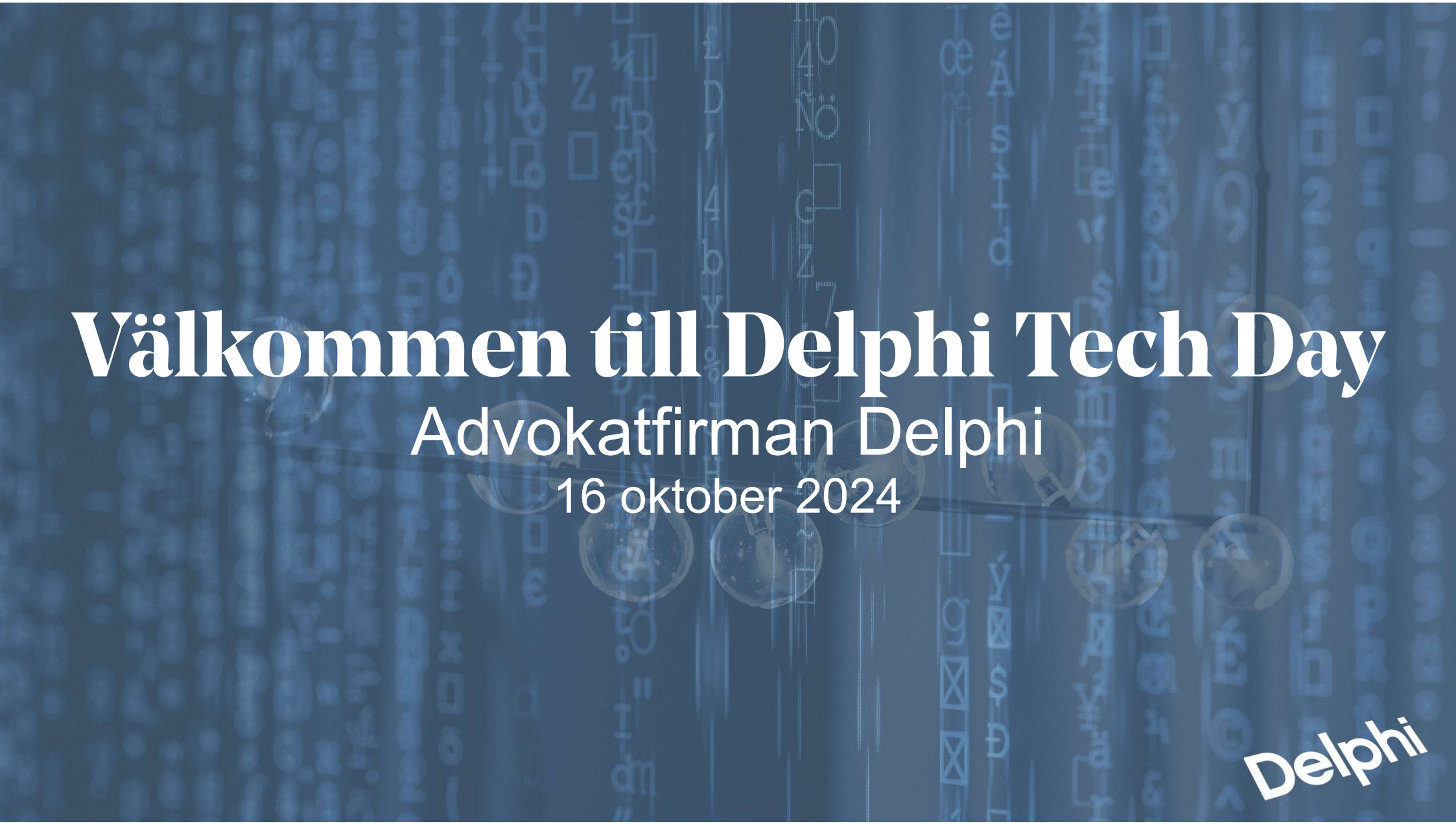

Välkommen till Delphi Tech Day
Advokatfirman Delphi
16 oktober 2024
Delphi

Nyhetspass

Delphi Tech Day 2024

DANIEL WESTMAN

Europeiska unionens
officiella tidning

SV
L-serien

2024/1689

12.7.2024

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2024/1689

av den 13 juni 2024

om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

Europeiska unionens
officiella tidning

SV
L-serien

2023/2854

22.12.2023

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2023/2854

av den 13 december 2023

om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

EUROPEAN UNION

THE EUROPEAN PARLIAMENT **THE COUNCIL**

Brussels, 25 September 2024
(OR. en)

2022/0302(COD) **PE-CONS 7/24**

JUSTCIV 17
JAI 111
CONSOM 32
COMPET 81
MI 78
FREMP 32
TELECOM 25
CYBER 15
DATAPROTECT 35
CODEC 163

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products and repealing Council Directive 85/374/EEC

Nya regler om cybersäkerhet

Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven

Stockholm 2024

STATENS OFFENTLIGA UTREDNINGAR

SOU 2024:18

Motståndskraft i samhällsviktiga tjänster

Slutbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven

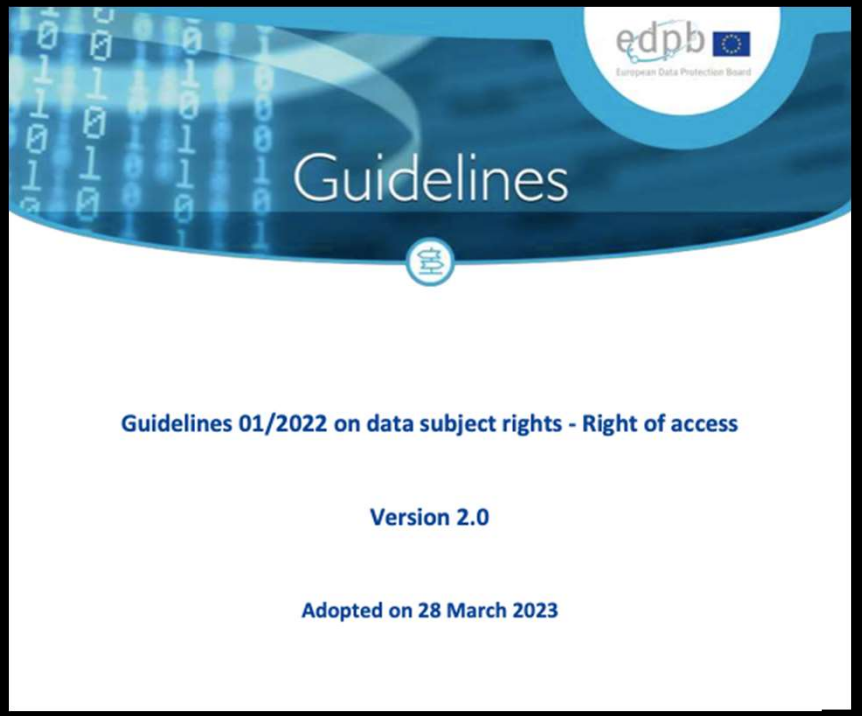
Stockholm 2024

STATENS OFFENTLIGA UTREDNINGAR

SOU 2024:64

Domar och vägledning om registerutdrag (rätt till tillgång)

- C-154/21, Österreichische Post AG
- C-487/21, Österreichische Datenschutzbehörde
- C-579/21, Pankki
- C-307/22 FT



EU-domstolen om känsliga personuppgifter

- C-21/23, Lindenapotheke
- Tidigare domar
  - C-184/20, Vyriausioji tarnybinės etikos komisija
  - C-252/21, Meta Platforms m.fl.

EU-domstolen om automatiserade beslut

- C-634/21, SCHUFA I

EU-domstolen om intresseavvägningen m.m.

