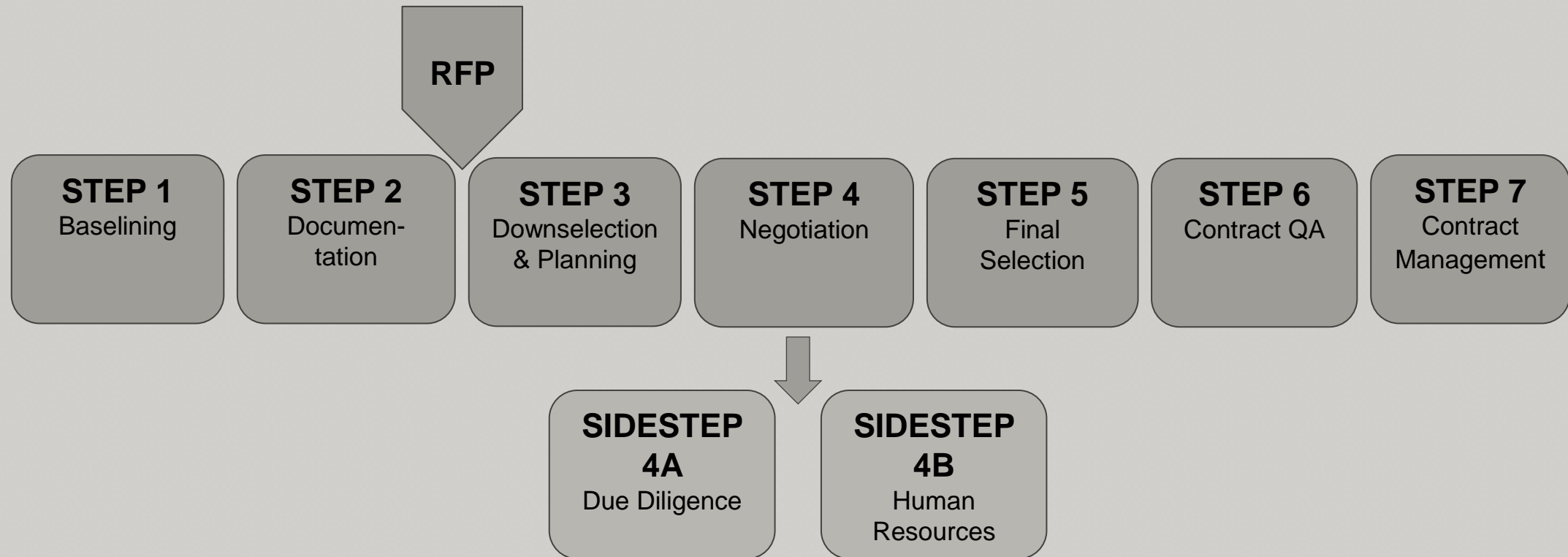
# Avtalstyp 2 – Tjänsteavtalet

- Grundläggande: Leveransen pågår under en längre tid.
- Viktiga villkor:
  - Transition – projektet för att komma till tjänsteleveransen
  - Transformation? – Projektet för att förändra leveransen
  - Tjänstebeskrivningen – vad ska levereras
  - Kvalitetsmått – servicenivåer
  - Flexibilitet – volymer och innehåll
  - Prismodellen – kan innehålla olika modeller för olika tjänster
  - Avtalstid – flexibel
  - IP-reglering. Undvik inlåsnings effekter
  - Reglering av Exit



# Kravställande i ett IT-avtal

# En dokument-fokuserad inköpsprocess (LOU ställer krav!)





# Steg 1 – Baselining

- Kunskap och koncensus om SYFTET. Sourcing strategi?
  - Mål och lösning
  - Kostnad?
  - Förändring?
  - Del av upphandlingsdokument och avtal!
- Det är avtalet som kommer att ge framgång – inte en PowerPoint
  - Arbeta med avtalsdokument från början
  - Risker med att ta in leverantörsdokument?
- Identifiera risker
  - Hur undviker vi risker?

# Steg 1 – Baselining, forts.

- Behov, mål och syfte
- Viktiga parametrar när man skapar baseline – grund för dokumentationsfasen
  - Skalbarhet
  - Flexibilitet eller fast leverans
  - Innovation i leveransen
  - Kostnadseffektivitet
  - Robust IT leverans
  - Samverkansmodell
  - Sanktioner/incitament
  - Avtalstid, "Termination for convenience", uppsägning med grund
  - Transition / Transformation

# Steg 1 – Hur löser man kraven?

- Exempel på hur olika behov kan förverkligas:
  - Innovation: Skapa en "pott" för innovation
  - Kostnadseffektivitet: Ersättningen sänks under avtalstiden. Förutbestämd nivå eller utvärdering?
  - Robust IT leverans: Stark och tydlig samverkansmodell. SLA. Viten?
    - Scope i ett projekt: T ex User Stories, budget, tidsplan
  - Kommersiellt upplägg:
    - Projekt – koppla till milstolpar, leveranser och acceptans
    - Tjänsteleverans: Flexibel. Tydliga priskomponenter.



# Steg 2 – Dokumentation

- Skapa upphandlingsdokumenten. Säkerställ:
  - Skapa underlag för avtalet. Återanvänd dokumentation i avtalet.
- Uppdelning: Vad är krav och vad är utvärdering?
  - Standard eller kundspecifikt? Inspiration:
  - Krav – dokument tas fram av kund:
    - Vilka delar tas fram av leverantör och utvärderas?
    - Leveransen. Kvalitetsmått – SLA
    - Avtalsvillkor – allmänna villkor
    - Prismodell
    - DEFINITIONER!
  - Utvärdering – dokument efterfrågas från leverantör
    - Tjänsteinnehåll / lösningsbeskrivning
    - Servicenivåer – faktiska KPI:er?
    - Transition
    - OBS – behov av synkronisering mot övriga delar i avtalet

# Kravspecifikation – nyckelpunkter

- Krav på en “leverabel” i ett leveransavtal
  - Rätt tid – annars försening. Viktig fråga: När är leveransen fullgjord?
    - Acceptanskriterier / avtalets specifikation?
    - Godkännande?
    - Blame game!
- Krav på leverans av tjänst i tjänsteavtalet
  - Ansvar även på kunden – beroenden? Ansvarsfördelning – RACI tabeller (Responsible, Accountable, Counsulted, Informed)
  - Förändrade behov / regulatoriska krav. Optioner.

