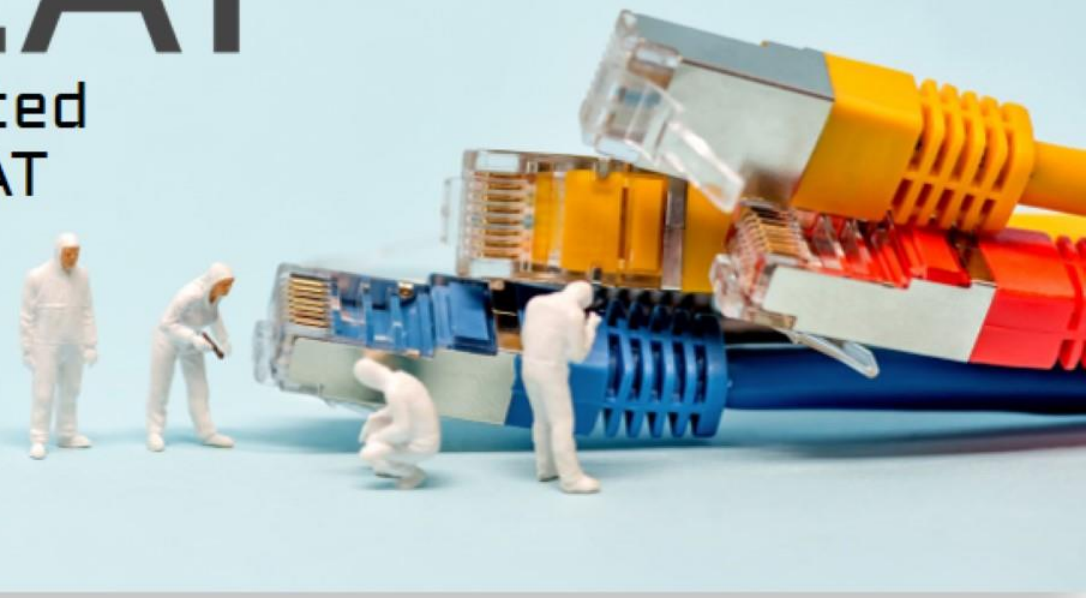
GREAT

Always connected
– that's GREAT



GREAT

Om GREAT

GREAT tror på digitaliseringens kraft och möjligheter genom att samarbeta, utbyta erfarenheter, driva debatt och sprida kunskap för att utveckla människor, företag och organisationer i Västsverige.

Vi är den naturliga samverkans-arenan för näringslivet, akademin och samhället i Västsverige kring aktuella IT-infrastruktur & digitaliseringsfrågor.

2004	50	8-10	WELL
startade	*medlemmar*	*aktiviteter/år*	*connected*

Medlemmar

Föreningen består av ett 50-tal aktörer; operatörer, företag, föreningar, universitet och högskolor, kommuner samt kommunala och regionala bolag. Som medlem ingår man i ett professionellt nätverk och man har möjlighet att vara med att påverka samt utveckla det digitala Västsverige.

Huvudsponsorer

Framtidens Bredband

Göteborgs Stad

Västra Götalandsregionen

GREAT

Verksamhet

Infrastruktur

Välfärdssamhället 2.0

Internet of Things

GREAT

GREAT verkar för det digitala samhällets utveckling, innovation och livskvalitet för individer, företag och organisationer.