- C-26/22 och C-64/22, Schuffa holding II
- C-17/22 and C-18/22, HTB
- C-621/22 Koninklijke Nederlandse Lawn Tennisbond

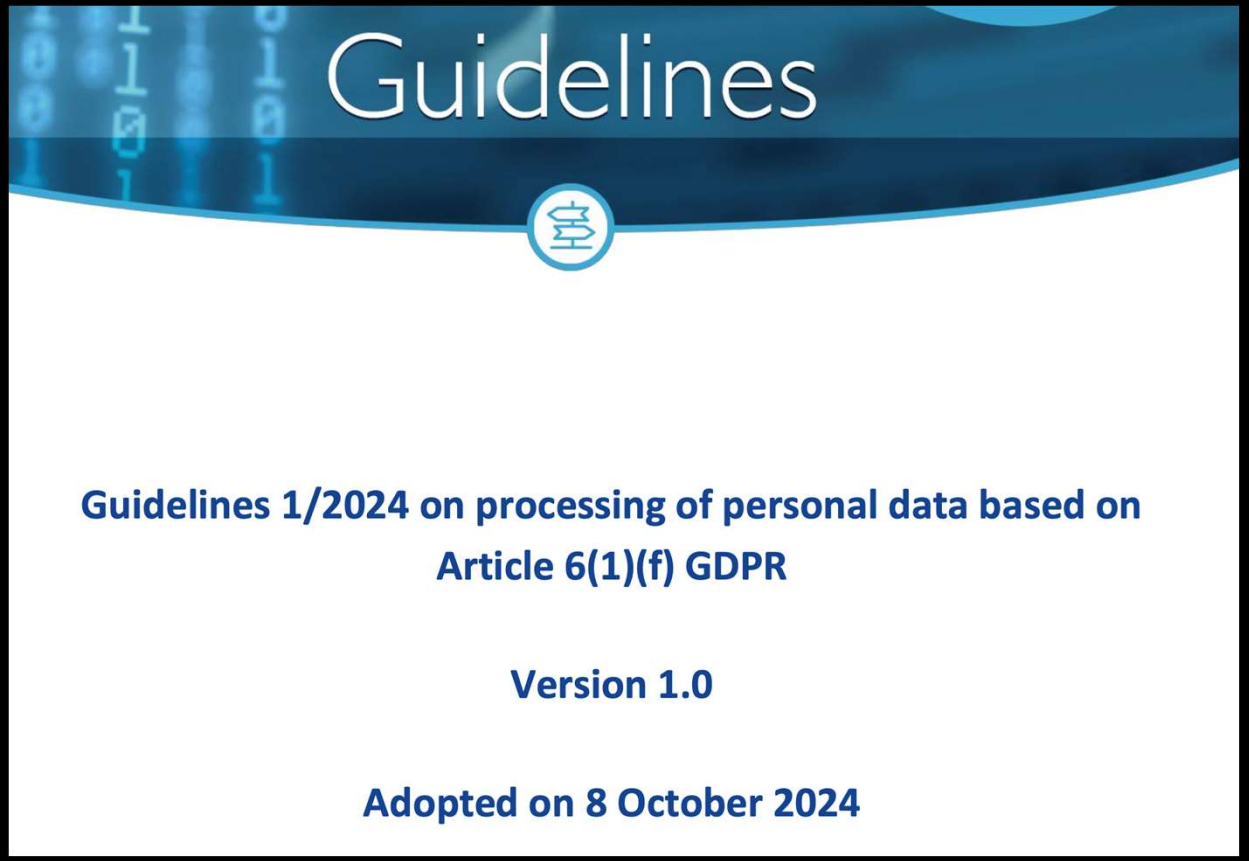
EU-domstolen om rätten till skadestånd

- C-300/21, Österreichische Post
- Exempel övriga mål
  - C-340/21 Natsionalna agentsia za prihodite
  - C-687/21 MediaMarktSaturn
  - C-741/21 juris

Förutsättningar för sanktionsavgift

- C-683/21, Nacionalinis visuomenės sveikatos centras
- C-807/21, Deutsche Wohnen

Riktlinjer (utkast) EDPB



EDPB (artikel 64)

Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms

Adopted on 17 April 2024

EDPB (artikel 64)

Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)

Adopted on 7 October 2024

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS INVESTIGATION INTO USE OF MICROSOFT 365 BY THE EUROPEAN COMMISSION (Case 2021-0518)

Decision

(8 March 2024)

IMY klar med fördjupade granskningar av dataskyddsombudens roll

Publicerad: 27 juni 2024

Integritetsskyddsmyndigheten (IMY) har granskat hur fem verksamheter med dataskyddsombud hanterar eventuella intressekonflikter för ombuden. Dessutom har ytterligare en verksamhet granskats för att kontrollera att ombudet har den roll och de resurser som krävs.

Privatperson | Verksamhet | IMY. Integritetsskydds myndigheten

Sanktionsavgift mot Avanza för överföring av personuppgifter till Meta

Publicerad: 25 juni 2024

Integritetsskyddsmyndigheten (IMY) utfärdar en sanktionsavgift på 15 miljoner kronor mot Avanza Bank AB. Detta för att banken använt en så kallad Meta-pixel på sin webbplats och app och som inneburit att uppgifter om exempelvis kunders värdepappersinnehav och kontonummer överförts till Meta.

Sanktionsavgifter mot Apoteket och Apohem för överföring av person-uppgifter till Meta

Publicerad: 30 augusti 2024

Integritetsskyddsmyndigheten (IMY) beslutar om sanktionsavgifter på 37 miljoner kronor mot Apoteket AB och 8 miljoner mot Apohem AB. Detta efter att bolagen använt den så kallade Meta-pixeln på sina webbplatser och överfört integritetskänsliga personuppgifter till Meta.

EUROPEAN
COMMISSION

Brussels, 25.7.2024
COM(2024) 357 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Second Report on the application of the General Data Protection Regulation

Några IT-rättsligt trender – personliga reflektioner

- AI och säkerhet i fokus
- Vad händer efter Digital Decade? Konsolidering/förenkling?
- Överlappande krav, skapa samlad kravmassa
- Påverkan på IT-avtalen
- Hantera skilda riskbegrepp
- Data governance-strukturer blir nödvändiga


DANIEL WESTMAN
danielwestman.org
0701-852 699
@netlawswe (X/Twitter)

Delphi

Den sekretessbrytande bestämmelsen för teknisk bearbetning och lagring

10 kap. 2 a § offentlighets- och sekretesslagen (2009:400) (OSL)

(Mycket) kort bakgrund

- Tidigare uppfattningar om begreppet ”röjande”
  - NJA 1991 s. 103 och AD 2019 nr 15 – sannolikhetsbedömning
  - JO-beslut från 2014

  - **Nu → Allt utlämnande är röjande, utkontraktering innebär alltid röjande**
  - Undantag vid tillräcklig kryptering

- Förhållandet mellan 10 kap. 2 a § OSL och tystnadspliktslagen

Delphi

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**”.

Delphi

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

Delphi

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

Delphi

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
- Förbättring och utveckling av leverantörens tjänster
- Övervakning av otillåten användning

Delphi

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**”.

Delphi

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?

Delphi

Workshop – leverantörens avtal i praktiken

- Tre jättar
- AWS (Amazon)
- Google Cloud
- Azure (Microsoft)

Delphi

För myndighetens räkning – exempel 1

DPA

Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data, Professional Services Data, and Personal Data only as described and subject to the limitations provided below (a) to provide Customer the Products and Services in accordance with Customer's documented instructions and (b) for business operations incident to providing the Products and Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data and Professional Services Data. Microsoft acquires no rights in Customer Data or Professional Services Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

"Product" has the meaning provided in the volume license agreement. For ease of reference, "Product" includes Online Services and Software, each as defined in the volume license agreement.

"Professional Services" means the following services: (a) Microsoft's consulting services, consisting of planning, advice, guidance, data migration, deployment and solution/software development services provided under a Microsoft Enterprise Services Work Order or, when agreed to in the Project Description, under a Cloud Workload Acceleration Agreement that incorporates this DPA by reference; and (b) technical support services provided by Microsoft that help customers identify and resolve issues affecting Products, including technical support provided as part of Microsoft Unified Support or Premier Support Services, and any other commercial technical support services. The Professional Services do not include the Products or, for purposes of the DPA only, Supplemental Professional Services.

Delphi

För myndighetens räkning – exempel 1

DPA

Processing to Provide Customer the Products and Services

For purposes of this DPA, "to provide" a Product consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security.

For purposes of this DPA, "to provide" Professional Services consists of:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and
- Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant.

Delphi

För myndighetens räkning – exempel 1

DPA

Processing for Business Operations Incident to Providing the Products and Services to Customer

For purposes of this DPA, "business operations" means the processing operations authorized by customer in this section.

Customer authorizes Microsoft:

(i.) to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and

(ii.) to calculate statistics related to Customer Data or Professional Services Data

in each case without accessing or analyzing the content of Customer Data or Professional Services Data and limited to achieving the purposes below, each as incident to providing the Products and Services to Customer.

Those purposes are:

- billing and account management;
- compensation such as calculating employee commissions and partner incentives;
- internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and
- financial reporting.

Delphi

För myndighetens räkning – exempel 2

Huvudavtalet

5. Intellectual Property Rights; Protection of Customer Data; Feedback.

5.1 *Intellectual Property Rights.* Except as expressly stated in this Agreement, this Agreement does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer retains all Intellectual Property Rights in Customer Data and Customer Applications, and Google retains all Intellectual Property Rights in the Services and Software.

5.2 *Protection of Customer Data.* Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. Google has implemented and will maintain technical, organizational, and physical measures to protect Customer Data, as further described in the Cloud Data Processing Addendum.