# Leveransavtalet – Agila utvecklingsprojekt

- Relation mellan krav / tid / pris
- Vad går in i avtalet? Lista på krav? Backlog eller bas för backlog?
  - Förfining av kraven till “Definition of Ready” – User Stories. Flyttas från backlog till sprint (utvecklingsfas) och utveckling kan påbörjas. Inkluderar beskrivning av funktion.
  - Definition of Done – acceptanskriterier för Sprint.
  - Betydelse av sprint respektive release
    - Låsning efter godkännande?
  - Om inte accept -/ inte tillräckligt med tid – tillbaka till backlog
- Normalt är tid prio 1 – sprintarna är fasta
- Viktiga beslutspunkter:
  - Besluts- och priorätt
  - Incitament - prismodell
  - Förseningsmekanism
  - Exit möjlighet



# Prismodeller för projektavtal

- Löpande räkning
  - Kontroll på resurstyp som används / faktureras
  - Transparent rapportering
  - Ev takpris?
- Fast Pris
  - Särskilt fokus på ändringshantering
- Risk – Reward lösningar
  - Koppla till budget - % av timpriset ovan
  - Exempel: Budget: 2 MSEK
    - Under budget: 120% av timpriset
    - Över budget: 80% av timpriset
- Agila avtal:
  - Teampris
  - Fast pris per ”story point”
    - Kräver att funktioner får en story point

# Exempel Story points

FUNCTIONALITY (USER STORY)	POINT
An employee submits a timecard for the past workweek	5
An employee submits expenses (with receipt) for the past workweek	8
A team manager checks submitted timecards for the past workweek	13
A team manager checks submitted expenses for the past workweek	13
A team manager returns an invalid timecard to the employee for correction	3
A team manager appoints a fall-back for checking timecards & expenses when he/she is unavailable	5
A department manager checks worked hours against contract hours for all employees	20

# Managed Services – tjänsteavtalet

- Tjänstebeskrivning: VAD ska levereras
- SLA/Servicenivåer: Kvalitet på leveransen
- Exempel – 3 nivåer:
  - Övergripande, funktionella krav
  - Statement of Work – aktiviteter. För båda parterna! RACI
  - Servicenivåer



# Managed Services – Servicenivåer

- Koppla till tjänst alternativt övergripande servicenivåer för alla tjänster, exempelvis incident management.
- Mätperiod
- Tillåten nedtid
- Mätmetodik
- Rapporteringskrav
- Konsekvenser
- Modell för viten / incitament
  - Tak
  - Omflyttningsrätt?
- Eskaleringsregler

# SLA Exempel

Service Level Name	Expected Service Level	Measurement Period	Service Hours	Service Level Credit Allocation Percentage (%) (At Risk Amount x Pool Allocation Weighting%)	Subject to Eamback (Y/N)	Definition and Measurement Methodology
Application Availability - Gold	99,90%	Monthly	24*7*365	30,00%	Y	<p>Definition: Availability of the Gold Application and the suppliers ability to "keep them up and running".</p> <p>Algorithm: Total minutes in time period minus adjusted appliaction unavailability minutes for Gold applications in time period. This result is divided by the total minutes in time period.</p>
Resolution of Incidents - Priority 1	100% resolved or workaround provided within 4 hours	Monthly	24*7*365	25,00%	Y	<p>Definition: Restoration of functionality or technical capability, or the successful implementation of a manual workaround (temporary restoration of functionality or a temporary bypass of functionality).</p> <p>Algorithm: (Total Number of Priority 1 Incidents resolved within service level divided by total number of Priority 1 Incidents) multiplied by 100</p>
Resolution of Incidents - Priority 2	95% resolved or workaround provided within 8 hours	Monthly	24*7*365	20,00%	Y	
Response Time - Priority 1 Incidents	95% within 30 minutes	Monthly	24*7*365	10,00%	N	<p>Definition: Response time is defined as starting from the time the Incident notification is received by the Supplier by the respective Incident team to the point to which the Incident is assigned to a nominated resource within Customer's Incident Management System.</p> <p>Algorithm: (Total Number of Priority 1 Incidents responded to within Service Level minutes divided by total number of Priority 1 Incidents) multiplied by 100</p>
Attrition Rate	8,00%	Monthly (on a 12-month rolling average)	n/a	5,00%	Y	
Standard Service Request	92% are delivered within committed timeframes	Monthly	N/A	10,00%	Y	95% are delivered within committed timeframes

# Regulatoriska krav

- Avtalet beroende även av regulatoriska krav
  - Personuppgiftshantering
  - Informationssäkerhet
  - Offentlighet och sekretess
  - M m
- Utgångspunkt: Vilken data / process ska hanteras
- Hur hantera förändringar i kraven?
- Tester / revision

# Prismodeller tjänsteavtalet

- Relation till tjänstebeskrivningen – vad kostar de olika tjänsterna
- Volymbaserade priser – vad är priskomponenten? Definition behövs
  - Överväg priskomponenter som kunden har kontroll över
- Ofta långa avtalstider
  - Benchmarking
  - Index
  - Omförhandling





# Avtalsförvaltning och Exit

# Ändringshantering

- Ändringshantering
  - Skilj mellan:
    - Operativa ändringar
    - Kontraktsändringar
- Process för ändringar
  - Kontraktsändringar – håll avtalsdokumenten uppdaterade. Komplettera med ändringslogg som beskriver ändringen.
    - Arbeta med optioner om möjligt.
  - Vissa ändringar utan leverantörens godkännande?
    - Policies, regulatoriska krav?

# Rapportering

- Servicenivåer, volymer, kostnader, personalförändringar
- Separat bilaga med rapporter – innehåll, mottagare, frekvens, leveranstid

# Eskalering av oenighet

- Del av samverkansorganisation
- Tydlig eskaleringsväg med tidsramar
- Tolkningsföreträde?

# Exit

- Successiv överflyttning? Överflyttningsassistans  
Kostnad  
Tidsperiod (inkl efter Avtalets upphörande)
- Information och dokumentation
- Kundens data
- Stöd i förnyad upphandling / due diligence
- Option att ta över utrustning / avtal
- Förslag: Årlig uppdatering av exit plan





# Agne Lindberg

Advokat/Partner/Head of Tech & IP

Mobil: 0709-25 25 25

E-post: [agne.lindberg@delphi.se](mailto:agne.lindberg@delphi.se)

**Advokatfirman Delphi**

Adress: Mäster Samuelsgatan 17, P.O. Box 1432, Stockholm, Sweden

Telefon: + 46 (0)8 677 54 00

[www.delphi.se](http://www.delphi.se)

# Bensträckare 14.15-14.25

Delphi



# Delphi Tech Day

21 september 2023

## Nyhetspass



**Olivia Svedmark**



**Lovisa Lennström**



**Peter Nordbeck**



**Agne Lindberg**

**Delphi**





Delphi

# Cookies – lärdomar från rättsutvecklingen





# Inledning



# Nuläge

**DIN HÄLSA TILL SALU**

## Apoteket anmäler sig själv efter avslöjandet – berättade om köp för Facebook

3:37 min [Min sida](#) [Dela](#)

Publicerat torsdag 28 april kl 05.00

- Det statliga Apoteket har skickat detaljerade uppgifter om sina kunder och deras webbköp av exempelvis receptfria läkemedel till Facebook, kan Ekot avslöja.
- Apoteket uppskattar att upp till en miljon kunder och besökare kan ha påverkats.
- "Vi vill göra om och vi vill göra rätt", säger Apotekets chefsjurist Anna Rogmark.

Vi går in på Apotekets nätbutik och söker på inkontinensskydd, paracetamol och klamydiatest. Vi ser på varje vara, lägger dem i varukorgen och går till kassa. När vi gör det här besöket har skickat uppgifter till Facebook. En vanlig kund inte ser så

**CPO MAGAZINE** HOME NEWS INSIGHTS RESOURCES

## French Regulator Hits Microsoft With €60 Million Fine Over Bing Cookie Consent

DATA PROTECTION NEWS · 3 MIN READ

SCOTT IKEDA · JANUARY 6, 2023

**PTS**

Bransch Privat Om PTS Kontakt **Press** Bloggen Nya LEK E-tjänster

Start > Nyheter > Internet > 2022 >

## PTS granskar om webbplatsinnehavare bryter kakreglerna

2022-10-07

### Nu inleder Post- och telestyrelsen (PTS) en granskning för att kontrollera om ett antal utvalda webbplatser bryter kakreglerna om kakor.

Kakor, också kallade cookies eller webbkakor, används för att spara eller få åtkomst till information som är lagrad på en användares dator eller mobil.

**PSYKISK OHÄLSA**

## Stödorganisation skickade anonyma användares uppgifter till Facebook

2:15 min [Min sida](#) [Dela](#)

Publicerat lördag 9 april kl 03.02

- Stödorganisationen Mind lovade användarna på sitt internetforum att de skulle få vara anonyma.
- Men Ekots granskning visar att Mind har skickat användares mejladresser och telefonnummer till Facebook.
- "Vi beklagar att vi inte haft kunskap om vad den här typen av funktioner innebär" säger Minds generalsekreterare Karin Schulz.

När vi går in på Minds webbplats får vi veta att "viss information" delas med sociala medieföretag som vi godkänner kakor. Så vi gör det, och registrerar oss på Minds forum där vi möts av löften om anonymitet.

"Mind Forum är en trygg plats på nätet där du anonymt kan prata om livet när det känns tufft."

"Alla våra medlemmar är anonyma och vi har ingen anmälningsplikt."

"OBS! Vi sparar aldrig ditt telefonnummer, det används endast för den här säkerhetskontrollen."

Vi får också ett anonymt alias som vi kan använda för att skriva inlägg.

**Men samtidigt som** vi registrerar oss skickas vårt telefonnummer och vår mejladress till Facebook. Varje gång vi sedan loggar in på forumet, så skickas mejladressen till Facebook igen.

Facebook får inte se vad personen som är inloggad skriver på forumet. Men däremot får Facebook se rubrikerna på de diskussionstrådar vi går in på, till exempel "Jag är rädd" eller "Ensam".

Till och med de anonyma alias som Mind ger sina användare finns bland de uppgifter som organisationen skickar till Facebook.

## Meta hit with \$413 million fine over EU data breaches that hit more than 500m users

The Facebook owner has faced a series of penalties over its behaviour in recent years

Published: January 04, 2023 20:36

AFP



Directed at Facebook's lead privacy regulator in an attempt to circumvent transparent cookie

- Advertisement -

# Begreppet "cookies"

- "Cookies och andra spårningstekniker"
- Samlingsnamn för tekniker som innebär att det lagras eller hämtas information från en enhet
  - Webbplats
  - Mail
  - App
  - Etc
- "cookies", "trackers", "pixlar", etc

-	Name	Value	Domain	Expires / Max-Age
▼ https://reverb.com (18)				
<input checked="" type="checkbox"/>	__ssid	715b3d3123225f0130c451ebf...	.reverb.com	1781897914
<input type="checkbox"/>	ab.storage.deviceId.2da41f3...	%7B%22g%22%3A%22cf7e...	.reverb.com	1687224454
<input type="checkbox"/>	ab.storage.sessionId.2da41f...	%7B%22g%22%3A%2277eb...	.reverb.com	1687224879
<input type="checkbox"/>	reverb_user_shipping_region	SE	.reverb.com	
<input type="checkbox"/>	reverb_user_currency	SEK	.reverb.com	
<input type="checkbox"/>	reverb_user_locale	en	.reverb.com	
<input type="checkbox"/>	reverb_user_country_code	SE	.reverb.com	
<input type="checkbox"/>	_gcl_au	1.1.44726639.1673861938	.reverb.com	1681637938
<input type="checkbox"/>	timezone	Europe/Berlin	reverb.com	1677582208
<input type="checkbox"/>	timezone_offset	1	reverb.com	1677582208
<input type="checkbox"/>	google_cid	1019173518.1655667514	reverb.com	
<input type="checkbox"/>	_fbp	fb.1.1673861939850.171523774	.reverb.com	1682848537
<input type="checkbox"/>	_ga	GA1.1.1019173518.1655667514	.reverb.com	1709632548.819...
<input type="checkbox"/>	reverb_page_views	15	reverb.com	1709632548.725...
<input type="checkbox"/>	_ga_K0VJZSKN23	GS1.1.1675069551.4.1.16750...	.reverb.com	1709632548.819...
<input type="checkbox"/>	elog-analytics-2	{%22lastSeen%22:16750725...	.reverb.com	1709632548.852...
<input type="checkbox"/>	csrf_token	A3my2eoXEhE7lbASR35A4C5...	reverb.com	1706608548.013...
<input type="checkbox"/>	_reverb_session	SWRKSkrNjNDTjI5SmMwc...	reverb.com	

# Cookies användningsområden

- Inställningar och funktionalitet på webbplatser
  - Varukorg på e-handelswebbplats
  - Språk
  - Valuta
  - Etc
- Webbanalys
  - Mätning på webbplats för beteendeanalys
- Marknadsföring
  - Räckvidd
  - Retargeting
  - Målgrupp
  - Attribution
  - Osv



# Två centrala regelverk

Information



Samtycke för icke  
nödvändiga cookies



Compliant med cookielagen

Information



- Laglig grund ex. samtycke eller intresseavvägning
- Överföring tredje land
- Gallringstider
- Etc.



Compliant med GDPR

## Cookielagen (lag om elektronisk kommunikation)

- E-privacydirektiv 2002/58/EG (EPD)
- PTS [information/vägledning](#) från 2022
- PTS tillsynsmyndighet för cookieanvändning



## GDPR

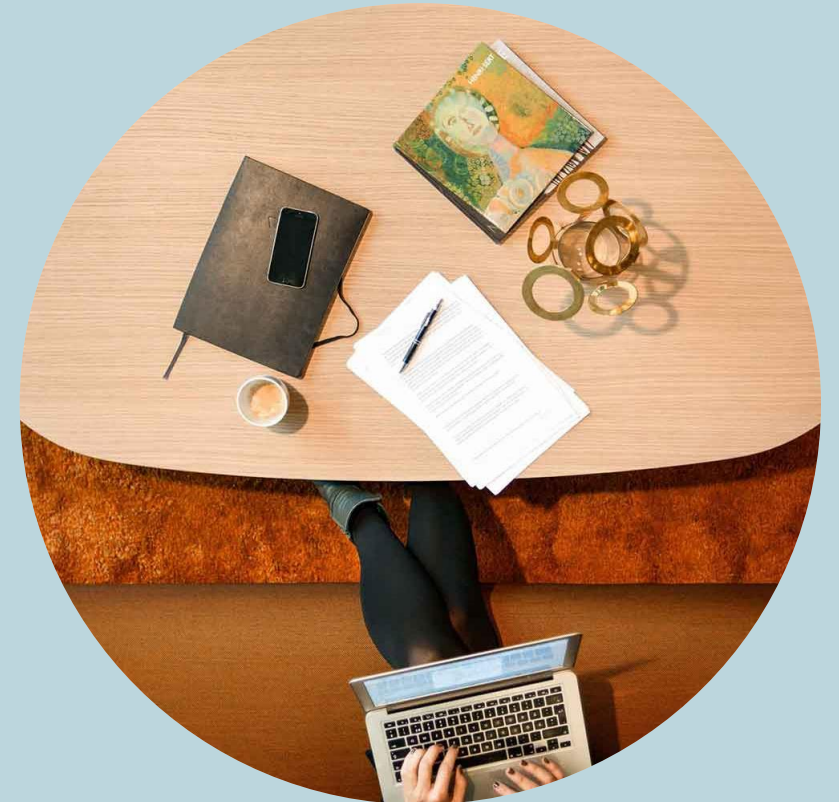
- EDPB/Artikel 29-arbetsgruppen
  - Transparensvägledningen från 2018
  - Vägledning om samtycke från 2020
  - Vägledning om manipulativ design från 2023
  - Cookie banner taskforce från 2023
- IMY är tillsynsmyndighet för personuppgiftsbehandling