5.3 *Customer Feedback.* At its option, Customer may provide feedback or suggestions about the Services to Google ("Feedback"). If Customer provides Feedback, then Google and its Affiliates may use that Feedback without restriction and without obligation to Customer.

Delphi

För myndighetens räkning – exempel 2

DPA

5.2 *Compliance with Customer's Instructions*. Customer instructs Google to process Customer Data in accordance with the applicable Agreement (including this Addendum) and applicable law only as follows:

a. to provide, secure, and monitor the Services and TSS (if applicable); and

b. as further specified via:

i. Customer's use of the Services (including via the Admin Console) and TSS (if applicable); and

ii. any other written instructions given by Customer and acknowledged by Google as constituting instructions under this Addendum

(collectively, the "*Instructions*").

- "*Services*" means the applicable services described in Appendix 4 (Specific Products).

Delphi

För myndighetens räkning – exempel 3

Huvudavtalet

1.4 Data Privacy. You may specify the AWS regions in which Your Content will be stored. You consent to the storage of Your Content in, and transfer of Your Content into, the AWS regions you select. We will not access or use Your Content except as necessary to maintain or provide the Services, or as necessary to comply with the law or a binding order of a governmental body. We will not (a) disclose Your Content to any government or third party or (b) move Your Content from the AWS regions selected by you; except in each case as necessary to comply with the law or a binding order of a governmental body. Unless it would violate the law or a binding order of a governmental body, we will give you notice of any legal requirement or order referred to in this Section 1.4. We will only use your Account Information in accordance with the Privacy Notice, and you consent to such usage. The Privacy Notice does not apply to Your Content.

Delphi

För myndighetens räkning – exempel 3

Huvudavtalet

"Service" means each of the services made available by us or our affiliates, including those web services described in the Service Terms. Services do not include Third-Party Content.

6. Proprietary Rights.

6.1 Your Content. Except as provided in this Section 6, we obtain no rights under this Agreement from you (or your licensors) to Your Content. You consent to our use of Your Content to provide the Services to you and any End Users.

Delphi

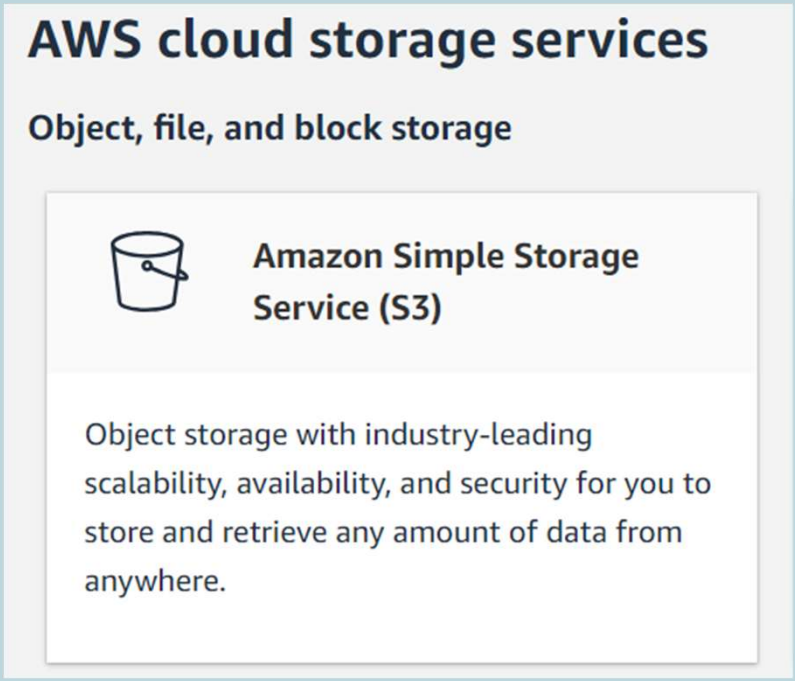
Teknisk bearbetning och lagring – exempel 1

Microsoft Copilot

Delphi

Teknisk bearbetning och lagring – exempel 2

Lagringstjänst AWS



Delphi

Olämplighetsbedömningen– exempel 1

Ändringar av avtalsvillkor och tjänster

1.4 *Modifications.*

(a) *To the Services.* Google may make commercially reasonable updates to the Services from time to time. Google will inform Customer if Google makes a material change to the Services that has a material impact on Customer's use of the Services provided that Customer has subscribed with Google to be informed about such change.

(b) *To the Agreement.* Google may make changes to this Agreement (including the URL Terms) and pricing from time to time. Unless otherwise noted by Google, material changes to the Agreement will become effective 30 days after they are posted, except to the extent the changes apply to new functionality or the Cloud Data Processing Addendum, or are required by applicable law, in which case they will be effective immediately. Google will provide at least 90 days' advance notice for materially adverse changes to any SLAs by (i) sending an email to the Notification Email Address; (ii) posting a notice in the Admin Console; or (iii) posting a notice to the applicable SLA webpage. If Customer does not agree to the revised Agreement, Customer may stop using the Services. Customer may also terminate this Agreement for convenience under Section 8.4 (Termination for Convenience). Customer's continued use of the Services after such material change will constitute Customer's consent to such changes. Google will post any modification to this Agreement to https://cloud.google.com/terms/.

Delphi

Olämplighetsbedömningen– exempel 2

Underleverantörer och personuppgiftsbiträden

Microsoft

Microsoft Online Services Subprocessors

Entity Name	Applicable Online Service or Product	Sub-processing Activity	Processing Location(s)	DnB Registered Address	Headquarters	DnB Registered Number	Parent Company
Accenture International Limited	SAP HANA on Azure (Large Instances)	Hardware and software installation and operations	In accordance with the customer-specified regionality of SAP HANA on Azure (Large Instances)	1 Grand Canal Square Dublin 2, Ireland	Ireland	985015354	Accenture Public Limited Company
Akamai Technologies, Inc.	Any Microsoft Online Service	Operating Content Delivery Network (CDN) infrastructure to efficiently deliver content	Worldwide	150 Broadway, Cambridge MA, 02142-1413 USA	United States	47775205	Akamai Technologies, Inc.
Databricks, Inc.	Azure Databricks	Deploying, operating, and troubleshooting Azure Databricks	Canada, France, Germany, Netherlands, United Kingdom, United States	160 Spear Street, FL 13, San Francisco, CA, 94105-1546 USA	United States	79356302	Databricks, Inc.
Edgio, Inc.	Any Microsoft Online Service	Operating Content Delivery Network (CDN) infrastructure to efficiently deliver content	Worldwide	11811 N. Tatum Blvd. Ste 3031 Phoenix, AZ 85028, USA	United States	118890507	Edgio, Inc.

Delphi

Workshop – key take aways

- Se över leverantörens krypteringslösningar
- Granska avtalsdefinitionerna noggrant
- Kolla DPA även för leverantörens användning av andra kunddata än personuppgifter
- Granska produktspecifika villkor – dessa kan skilja sig från huvudavtalet
- Granska produktvillkoren och de tekniska specifikationerna – teknisk bearbetning eller teknisk lagring
- Håll koll på uppdaterade avtalsvillkor och produktfunktioner
- Kolla upp underleverantörer och underbiträden
- Bocka av alla rekvisit i olämplighetsbedömningen

Delphi

Tack!