# PTS tillsyn

- 2022 inleddes tillsyn mot
  - Swedbank
  - Folkhälsomyndigheten
  - Konsumentverket
  - Tele2
- Underrättelse juni 2023 – PTS misstänker att bolagen inte inhämtar giltiga samtycken enligt cookielagen
  - Lika enkelt att neka lagring och dra tillbaka samtycken som att lämna samtycken
  - Ofullständig information
- Bolagen yttrade sig om vidtagna åtgärder



# IMY tillsyn

- 2020 inleddes tillsyn mot
  - CDON
  - Coop
  - Dagens Industri
  - Tele2
- Överföring av personuppgifter till USA via Google Analytics (version från 2020)
- Juni 2023 kom beslut från IMY
  - Överföring skedde baserat på standardavtalsklausuler utan att bolagen vidtagit tillräckliga skyddsåtgärder
  - Sanktionsavgifter till Tele2 och CDON
  - Samtliga bolag föreläggs att sluta med verktuget (dock ej Tele2 som slutat på eget initiativ)

2023-09-21



Delphi



# Lärdomar

# Samma höga krav på utformning av samtycke

- "GDPR-samtycken"
  - *"frivilligt, specifik, informerad, otvetydig viljeyttring"*





# Frivillig och otvetydig viljeyttring

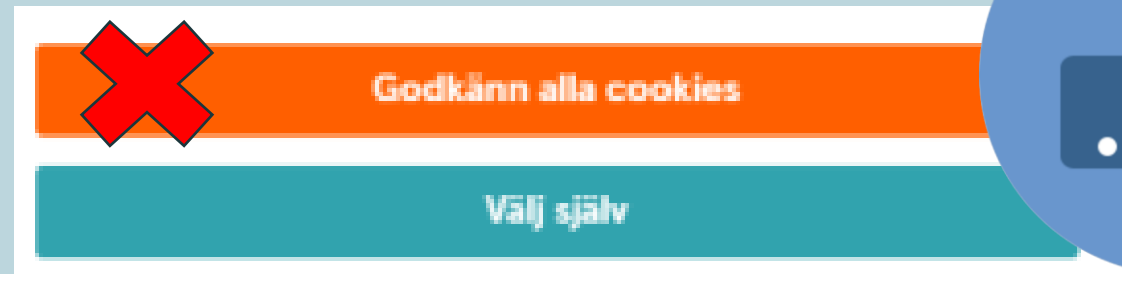
- Aktiv åtgärd för att samtycka
- Ej "förikryssade" samtycken
- Lika enkelt att neka som att samtycka
- Enkelt att tacka nej



Godkänn alla cookies

Godkänn bara nödvändiga cookies

[Välj själv](#)



Godkänn alla cookies

Välj själv



## Denna webbplats använder cookies

Ap... cookies för att webbsidan ska fungera och för att kunna anpassa din upplevelse, samt för att kunna förbättra webbplatsen. De... är både våra egna och tredje... klicka... cookies. Om du vill göra ändringar i hur vi använder cookies, läs mer om vår behandling av cookies och personuppgifter.

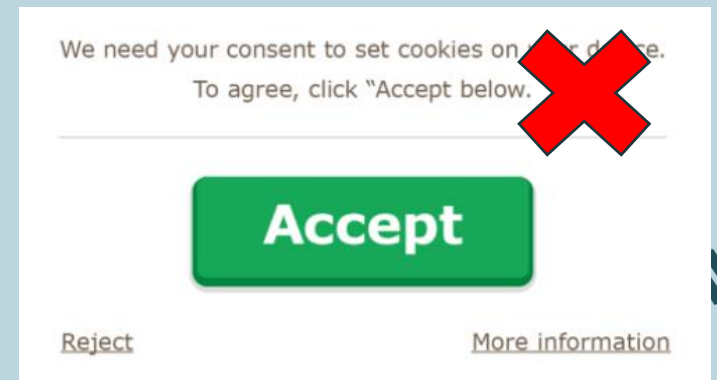
Användning av sajten godkänner cookies för personalisering, trafikanalys och annonser. Data delas med partners. [Läs mer!](#)

Tillåt nödvändiga Tillåt urval Tillåt alla cookies

Nödvändig  Funktionella  Statistik  Marknadsföring

[Visa detaljer](#) ▼

2023-09-21




We need your consent to set cookies on this device. To agree, click "Accept below."

Accept

[Reject](#) [More information](#)

# Specifik viljeyttring

- Separata samtycken för olika ändamål
  - Kan kräva många rutor!
- Baka inte in samtycket i villkor



**Vi värdesätter din integritet**

Vi använder tekniska-, analytiska- och marknadsförings-cookies för att hjälpa dig med saker som att logga in och att återuppta din sökning från där du slutade. Låter det bra?

**Godkänn**

**Nej tack**

---

**Välj individuella kategorier**

Läs mer om vårt användande av cookies här: [Sekretesspolicy](#)



# Återkallande av samtycke

- Ska vara lika lätt att återkalla som att ge sitt samtycke

[Om webbplatsen](#) | [Webbkarta](#) | [Kakor \(cookies\)](#) | [Ändra val för kakor](#)

## Our use of cookies

We use necessary cookies to make our site work. We'd also like to set analytics cookies that help us make improvements by measuring how you use the site. These will be set only if you accept.

For more detailed information about the cookies we use, see our [Cookies page](#). ↗

Accept all cookies

Reject all cookies

## Necessary cookies

Necessary cookies enable core functionality such as security, network management, and accessibility. You may disable these by changing your browser settings, but this may affect how the website functions.

## Analytics cookies

Off

We'd like to collect website analytics information using Silktide to help us improve the website. We collect this data by running Silktide analytics JavaScript on your device, which collects data about how you have interacted with our site. The data is collected in a way that does not directly identify anyone. For more information please see our [Cookies page](#).

Save and close



# Informerad viljeyttring

- Tydlig information om alla cookies och all personuppgiftsbehandling i skikt
- Första lagret – "Cookiebanners"
  - Placeras vid besökarens första besök
  - Här inhämtas samtycken
- Andra lagret – Cookie policy och personuppgiftspolicy
  - Fullständig information om cookie & personuppgiftsbehandling

Privacy  
policy

Cookie  
policy

Cookiebanner

....