Peter Nordbeck

Partner / Advokat

Peter.nordbeck@delphi.se

Olivia Svedmark

Associate

Olivia.svedmark@delphi.se

Erik Ålander

Senior Associate / Advokat

Erik.alander@delphi.se

Delphi

Delphi

/ We love challenges

IT och informationssäkerhet

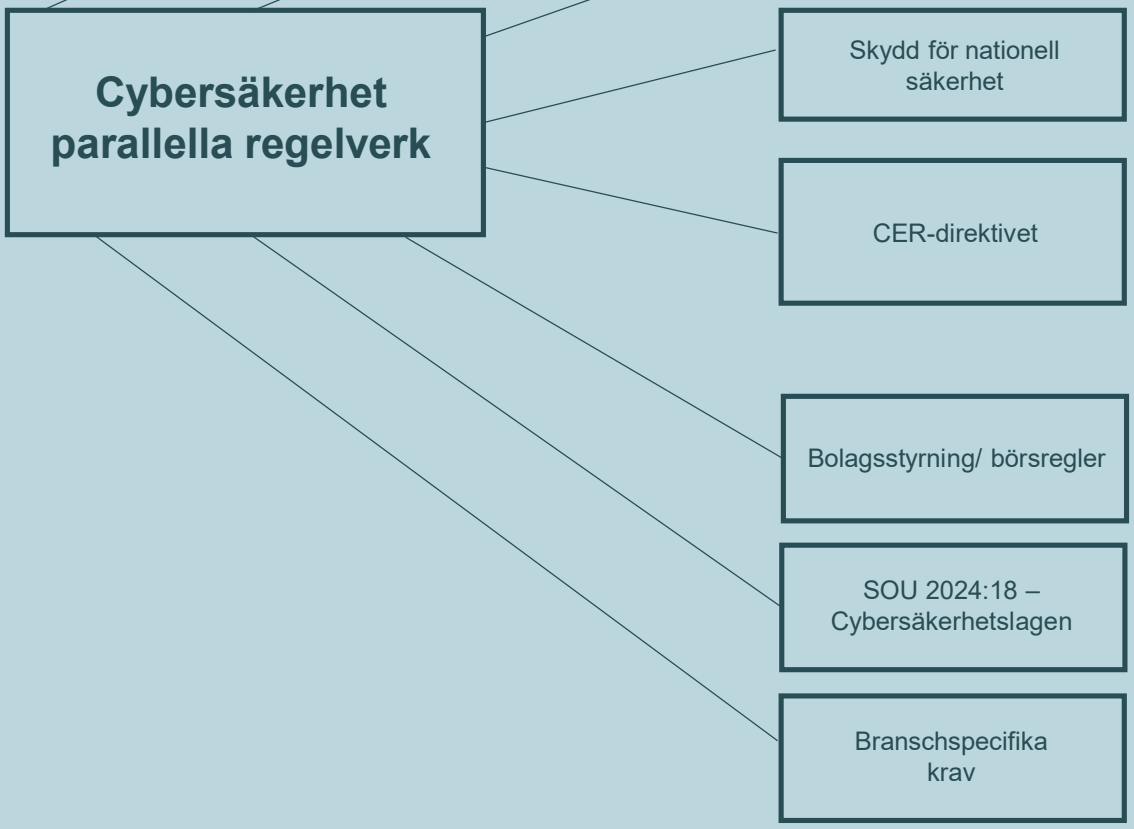
Dahae Roland
Agne Lindberg
John Herrman

Några begrepp

- **Informationssäkerhet - den samlade, övergripande säkerhet som ska se till att den information som finns i en organisation alltid är korrekt, tillgänglig och skyddad från obehörig åtkomst. All information – oavsett digital eller inte**
  - Konfidentialitet – ingen obehörig åtkomst eller behandling
  - Integritet – korrekt och oförändrad
  - Autenticitet – informationen kommer från den som påstås
  - Tillgänglighet – vid behov
  - Spårbarhet
- **IT säkerhet – skydd av digital information och de tekniska systemen. Delmängd av informationssäkerhet**

Delphi

Den rättsliga kartan Informationssäkerhet



- GDPR
- Patientsäkerhet

- NIS (Lag om informationssäkerhet i samhällsviktiga och digitala tjänster), Cybersäkerhetslagen
- CER direktivet (motståndskraft)

- Cyber Resilience Act, Cybersäkerhetsförordningen

- Säkerhetsskyddslagen. Säkerhetsskyddsanalys. Skydda säkerhetskyddsklassificerade uppgifter från röjande/ otillgänglighet/förstörande

- Bredare än cybersäkerhet – även andra hot (terror, sabotage, naturkatastrof)
- Nationell strategi, nationell riskbedömning
- Identifiera risker – lämpliga tekniska, organisatoriska och säkerhetsmässiga åtgärder. Incidentrapportering.
- Förslag i september 2024 – lag om motståndskraft hos kritiska verksamhetsutövare. 1/8 2025

- Krav på att information är korrekt och skydd för handel med aktier m.m. (bolagsstyrning)

- Från och med 1 januari 2025 –NIS 2-direktivet implementeras i Sverige

- DORA, EBA, MSB:s riktlinjer

Delphi

Gemensamma nämnare!

- **Riskinventering och säkerhetsåtgärder.** Proportionalitet. Tekniska och organisatoriska åtgärder!
- **Krav på övervakning och uppföljning**
- **Krav på kontinuitets- och återställandeplaner, inkl. testning**
- **Incidenthantering och -rapportering**
- **Systematiskt arbete**
- **Krav på leverantörskedjan**
- **Utbildning**
- **Dokumentera: analyser – åtgärder – incidenter – uppföljningar – uppdateringar**
- **OBS! En informationssäkerhetsprocess – inte en process per regelverk!**

Delphi

Från NIS 1 till NIS 2

- **NIS 1**
  - 7 sektorer / 3 digitala tjänster
  - Variationer i krav och incidentrapportering
  - Otydliga krav
  - Svaga sanktioner
  - Omfattar del av verksamheten
  - Inga tydliga krav på leveranskedjan (supply chain)
  - Bristande internationellt samarbete
- **NIS 2**
  - 18 sektorer (väsentliga och viktiga verksamhets-utövare). Exempel på nytt: Offentlig förvaltning och IKT tjänster
  - Enhetliga krav och incidentrapportering
  - Lite skarpare krav
  - Kraftigare sanktioner / nya sanktioner
  - Omfattar hela verksamheten
  - Krav på leverantörskedjan
  - Stärkt internationellt samarbete
  - Paketlösning med CER
  - Brasklapp – ingen prop ännu! Omfattande remissvar. Genomförandeakten fortfarande i förslagsform.

Delphi

Informationssäkerhet – ett ansvar för ledningen!

- ***Artikel 20.1:*** *Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.*
- **SOU 2024:18:** Behövs inte särskild regel – följer av 8 kap 4§ ABL – styrelsen svarar för bolagets organisation och förvaltning. Off verksamhet – se artikel 20.2 – NIS 2 har ingen påverkan på ansvarsregler i nationell rätt för offentliga verksamheter.
- **Utbildning** av ledningen obligatorisk**. Övrig personal** – ska erbjudas

Delphi

Krav på verksamhetsutövare – riskhanteringsåtgärder (3 kap.)

- OBS – hela verksamheten omfattas, inte bara den verksamhet som ”triggar” lagens tillämplighet
- Anmälan till tillsynsmyndighet: identitet, kontaktuppgifter, verksamhet
- Riskhanteringsåtgärder
  - Riskanalys – riskexponering, sannolikhet och konsekvenser
  - Proportionella åtgärder baserat på riskanalys
  - Dokumentera!
  - Obligatoriska moment! (se nästa sida)
- Systematiskt arbete! Föreskrifter kommer!
  - Långsiktigt / Kontinuerligt / Metodiskt
  - ISO 27000-serien
- Incidentanmälan till MSB

Delphi

Riskhantering – obligatoriska moment

- Incidenthantering,
- kontinuitetshantering (backup, BCP, DR). Behov av att bedöma RPO (hur färsk data) & RTO (tid för återläsning),
- säkerhet i leveranskedjan,
- säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation, Avser köp! Inte exempelvis utkontraktering,
- strategier och förfaranden för användning av kryptografi och kryptering,
- personalsäkerhet,
- strategier för åtkomstkontroll och tillgångsförvaltning,
- säkrade lösningar för kommunikation och
- lösningar för autentisering.
- Föreskrifter kommer!

Delphi

Tillsyn & Sanktioner

- Tillsyn: Revision, föreläggande, säkerhetsrevision, säkerhetsscanning
- Ingripanden:
  - Föreläggande – kan förenas med vite
  - Förbud att utöva ledningsfunktion (förvaltningsdomstol) – allvarlig överträdelse av uppsåt/grov oaktsamhet
  - Sanktionsavgift
    - Väsentliga: Högsta av 2% av global årsomsättning/10 MEUR
    - Viktiga: Högsta av 1,4% av global årsomsättning/7 MEUR
    - Offentlig verksamhet: Max 10 MSEK
  - Alternativt: Anmärkning - varning

Delphi

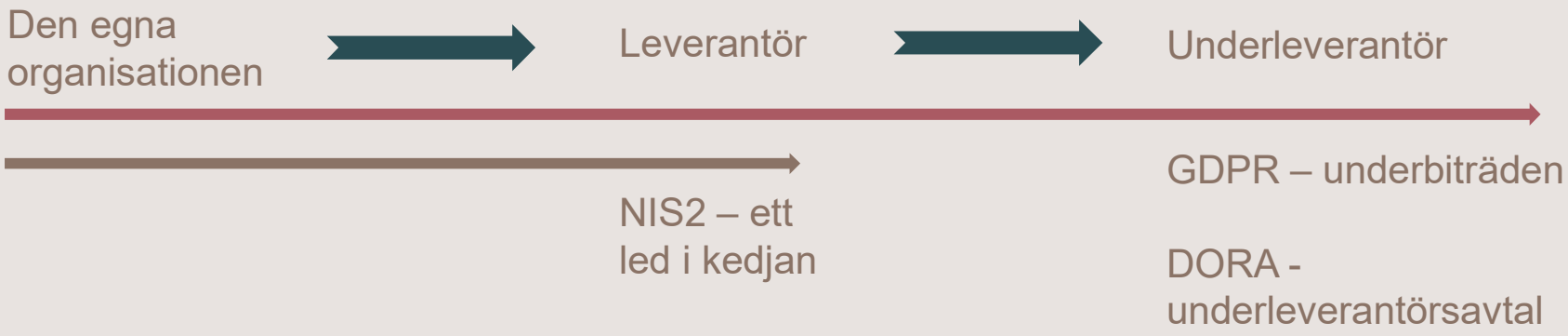
(CER) Lag om motståndskraft hos kritiska verksamhetsutövare – viktiga principer