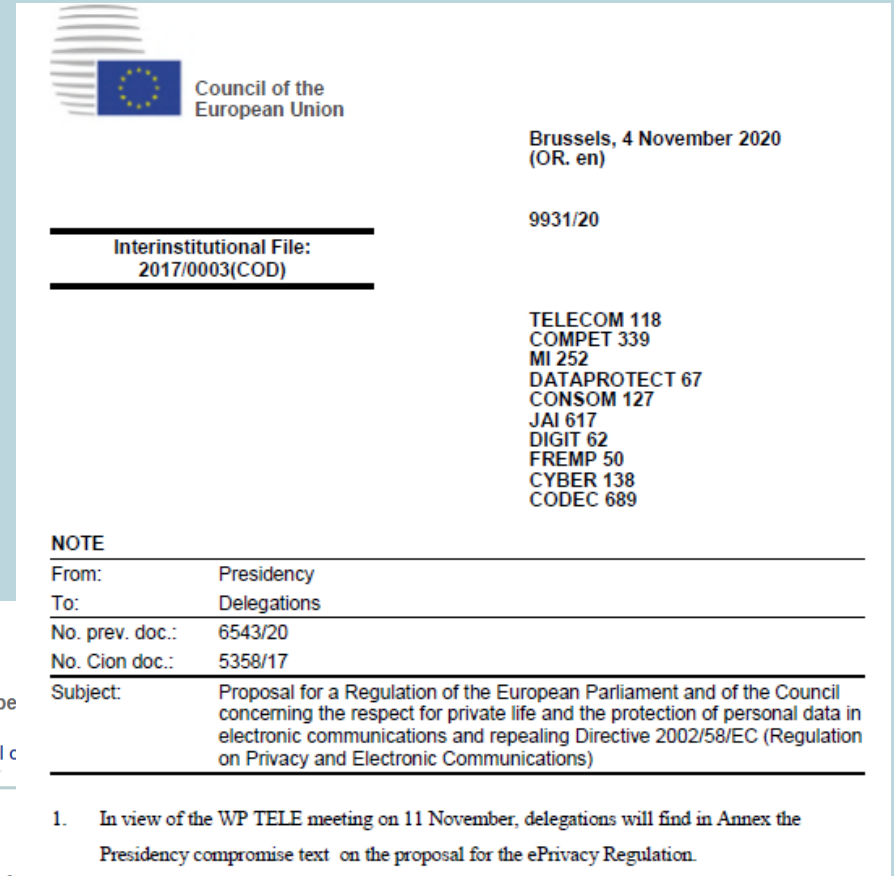
*Här kan du läsa mer om hur vi behandlar dina personuppgifter.*

*Här hittar du information om hur vi använder cookies.*

# Avslutning

- Cookies har olika användningsområden.
- Mycket att tänka på för att vara compliant.
- Många lärdomar senaste åren om vad kraven för giltiga samtycken innebär men mer kommer så följ rättsutvecklingen!
- Viktigt att ha en rutiner kring sin användning av cookies för att säkerställa compliance. Ska legal klarera alla nya funktioner på hemsidan?
- Kommer den potentiella ePrivacyförordningen göra det enklare?

2023-09-21



Council of the European Union

Brussels, 4 November 2020  
(OR. en)

9931/20

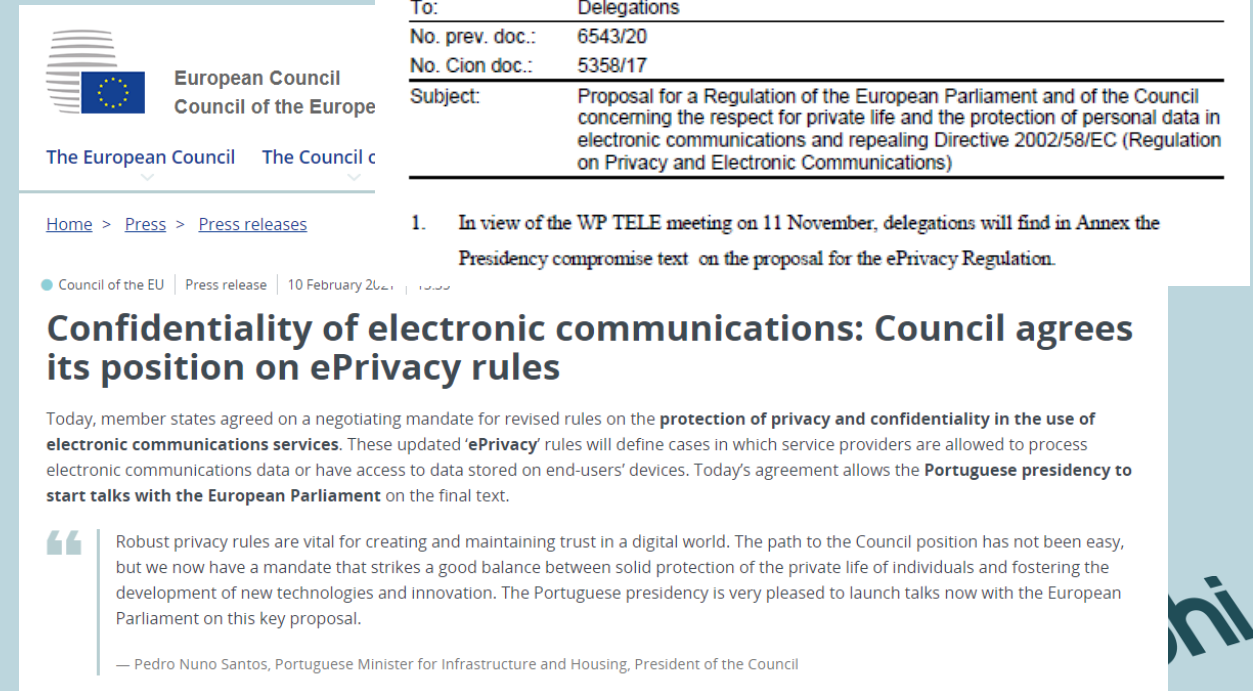
Interinstitutional File:  
2017/0003(COD)

TELECOM 118  
COMPET 339  
MI 252  
DATAPROTECT 67  
CONSOM 127  
JAI 617  
DIGIT 62  
FREMP 50  
CYBER 138  
CODEC 689

**NOTE**

From:	Presidency
To:	Delegations
No. prev. doc.:	6543/20
No. Cion doc.:	5358/17
Subject:	Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

1. In view of the WP TELE meeting on 11 November, delegations will find in Annex the Presidency compromise text on the proposal for the ePrivacy Regulation.



European Council  
Council of the Europe

The European Council The Council of the Europe

[Home](#) > [Press](#) > [Press releases](#)

Council of the EU | Press release | 10 February 2021

## Confidentiality of electronic communications: Council agrees its position on ePrivacy rules

Today, member states agreed on a negotiating mandate for revised rules on the **protection of privacy and confidentiality in the use of electronic communications services**. These updated 'ePrivacy' rules will define cases in which service providers are allowed to process electronic communications data or have access to data stored on end-users' devices. Today's agreement allows the **Portuguese presidency to start talks with the European Parliament** on the final text.

“ Robust privacy rules are vital for creating and maintaining trust in a digital world. The path to the Council position has not been easy, but we now have a mandate that strikes a good balance between solid protection of the private life of individuals and fostering the development of new technologies and innovation. The Portuguese presidency is very pleased to launch talks now with the European Parliament on this key proposal.

— Pedro Nuno Santos, Portuguese Minister for Infrastructure and Housing, President of the Council

**Delphi**

**/ We love challenges**





Delphi

# Överföring av personuppgifter till länder utanför EU/EES

Peter Nordbeck

# Bakgrund – gammalt och nytt

- Schrems II juli 2020
  - EU-domstolen underkände Privacy Shield
  - Standardavtalsklausuler fortfarande möjliga att använda
  - Men - undersökning av lagen/rättstillämpningen i det tredje landet
- EDPB:s rekommendationer
  - Första versionen november 2020
  - Andra versionen juni 2021
  - "TIA"
- Nya standardavtalsklausuler juni 2021
- Microsoft EU Data Boundary januari 2023
- AWS Dedicated Local Zones augusti 2023
- Mycket fokus på överföringar till USA



# European Union–U.S. Data Privacy Framework

- Principöverenskommelse i mars 2022
- Förhandlingar mellan EU och USA
- Executive Order i oktober 2022
- Kritiska remissinstanser
- EU-kommissionen fattar beslut om adekvat skyddsnivå för USA i juli 2023
  - Gäller för överföringar till organisationer som anslutit sig till ramverket
  - Överföringar kan ske utan krav på skyddsåtgärder som t.ex. standardavtalsklausuler
  - Inga krav på ytterligare skyddsåtgärder

# Konsekvenser av adekvansbeslutet

- Adekvansbeslutet gäller för överföringar till USA
- Alltjämt krav på att göra en TIA vid överföringar till andra tredje länder
- Adekvansbeslutet gäller bara för överföringar till de organisationer som anslutit sig till ramverket
  - Bör vara mindre problematiskt i de flesta fallen – alla de stora leverantörerna lär delta
  - För mindre leverantörer som inte anslutit sig – bedömningar som EU-kommissionen gjort i adekvansbeslutet betydelsefulla vid upprättandet av en TIA
  - Undersök om leverantören finns med på listan!
- Adekvansbeslutet vs IMY:s beslut om Google Analytics
  - IMY:s invändningar får anses omhändertagna genom adekvansbeslutet

# Praktiska utmaningar med adekvansbeslutet

- Supporttjänster och andra tjänster kan tillhandahållas från andra tredjeländer än USA
- Vad gäller i en sådan situation?
  - Vem ansvarar för att säkerställa att supportleverantören behandlar personuppgifter i enlighet med ramverket och GDPR?
  - GDPR artikel 44
  - Avtal med underbiträdet
- Hur ser man vilka länder som support utförs från?
  - Ofta svårt att utläsa av avtalet, otydliga skrivningar

# Praktiska utmaningar med adekvansbeslutet, forts

- Kommer supportleverantören att behandla personuppgifter?
  - Ofta svårt att utläsa av avtalet, otydliga skrivningar
- Hur gör man då?
  - Svårt att få ordentliga svar från leverantören
  - Analys utifrån avtalet och de faktiska omständigheterna
  - Göra en TIA på supportleverantören?
    - Typ av personuppgifter
    - Säkerhetsåtgärder, t.ex. kryptering
    - Riskbedömning
- Utmaning även i förhållande till Microsoft EU Data Boundary

# Elefanten i rummet – Schrems III

- Blir det en Schrems III?
  - NOYB kommer att utmana beslutet
  - Medlem av franska parlamentet utmanar beslutet
  - Adekvansbeslutet kommer att prövas av EU-domstolen
- Hur bör man förhålla sig till beslutet under tiden?
  - Utgå från att det är möjligt att överföra personuppgifter till USA med stöd av adekvansbeslutet
  - Ta höjd för ändrade förutsättningar i avtalet
  - Ha en reservplan
  - Följ utvecklingen



**Delphi**

**En ny sekretessbrytande  
bestämmelse i offentlighets-  
och sekretesslagen  
(2009:400) (OSL)**





# (Mycket) kort bakgrund

- JO-beslut från 2014
- Olika uppfattningar om begreppet ”röjande”
  - Allt utlämnande är röjande, utkontraktering innebär alltid röjande
  - NJA 1991 s. 103 och AD 2019 nr 15 – sannolikhetsbedömning
- Betydelsen av Cloud Act
  - Ej automatiskt röjande enligt 8 kap. 3§ OSL
- Utlämnande av uppgifter till leverantören
  - Skadeprövning – beror på rekvisit
- Tystnadspliktslagen
- Sekretessbrytande bestämmelsen

# Tystnadspliktslagen VS 10 kap. 2 a § OSL

## Tystnadspliktslagen

- Underlättar vid skadeprövning enligt OSL

men

- Saknar betydelse vid absolut sekretess
- Verkställighetsproblematik avseende utländska leverantörer

## 10 kap. 2 a § OSL

- Ingen skadeprövning behövs
- Tillämpas även vid absolut sekretess

# 10 kap. 2 a § OSL

”Sekretess hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att **endast tekniskt bearbeta eller tekniskt lagra uppgiften**, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut”.

# Tillämpning – teknisk bearbetning eller lagring

## Teknisk bearbetning och lagring:

- Samma innebörd som i tystnadspliktslagen och tryckfrihetsförordningen
  - Grundläggande IT-driftstjänster och IT-baserade funktioner – ex. teknisk infrastruktur eller en teknisk plattform för IT-drift samt tillhandahållande av en IT-baserad funktion – ex. en applikation eller en standardiserad eller anpassad digital tjänst.
  - Införa, förvalta, utveckla och avveckla en IT-driftstjänst
- Åtgärder för upprätthållande av tillgänglighet, funktionalitet och prestanda i IT-driftstjänst genom
    - förändringar i tjänstens funktionalitet
    - etablering av tilläggstjänst eller integration med andra tjänster
    - konfiguration, test och utveckling
    - supporttjänster
    - säkerhetstester och säkerhetsåtgärder
  - Migrering och exportering av uppgifter vid avveckling av en tjänst

# Tillämpning – teknisk bearbetning eller lagring forts...

- De åtgärder som omfattas av uttrycket teknisk bearbetning eller teknisk lagring kan komma att förändras över tid
- Diarie- och ärendehanteringssystem eller system för kontorsstöd, som kan inkludera e-post, kalender och dokumenthanteringsstöd
- Teknikneutralt: molntjänstlösningar och "on prem" lösningar omfattas
- **Endast** teknisk bearbetning och lagring - om samma uppgifter hanteras i ett annat informationsflöde som inte utgör teknisk bearbetning och lagring behöver dessa flöden enligt eSams uppfattning hållas åtskilda

## Ej teknisk bearbetning eller lagring:

- Analys
- Försäljning av information
- Tillföra informationen något nytt eller kompletterande innehåll
- Utkontraktering av arbetsuppgifter hänförliga till vård- och omsorgssektorns behandling av personuppgifter vid t.ex. journalföring, bedömning av röntgenbilder eller patientrådgivning
- AI-verktyg inom ramen för de tjänster en myndighet tillhandahåller?



# 10 kap. 2 a § OSL

”Sekretess hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet som **för den utlämnande myndighetens räkning** har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut”.

# Tillämpning – ”för den utelämnande myndighetens räkning”

**För den utelämnande myndighetens räkning:**

Leverantören får inte under några omständigheter behandla uppgifterna för eget ändamål, ex. statistik eller förbättring av tjänsten

# Tillämpning – olämplighetsbedömningen

- En allsidig prövning av alla omständigheter som är relevanta i det enskilda

## fallet:

- Vilken typ av uppgifter det rör sig om – är det känsliga uppgifter relaterade till exempelvis rikets säkerhet?
- Vilka intressen ligger till grund för sekretessen?
- Uppgifternas omfattning
- Uppgiftsmottagarens skydd av uppgifterna – vilka skyddsåtgärder vidtas och finns en lag- eller avtalsreglerad tystnadsplikt?
- Avtalsförhållandet mellan myndigheten och uppgiftsmottagaren – myndighetens kontroll över uppgifterna
- Var kommer uppgifterna hanteras geografiskt?
- Kommer underleverantörer få tillgång till uppgifterna?
- Kommer uppgifterna samlokaliseras med andra kunders uppgifter?
- Extraterritoriell lagstiftning: kan utländska myndigheter få tillgång till uppgifterna?