- **Krav på medlemsstaterna – nationell strategi och nationell riskbedömning**
- **Identifiera tillhandahållare av samhällsviktigt verksamhet för varje sektor**
- **Samhällsviktiga verksamheter ska 1) göra riskbedömning och 2) vidta lämpliga och proportionella tekniska och organisatoriska åtgärder (”Allriskperspektiv”), inkl.:**
  - Förhindra incidenter – inkl. åtgärder för att reducera katastrofrisk och för anpassning till klimatförändringar
  - Fysiskt skydd av känsliga områden, anläggningar och infra
  - Stå emot och lindra konsekvenser av incident – inkl. varningsrutiner
  - Återhämta sig från incidenter, inkl. driftskontinuitetsplaner och alternativa försörjningskedjor
- **Krav på incidentrapportering (även vid risk för incident)**
- **Bakgrundskontroller**
  - Viktiga befattningar

Delphi


Leveranskedjan

Hantering av leveranskedjan



Tre faser inför och under avtalsförhållandet

Inför anlitande av leverantör – utvärdering och kravställning

Under avtalstiden – revision och incidentrapportering

Om det inte blir som man tänkt – exit?

Delphi

1. Inför anlitande av leverantör – utvärdering

- Bedömning av övergripande kvalitet och resiliens hos produkter och tjänster och riskhanteringsåtgärder för cybersäkerhet
- Fokus på leverantörens befintliga säkerhetsrutiner, kapacitet och historik
- Utvärdering av leverantörens säkerhetserbjudande/GAP-analys i förhållande till regulatoriska krav
- Hur stor del av leveransen utförs av leverantören vs. underleverantörer och kontroll/insyn över dessa?
- Certifieringar eller rapporteringsramverk (t.ex. ISO 27000-serien eller SOC 2)?
- Referenser från kunder som omfattas av samma eller liknande regelverk?
- Hur ser leverantörens cybersäkerhetspraxis ut?

Delphi

2. Inför anlitande av leverantör (forts.) – kravställning i avtal

- Införliva riskhanteringsåtgärder för cybersäkerhet i avtalet
- Definiera krav på säkerhet som ska gälla – särskilda standarder, certifieringar, nivå osv.
- Skyldighet att följa utvecklingen över tid och anpassa/uppdatera säkerheten
- Risk management – hantering av olika risker. Samordna med befintliga åtgärder, t.ex. tekniska och organisatoriska åtgärder enligt GDPR
- Kontinuitetsplanering
- Incidenthantering och revision
- Regelbunden testning och delning av resultat
- Flow down till underleverantörer

Delphi

3. Under avtalstiden – revision

- Avtalet måste innehålla krav för att möjliggöra revision och rapportering
- Bra verktyg för att säkerställa och dokumentera att aktuella säkerhetskrav upprätthålls
- Se till att revisionsrätten även gäller under-leverantörer
- Krav på att testa kontinuitetsplaner regelbundet samt ta del av resultatet

Delphi

4. Under avtalstiden (forts.) – incident-rapportering

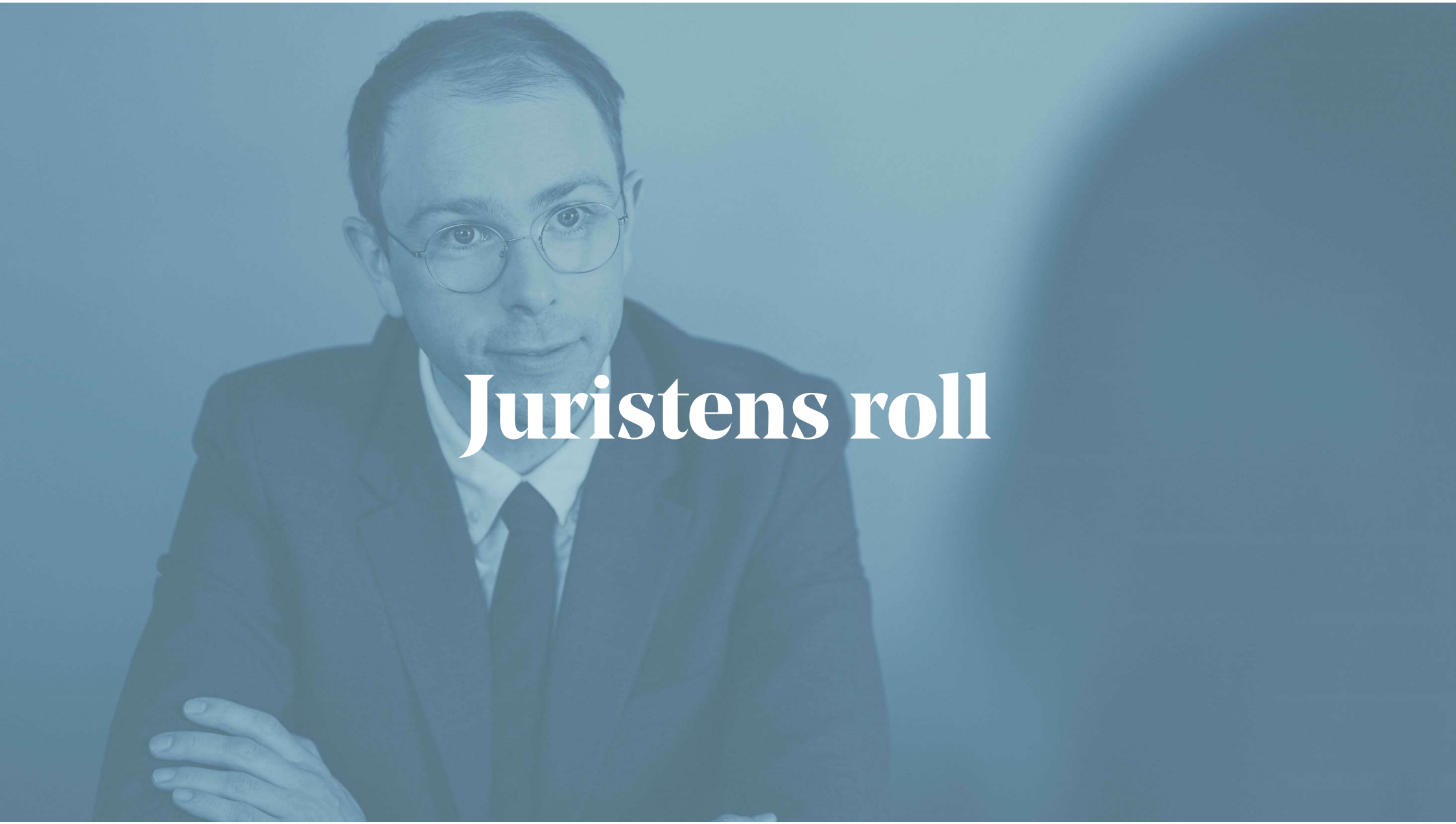
- Olika krav enligt olika regelverk – använd befintliga processer och anpassa till specifika krav
- Observera särskilda tidsfrister, t.ex. :
  - NIS: Inom 24 h
  - GDPR: Inom 72
  - DORA: ”Utan onödigt dröjsmål”
- Gemensam och enhetlig incidenthantering för leverantör och underleverantörer
- Rapportering av vissa särskilda händelser som kan påverka incidenthanteringen, t.ex. förvärv, byte av underleverantör

Delphi

5. Om det knakar eller blir skilsmässa – vad händer då?

- Måste finnas kontraktuella medel att hantera brister
- Om ingen bättring/särskilt allvarliga brister hos leverantör – måste finnas möjlighet till förtida exit
- SLA med krav på åtgärd inom viss tid vid vissa säkerhetsbrister. Om inte möjligt – alternativ lösning, t.ex. förtida exit
- Möjlighet att kräva utbyte av underleverantör vid upprepade/särskilt allvarliga brister
- Under exitperiod måste säkerhetskrav uppfyllas och assistans vid återtagande
- Återanvänd tidigare utvärdering för att kravställa mot ”nästa” leverantör

Delphi


Juristens roll

Juristens roll i informationssäkerhets-arbetet

- Din expertis och arbetsmetodik är viktig – exakt roll skiljer sig!
- Hur angriper du situationen – **Exempel på arbetsmetodik**
  I. Identifiera baseline – Hitta dina vänner/stakeholders och få information om nuläget i verksamhetens informationssäkerhetsarbete

  II. Har något relevant förändrats i verksamheten sedan sist?

  III. Hur ser uppföljningen och efterlevnad av informationssäkerhet ut i praktiken (rutiner, behörigheter, ändringar osv.)?

  IV. Mappa nuläge/baseline mot tillämpliga regler – Hitta bristerna/gapen!

  V. Åtgärdsplan tillsammans med stakeholders

  VI. Uppföljning och dokumentation

Delphi

Juristens roll i informationssäkerhets-arbetet

- Exempel på **juristens verktyg** som underlättar arbetet och tillför värde till verksamheten

  I. Styrdokument

  II. Avtalet och avtalsförhandling – juristens hemmaplan

Delphi

Styrning och kontroller

Klassning av information och funktioner nödvändig

- **Informationssäkerhet – riskbaserade åtgärder. Behov av olika nivåer för olika typer av information/tjänster/verksamhet**
- **Regelverken bygger på riskbaserade & proportionerliga åtgärder – beror på risknivå**
- **Exempel på informationsklassning**
  - Personuppgifter (vanliga, känsliga, brott, personnummer)
  - Risknivåer – styr krav på säkerhetsåtgärder, access, kontroller
    - Publik – Intern – Konfidentiell
  - Del av informationssäkerhetspolicy / riktlinjer
  - Styr även leverantörsavtalet

Delphi

Styrning / ledningssystem - styrdokument som behövs - checklista

- Policy
  - Grundläggande principer och värderingar
    - IT-policy
    - Informationssäkerhetspolicy
    - Personuppgifter
- Riktlinjer - Förtydligar och konkretiserar. Tekniska och organisatoriska åtgärder
  - Risk Management process
  - Access/behörighet
  - Change/Ändringar. Inkl. kontroll på inventarier
  - Övervakning, incident och problem
  - BCP / Disaster Recovery
  - Användning – internet, e-post, mobila enheter, distansarbete
- Innehåll
  - Vem beslutar? Vem ”äger”? Roller och ansvar!
  - Uppdateringsansvar
  - Kontroll och uppföljning. Kontroll av om fel begås!

Delphi

NIS 2 och styrdokument

- **Policy för informationssäkerhet (punkt 1.1 i Bilaga till Genomförandeakten) (utdrag)**
  - Fastställa mål för informationssäkerhet
  - Risktoleransnivå (peka på Risk Management – se nästa bild)
  - Kontinuerlig förbättring
  - Åtagande att tillhandahålla resurser för genomförande (personal, ekonomi, teknik)
  - Kommuniceras till anställda
  - Fastställa roller och ansvar
    - Minst en person ska rapportera till ledning
  - Lista dokumentation som ska bevaras (Jfr Gallring i GDPR)
  - Lista ämnesspecifika policies / instruktioner
  - Datum för godkännande
- **Ska ses över och uppdateras med planerade intervall OCH efter betydande incidenter eller förändringar**

Delphi

NIS 2 och styrdokument

- **Riskhanteringspolicy (punkt 2) i bilaga till genomförandeakten (utdrag)**
  - Upprätthålla en riskhanteringsram (Risk management process)
  - Riskbedömningar ska göras och dokumenteras. Resultat = genomförandeplan som ska genomföras
  - Resultatet och ev kvarvarande risker ska godkännas av ledningen (eller riskägare och informera ledningen)
  - Minimikrav på riskhanteringspolicy:
    - Riskhanteringsmetod och verktyg baserad på standarder
    - Riskkriterier
    - Riskidentifiering – tillgänglighet, integritet, autenticitet och konfidentialitet
    - Bedöma risker baserat på riskkriterier
    - Identifiera riskhanteringsåtgärder
    - Vem ansvarar för att genomföra riskhanteringsåtgärder och när?
    - Dokumentera (inkl. vilka risker man anser kan finnas kvar)

Delphi

Avslutande ord

Checklistor

Frågor om er förmåga att uppfylla kraven? Checklista – några viktiga moment

- Är ledningen involverad?
- Tillhandahåller du utbildning för anställda – inkl. ledning?
- Finns det förmåga och rutiner för incidenthantering – rapport inom 24 h?
- Utför ni regelbundet riskbedömningar med riskägare, inkl. risker i leverantörskedjan?
- Har ni en kontinuitetsplan och återställandeplan?
- Har ni dokumenterade policies och instruktioner på plats för styrning och uppföljning / kontroll?
  - Finns det ägare? Rapportering och uppföljning?
- Tar ni med informationssäkerhetskrav i era leverantörsavtal?
- Utför ni regelbundet interna revisioner och tester? Även leverantörer?
- Har ni dokumenterat bedömningar och åtgärder?

Delphi

Checklistor

Utgångspunkter för att säkerställa säkerhet i leveranskedjan enligt NIS2

Grundläggande säkerhetsåtgärder för att uppfylla kraven i NIS2

Delphi

Kontaktuppgifter

Dahae Roland

Advokat / Partner

dahae.roland@delphi.se

Agne Lindberg

Advokat / Partner

agne.lindberg@delphi.se

John Herrman

Advokat

john.herrman@delphi.se

Delphi

Delphi

/ We love challenges

AI & Governance: Juristens guide till AI-galaxen

Delphi Tech Day, 16 oktober 2024

Föreläsare

Johan Hübner

Partner / Advokat

Johan.hubner@delphi.se

Linus Larsén

Senior Associate / Advokat

Linus.larsen@delphi.se

Lovisa Lennström

Senior Associate / Advokat

Lovisa.lennstrom@delphi.se

Delphi

Agenda

- Case
- AI – inköp och avtal
- Checklista för inköp av AI – med fokus

Delphi

Case

Case - omständigheter

- Bolaget Rekryterarna AB vill med hjälp av en AI-lösning addera nya funktioner i sitt verktyg för att rekrytera nya medarbetare och utvärdera medarbetares prestationer. AI-systemet kommer därför bland annat behandla personuppgifter. AI AB har skapat tjänsten och AI-lösningen tillhandahålls som en molntjänst. AI AB:s modell är tränad på testdata (som används för att på ett oberoende sätt kunna utvärdera AI-systemet innan det tas i bruk) och används redan av konkurrenter till Rekryterarna AB.
- Rekryterarna AB ser att den nya funktionen kommer leda till ökad effektivitet i deras arbete omgående, men har insett att den största potentialen ligger i att AI-lösningen kontinuerligt tränas och vidareutvecklas. AI AB framhåller att nya tjänster och modeller kan utvecklas baserat på den kunddata som skapas i tjänsten och som samlas in från Rekryterarna AB:s kandidater och anställda.
- Integrationen av AI-lösningen är en relativt enkel och smidig process. Däremot är avtalet som AI AB tillhandahållit generellt sett mycket leverantörvänligt och det framgår att AI AB inte tar ansvar för omständigheter som härrör från användning av funktionen samt att AI AB har rätt att nyttja Rekryterarna AB:s kunddata för egna ändamål (exempelvis att träna AI-lösningen och utveckla nya produkter).

Delphi

AI – inköp och avtal

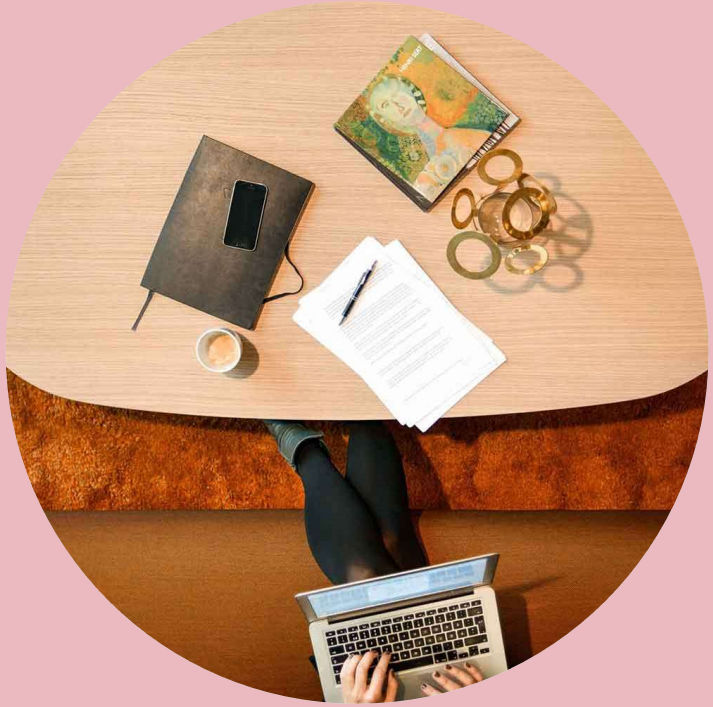
Introduktion

- Vad menas med AI-inköp?
- Bakgrund: AI-inköp
  - Helt nytt landskap av tjänster
  - Användningen i organisationer har exploderat
  - Förväntas öka i betydelse
- Fokus: Juridiken i inköpsprocessen i ett sammanhang
- Checklista – axplock viktiga bitar!