# Tillämpning – olämplighetsbedömningen

## Praktiska medskick:

### Allmänt

- Dokumentera hur olämplighetsbedömningen gjorts

### Avtalet med leverantören

- Förbud mot användning för egna ändamål
- Sekretess
- Skyddsnivå tekniskt och organisatoriskt
- Vad som händer med uppgifterna när avtalet sägs upp
- Funktion för uppföljning/revision
- Utelämnande av uppgifter till underleverantörer och krav på underleverantörer
- Ta hjälp av leverantören vid upphandlingen - information

# NIS-lagen

- NIS 1: 2018-08-01 (Lag om informationssäkerhet för samhällsviktiga och digitala tjänster)
- Vem omfattas
  - Samhällsviktiga tjänster (Bank, Energi, Hälso/Sjukvård, dricksvatten, transport)
  - Digitala tjänster (Marknadsplatser, sökmotorer, molntjänster) (Färre krav)
- Vad innebär NIS?
  - Säkerhetsåtgärder:
  - Samhällsviktiga: Systematiskt och riskbaserat säkerhetsarbete. Anmälningsskyldighet
  - Alla: Vidta ändamålsenliga och proportionerliga tekniska och organisatoriska åtgärder + åtgärder för att minska effekt av incident
  - Incidentrapportering



# NIS 2

- Direktiv: Ska införlivas senast 18 oktober 2024 (utredning redovisas 23 februari 2024)
- Avser nationella åtaganden och krav på väsentliga och viktiga enheter! Krav på cyberkrishanteringsmyndighet och CISRT team, internationellt samarbete mm.
- Fler sektorer (Väsentliga / Viktiga). Exempel:
  - Avlopp, fjärrvärme
  - Offentliga förvaltningsentiteter
    - Allmännas intresse
    - Finansieras av staten, regionala myndigheter eller andra off rättsliga organ
    - Befogenhet rikta beslut till fysiska eller juridiska personer som påverkar rättigheter avseende gränsöverskridande rörlighet
  - Post och bud
  - Livsmedelsproduktion + distribution
  - Tillverkning ex vis datorer, medicintekniska produkter, motorfordon
  - Mycket är samma för viktiga och väsentliga entiteter. Undantag: Myndigheters tillsyn / sanktioner

# NIS 2

- Mer detaljerade krav på riskhantering
  - ”Lämpliga och proportionerliga tekniska och organisatoriska åtgärder” – jfr GDPR
  - Nämner specifika krav – ex vis, kryptering, åtkomstkontroll, multifaktorautentisering
  - Med beaktande av ”relevanta och internationella standarder”
- Supply Chain – produkter och tjänster – bedömning och avtalshantering. Särskilt viktigt för leverantör av säkerhetstjänst
- Nya rapporteringströsklar och process för incidenter – ”betydande incident”. Anmäls till CSIRT team och användare.
  - Inte bara incidenter utan hot som kan leda till incident
  - Allvarliga störningar/ekonomiska förluster påverkan gm vållande av materiell skada
- Höjda sanktionsavgifter – 10 MEUR / 2 % av global årsomsättning (väsentliga)

# NIS 2 – vad göra?

- Omfattas vår verksamhet?
- Systematiskt och riskbaserat informationssäkerhetsarbete
  - ISO 27000 (artikel 21 & 24)
  - Policy och instruktioner
  - Incidenthantering (förebygg, upptäck, reagera)
  - Kontinuitetsplanering/krishantering
- Supply chain (Jfr skäl 85-86)
  - Kartlägg leverantörer och baseline
  - Se över avtal - säkerhetskrav
  - Implementera incidenthantering och kontinuitetsplanering / rutiner för kontroll och revision
  - Kostnadsdrivande omförhandling?
- Börja nu!

# Runt hörnet?

## Tillgänglighetsdirektivet

- Ställer nya krav på tillgänglighet för vissa produkter och tjänster
- Omfattande krav – påbörja ert arbete redan nu!

## Data Act

- Ämnar skapa ett gemensamt dataflöde inom EU
- Krav på att uppkopplade produkter (IoT) ska utformas så att det blir lättare att ge och få åtkomst till data

# Bensträckare och fika 15.25-15.45

Delphi



# Delphi Tech Day

21 september 2023

## Från paragrafer till programmering: AI-projekt hos Försäkringskassan



**Fredrik Ivarsson**  
Verksamhetsutvecklare



**Frode Randers**  
IT Architekt



**Daniel Westman**  
Oberoende forskare och  
rådgivare, expert på techjuridik

**Delphi**

# AI-projekt hos Försäkringskassan

Från paragrafer till programmering



# Vilka är vi?

- Fredrik Ivarsson
- Frode Randers



# Vad har vi gjort?

## Labbverksamhet

Möjliggör för verksamheten att klämma och känna på tillämpad AI

## Samordning

Samordna verksamheter i processer kring tillämpad AI

## Etik

Statliga värdegrunden och lagstiftning gäller oavsett hantering  
- Manuellt, Maskinellt, AI

## Helhetsgrepp

Ny teknik → nya möjligheter → skärskåda hela verksamhetsprocessen → Större effekter

## Juridik

Tätt samarbete med Rättsavdelningen utifrån dataskyddsperspektiv

# Förutsättningar

**3.** AI är endast ett verktyg för att nå ett mål, AI är inte ett mål i sig. Hantera hypen och förväntningarna kring AI

**2.** Innovation är nyckeln. Våga testa hypoteser och gör det i småsteg och visa på möjligheterna

**1.** Verksamhet, verksamhet, verksamhet, verksamhet, verksamhet



**4.** AI projekt kräver en kulturell förändring och bjuder många gånger på riktiga överraskningar. Dessa förändringarna kräver ett stort sponsorskap och vilja att förändra