Delphi

Inköpsprocessen

- Många aspekter är relevanta
- Unik för varje organisation
- Lagkrav på vissa områden
- Vissa aspekter, möjligheter och risker är gemensamma



Delphi

Checklista för inköp av AI

Steg I: Kartläggning och utredning

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 (t.ex. potentiella skadetyper, förekomst av personuppgifter och annan känslig information, riskklassificering enligt AI-förordningen, immateriella 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?

Delphi

Steg II: Fördjupad utredning av viktiga risker

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) 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

Delphi

Steg III: Mitigeringsfasen

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. 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

Steg I: Kartläggning och utredning

1. Kartlägg AI-systemets roll internt

- Syfte och behov?
- Vilka aktörer är inblandade?
  - Inköp, affär, juridik, informationssäkerhet m.m.
- Vad är relationen till verksamheten i övrigt?
  - IT-miljö i övrigt
  - Teknisk natur
- Internt projekt?
- Data?

Delphi

2. Bedöm AI-systemets natur

- Leverantör
  - Etablerad relation?
  - Sektorer?
- Data
  - Kund och/eller leverantör ansvarar?
  - Annan leverantör för data?
- Tjänst
  - Cloud
  - On-prem
  - Projekt
  - Tredjepartsberoenden/open source
  - Hårdvarukomponenter

Delphi

3. Riskklassificera AI-systemet

Risk	Exempel på riskfaktorer
Projektrisker	• Ansvarfördelning kund/leverantör • Tidsplan och förseningar • Tredjeparter
Personuppgifter och annan känslig information	• Mängd personuppgifter • Känsliga personuppgifter (direkt eller indirekt) • Annan affärskänslig information • Sekretesskyddad information (OSL, finans m.m.)
Skadetyper	• Ekonomisk skada • Goodwill • Integritet • Person- och sakskada (fysiska miljöer och hårdvara

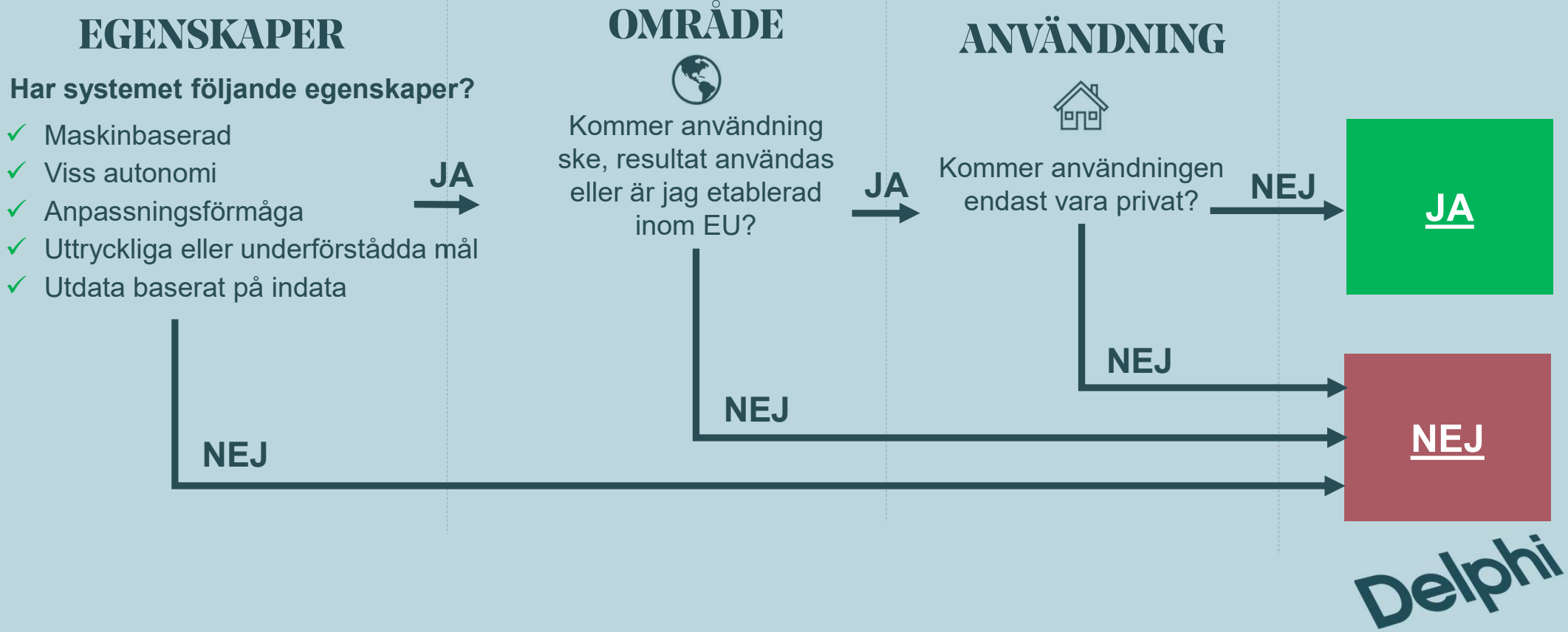
Delphi

3. Riskklassificera AI-systemet

Risk	Exempel på riskfaktorer
Immateriella rättigheter	• Intrång i annans rätt • Förlust av kontroll över befintlig IP • Förlust av kontroll över skapat resultat
AI-förordningen	• Definition av AI • Roll • Användningsområden och risknivå
Informationssäkerhet	• Infosäk allmänt • AI-specifika risker

Delphi

Omfattas min AI-användning?



Delphi

Vilka aktörer träffas?

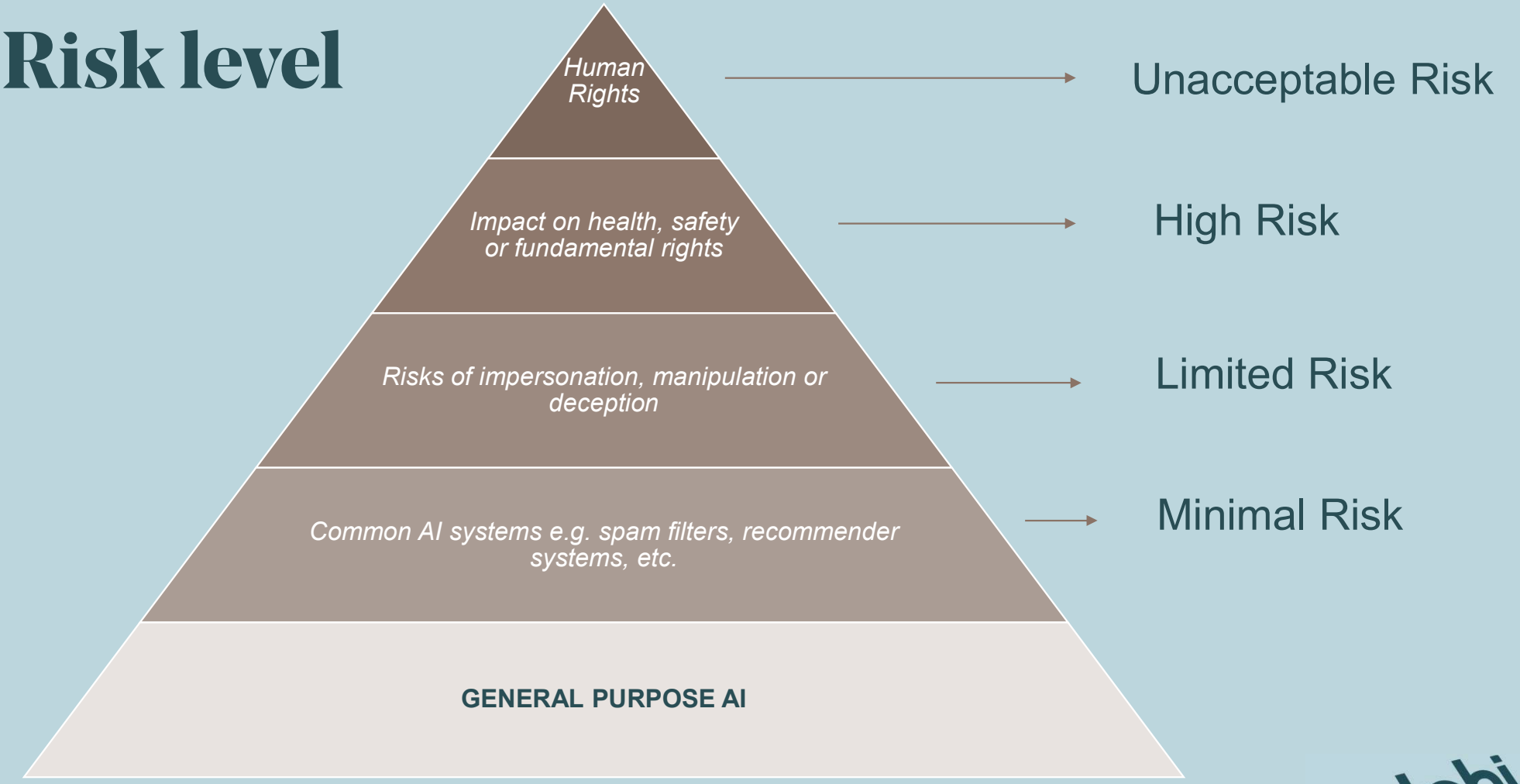
Obs! Ni kan kategoriseras som flera aktörer samtidigt

Leverantörer	Tillhanda-hållare	Importörer	Distributörer	Produkt-tillverkare	Ombud	Berörda personer som befinner sig i EU
Den som utvecklar eller låter utveckla AI-system eller en AI-modell för allmänna ändamål eller som har ett AI-system eller en AI-modell för allmänna ändamål och släpper ut det eller den på marknaden eller tar AI-systemet i bruk i eget namn eller under eget varumärke	Den som under eget överinseende använder ett AI-system, utom när AI-systemet används inom ramen för en personlig icke-yrkesmässig verksamhet	Den som befinner sig eller är etablerad i unionen och som släpper ut ett AI-system på marknaden som bär namnet på eller varumärket för en fysisk eller juridisk person som är etablerad i ett tredjeland	En annan än leverantören eller importören, som tillhandahåller ett AI-system på unionsmarknaden		Den som befinner sig i eller är etablerad i EU och som har fått och godtagit en skriftlig fullmakt från en leverantör av ett AI-system eller av en AI-modell för allmänna ändamål för att för dennes räkning fullgöra respektive genomföra de skyldigheter och förfaranden som fastställs i denna förordning	Användare
T.ex. OpenAI Google	T.ex. företag som implementerar AI:n i sin kundtjänstchatt					

Operatörer

Delphi

Risk level



Delphi

Högrisk-AI

- Högrisk AI inte förbjudet, men höga krav för dessa

Ansiktsigenkänning för att identifiera människor

Användning i kritisk infrastruktur, t.ex. vatten, el

Utbildning – antagning, bedöma fusk

HR – bedöma anställning, befordran etc.

Försäkring – besluta om rätt till försäkring

Kreditprövning

Det offentliga – AI som räknar ut om man har rätt till bidrag eller används vid val

Delphi

4. Vidta åtgärder baserat på risken

- Avtal
- Organisatoriskt
- Tekniskt

Delphi

5. Registrering, ansökningar m.m.

- Förhandssamråd
- AI-förordningen
- Sektorsspecifikt, finans m.m.
- Säkerhet

Delphi

Steg II: Fördjupad utredning av viktiga risker

6. Dataskydd – fördjupad analys

- Vad utgör personuppgifter?
- Ansvarsfördelning?
- Konsekvensbedömning
  - Förhandssamråd?
- Grundläggande principer och laglig grund
- Information
- Tekniska och organisatoriska åtgärder, incidenthantering
- Automatiserade beslut?

Delphi

7. Immaterialrätt – fördjupad analys

- Träning
- Input
- Output
- AI-modellen och mjukvaran i sig
- Användningsbegränsningar
- Tredjepartsmjukvara/open source
- Exit

Delphi

Steg III: Mitigeringsfasen

8. Försäkringar

- Traditionellt skydd ofta ej tillräckligt
- Mer under Avtalet

Delphi

9. Avtalet – I (typer av avtal)

- Avtal för molntjänster
  - PaaS, IaaS, SaaS
  - AIaaS
- Licensavtal
  - av AI
  - av data
- API-avtal
- Avtal om utveckling
- Forsknings- och samarbetsavtal

Delphi

9. Avtalet – II (avtalets innehåll)

- Tänk på alla relevanta rättigheter
  - **Rätt att använda indata**
  - **Rätt att använda, utveckla, göra ändringar etc. i AI-modellen**
  - **Rätt till tränad modell**
  - **Rätt till utdata**
  - **Vad är viktigt?**
- Personuppgiftsfrågor och sekretess
  - **Roller,** leverantörens användning, tredjelandsöverföringar m.m.
- **Servicenivåer, tillgång till processorkraft m.m.**
- **Begränsningar av hur AI-produkten får användas**
- Etik- och uppförandekoder
- Exponering för risker
  - **Begränsning av ansvar**
  - **”Super-caps”**
  - **Presumtioner**
- **Skadeslöshetsförbindelser**
  - **Vissa typer av skador**
  - **Immateriella rättigheter**
- Försäkringar hos leverantören
- Val av lag

Delphi

10. Interna policys m.m.

- Begränsningar kring användningsområden och funktionalitet (internt)
- Kontinuerlig utvärdering, fånga förändringar
- Tekniska och organisatoriska åtgärder
  - **Behörighetstilldelning**
  - **Utbildning**
  - **Kryptering**
  - **Datalagring**
- Certifieringar?
- Interna styrdokument och kontrollfunktioner (AI-policys)

Delphi

10. Interna policys m.m. forts.

AI kan användas av företag på, huvudsakligen, tre sätt

1. Som en assistent till det dagliga arbetet
2. För att leverera eller utveckla produkter eller tjänster
3. Som leverans av AI-tjänster som en produkt eller tjänst i sig självt

Delphi

10. Interna policys m.m. forts.

AI som assistent	AI som del av produktionen
Allmänna krav att data som används som datainmatning (prompts) inte är konfidentiell, skyddad av immateriella rättigheter eller integritetskänslig (men det beror på verktyget)	Följ andra befintliga policys gällande utveckling inom företaget
Central loggning av prompts rekommenderas för att säkerställa spårbarhet	Beakta konsekvenserna av AI-förordningen (minimal risk, begränsad risk [de flesta chatbots/Generativ AI], hög risk samt oacceptabel risk)
Utvärdera utdata för tillförlitlighet, immateriella rättigheter etc.	Granska kod som har genererats med hjälp av verktyg från tredje part för att undvika intrång i immateriella rättigheter eller krav på offentliggörande (GPL eller liknande)
	Kontrollera att tillämpliga EULAs eller försäljningsvillkor är förenliga med användningen av AI

Delphi

10. Interna policys m.m. forts.

AI policys/guidelines/instruktioner måste passa in i en redan existerande hierarki av policys kopplat till IT (IT, IT-säkerhet, Informationsklassificering, integritet, open source, IPR osv.)

- **IT och IT-säkerhet**: AI-verktyg är som vilket annat externt molnbaserat verktyg som helst, och vid upphandling ska det tas hänsyn till samma frågor.
- **Informationsklassificering**: Det måste fastställas vilka informationsklasser som kan användas i specifika AI-verktyg till följd av frågor gällande sekretess. Vissa verktyg tränar på data, medans vissa inte gör. Vissa kan användas i privata teknologistacks. Generella regler måste fastställas, då för hög detaljrikedom kan leda till risker och förvirring.

Delphi

10. Interna policys m.m. forts.

- **Immaterialrätt**: Produkter av AI skapar inte exklusiva rättigheter rent immaterialrättsligt än så länge. Ha detta i beaktande innan du gör verk som skapats av eller med hjälp av AI tillgängliga
- **Integritet**: Troligen måste en DPIA genomföras. Överväg överföringar till tredje part
- **Lista över tillåtna verktyg eller lista över otillåtna?**
  - **Fördelar: Kan öka känslan av säkerhet.**
  - **Nackdelar: Ökad byråkrati och hämmande effekt på kreativiteten. Mitt råd är en svartlista istället**
  - **Användningsområden?**

Delphi

Summering

- Tänk igenom er egen process för inköp
- Kartlägg interna behov och tänkt användning av tjänsten
- Sammanställ risker på relevanta områden
- Hantera riskerna genom:
  - **Avtalet**
  - **Tekniska åtgärder**
  - **Organisatoriska åtgärder**

Delphi


Tack!

Delphi

/ We love challenges