**5.** Underskatta inte tiden det tar att gå från en idé till en produktionsatt AI-lösning

**6.** Transparens, informationssäkerhet  
Juridik, etik och moral



# Rättsliga överväganden

- "AI-PM"
- AI-förordningen

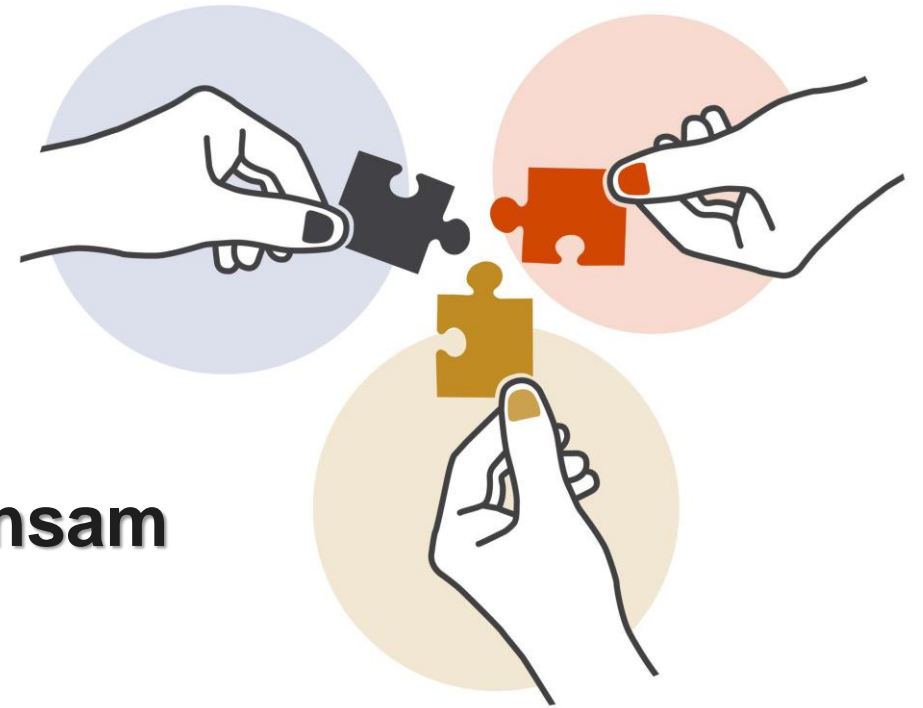


# Upptäckter och medskick



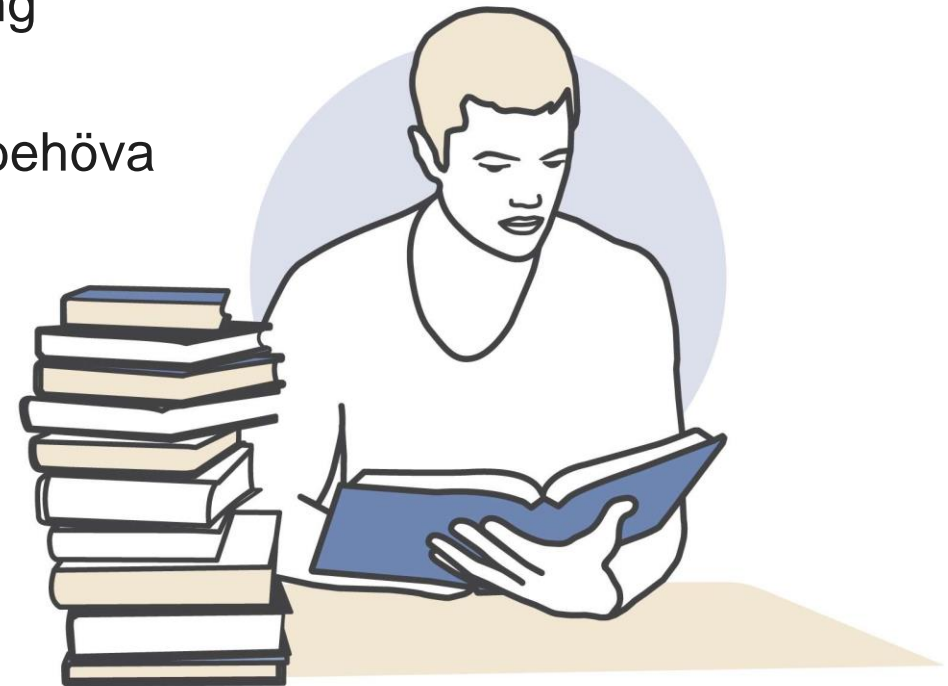
# Tillsammans

- Förstå varandras världar - juridik och teknik
  - Olika språk, olika verkligheter, olika utgångslägen
- Konkret exempel databaser inom juridik vs teknik
  - Socialförsäkringsdatabasen
- Förståelse för varandra
  - ”Jurister är nej-sägare”
  - ”IT-människor tror dom kan allt”
- Ofta finns inte svaren
  - Arbeta utforskande, med t.ex. AI-förordningen
- Jobba förutsättningslöst med en **gemensam målbild**



# Kunskap före produkt

- Förståelse och kunskap
- Vi är unika
  - Finns inte dussinet Försäkringskassor eller Migrationsverk
  - Finns likheter med andra verksamheter men vi har unika förutsättningar och behöver förstå dom för framgång
- Område som utvecklas snabbt
  - Färdiga svar kommer inte finnas utan kommer att behöva arbetas fram under resans gång



# Frågor





# Delphi Tech Day

21 september 2023

## Juridisk checklista för AI- projekt i offentlig sektor



Erik Ålander



Linus Larsén



Daniel Westman  
Moderator

Delphi

A woman with dark hair pulled back, wearing a white blazer over a dark top and a necklace, is shown from the chest up. She is looking off to the right with a thoughtful expression. Her hands are clasped in front of her. The background is a blurred building with windows. The entire image has a blue color cast. The text 'Vad är AI-juridik' is overlaid in white, bold, serif font across the center of the image.

# Vad är AI-juridik

# Vad är "AI-juridik"?





**Delphi**

# **10 punkter för AI- projekt**

# 10 punkter att tänka på rörande AI-projekt

1. Kartlägg noggrant hur AI-systemet ska användas i din verksamhet eller passar in i din produktportfölj
2. Bedöm AI-systemet utifrån a) leverantör, b) information om träningsdata och c) lokalisering av data
3. Riskklassificera AI-systemet utifrån olika riskfaktorer (potentiella skadetyper, förekomst av personuppgifter, sekretessfrågor och annan känslig information, riskklassificering enligt AI-förordningen, rättighetsfrågor)
4. Utifrån bedömningen under punkt 3 – se till att du vidtar de åtgärder som krävs för din riskklassificering
5. Finns det något krav på registrering eller ansökan till tillsynsmyndighet?



# 10 punkter att tänka på rörande AI-projekt

6. Dataskydd: gör en normal riskbedömning, säkerställ att ändamålen, informationskraven och de tekniska och organisatoriska skyddsåtgärderna är adekvata och på plats. Ansvars- och biträdesfrågorna kan vara mycket mer komplexa och kommer få väldigt stor betydelse.
7. Immaterialrätt: baserat på era behov, bedöm i mer detalj huruvida ni behöver a) rätt att använda indata, b) rätt att använda, utveckla, göra ändringar etc. i AI-modellen, c) att om modellen är färdigtränad att du har rätt till att använda tränad modell och eventuella utvecklingar, d) rätt till utdata och e) open source-frågor
8. Bedöm dina försäkringar så att de täcker användning av AI-systemet.
9. Avtal: Se till att avtalet täcker alla föregående punkter, säkerställ att leverantören tar ett adekvat ansvar – särskilt om det är ett system som tillhandahålls som en tjänst.

# 10 punkter att tänka på rörande AI-projekt

10. Utarbeta interna rutiner och policies baserat på alla föregående punkter så att AI-systemet inte används utöver dessa ramar eller i övrigt bryter andra användningsbegränsningar (operationella eller regulatoriska)

# Delphi Tech Day

21 september 2023

## Avslutande kommentarer



Agne Lindberg



Daniel Westman

Delphi



# Delphi Tech Day

21 september 2023



**Agne Lindberg**

+46 709 25 25 25

Agne.Lindberg@delphi.se



**Erik Ålander**

+46 709 25 25 17

Erik.Alander@delphi.se



**John Neway Herrman**

+46 709 25 25 84

John.Herrman@delphi.se



**Linus Larsén**

+46 709 25 25 45

Linus.Larsen@delphi.se



**Lovisa Lennström**

+46 709 25 25 35

Lovisa.Lennstrom@delphi.se



**Olivia Svedmark**

+46 767 72 00 12

Olivia.Svedmark@delphi.se



**Peter Nordbeck**

+46 709 25 25 01

Peter.Nordbeck@delphi.se

**Delphi**



# Delphi Tech Day

21 september 2023

## Följ oss här!

<https://www.delphi.se/sv/>

<https://www.delphi.se/sv/tech-blog/>

[in https://www.linkedin.com/company/advokatfirman-delphi/](https://www.linkedin.com/company/advokatfirman-delphi/)

[@advokatfirman.delphi](https://www.instagram.com/advokatfirman.delphi)

Delphi