great-it.se

SETTERWALLS

ETT ÅR MED GDPR

Setterwalls i samarbete med GREAT och Telia Sverige

JOHANNA PERSSON & BOBI MITROVIC

2019-05-22

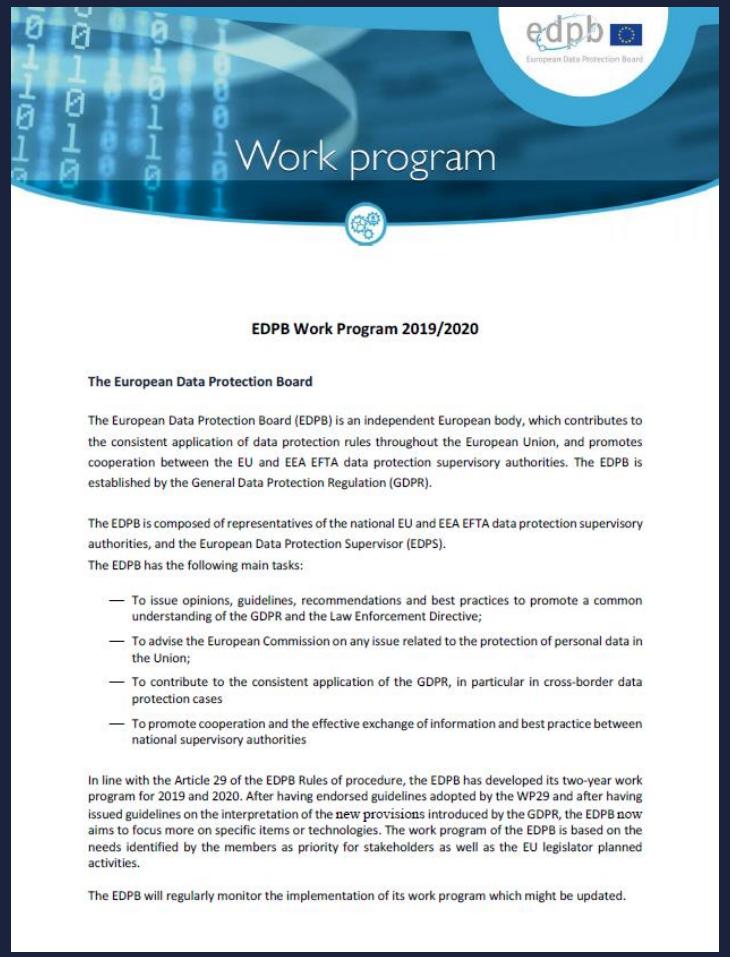
Agenda

- DEL 1 – Hur har tillsynsmyndigheterna agerat under det gångna året?
- DEL 2 – Vanligaste bristerna vid översyn av GDPR-compliance
- DEL 3 – Samtal med Telia Sveriges Dataskyddsombud Ida Mazzenga

DEL 1 - Hur har tillsynsmyndigheterna agerat under det gångna året?

Audits, incidenter och plan framåt

EDBPs aktiviteter under 2019 - 2020



EDPB Work Program 2019/2020

The European Data Protection Board

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU and EEA EFTA data protection supervisory authorities. The EDPB is established by the General Data Protection Regulation (GDPR).

The EDPB is composed of representatives of the national EU and EEA EFTA data protection supervisory authorities, and the European Data Protection Supervisor (EDPS).
The EDPB has the following main tasks:

- To issue opinions, guidelines, recommendations and best practices to promote a common understanding of the GDPR and the Law Enforcement Directive;
- To advise the European Commission on any issue related to the protection of personal data in the Union;
- To contribute to the consistent application of the GDPR, in particular in cross-border data protection cases
- To promote cooperation and the effective exchange of information and best practice between national supervisory authorities

In line with the Article 29 of the EDPB Rules of procedure, the EDPB has developed its two-year work program for 2019 and 2020. After having endorsed guidelines adopted by the WP29 and after having issued guidelines on the interpretation of the new provisions introduced by the GDPR, the EDPB now aims to focus more on specific items or technologies. The work program of the EDPB is based on the needs identified by the members as priority for stakeholders as well as the EU legislator planned activities.

The EDPB will regularly monitor the implementation of its work program which might be updated.

I. Guidelines

- Guidelines on Codes of Conduct and Monitoring Bodies
- Guidelines on delisting
- Guidelines on PSD2 and GDPR
- Guidelines on international transfers between public bodies for administrative cooperation purposes
- Guidelines Certification and Codes of Conduct as a tool for transfers
- Guidelines on Connected vehicles
- Guidelines on Certification (finalisation after the public consultation)
- Guidelines on video surveillance
- Guidelines on Data Protection by Design and by Default
- Guidelines on Targeting of social media users
- Guidelines on children's data
- Guidelines on reliance on Art. 6(1) b in the context of online services
- Guidelines on concepts of controller and processor (Update of the WP29 Opinion)
- Guidelines on the notion of legitimate interest of the data controller (Update of the WP29 Opinion)
- Guidelines on the Territorial Scope of the GDPR (finalisation after the public consultation)
- Guidelines on the powers of DPAs in accordance with Art. 47 of the Law Enforcement Directive
- Guidelines on data subjects rights with main focus at a first stage on the rights of access, erasure, objection, restriction and limitations to these rights

Tillsyn inom EU

- **Österrike** 2018-10-05: Sportcafé – ingen information om kameraövervakning.
- **Portugal** 2018-10-11: Sjukhus – ej vidtagit tillräckliga tekniska säkerhetsåtgärder.
- **Tyskland** 2018-11-22: Knuddels.de – ej vidtagit tillräckliga tekniska säkerhetsåtgärder.
- **Frankrike** 2019-01-21: Google –
    1. Ingen lättillgänglig information.
    2. Inte tillräckligt informativt, specifikt och otvetydigt samtycke vid individanpassad annonsering.
- **Österrike** 2019-02-12: Österreichische Post – dataanalys utgjorde behandling av känsliga personuppgifter.
- **Polen** 2019-03-26: Bisnode – ingen information vid scraping av personuppgifter.
- **Litauen** 2019-05-16: Betalningsleverantör – behandling av mer personuppgifter än nödvändigt samt ej anmäld personuppgiftsincident.

Datainspektionens tillsynsplan för 2019 - 2020

- **Prioriterade rättsområden**
  - Personuppgiftsansvarig eller personuppgiftsbiträde
  - Samtycke som rättslig grund
  - Gränsdragning mellan betaltjänstlagen och kreditupplysningsverksamhet
- **Exempel på branscher eller verksamheter under lupp**
  - Hälso- och sjukvården
  - Arbetsgivares behandling av anställdas personuppgifter
  - Mobila operativsystem
  - Detaljhandeln (särskilt kundklubbar)
  - Betalningsförmedlare
  - Nya tillämpningsområden för existerande teknik samt ny och utvecklad teknik

Datainspektionen

Datainspektionens styrdokument

Dnr: DI-2019-841
Beslutsdataum: 2019-03-19
Beslutad av: Generaldirektören

Tillsynsplan 2019-2020

Mål

Enligt Datainspektionens tillsynspolicy är ett övergripande mål för tillsynsverksamheten att nå så stora effekter som möjligt i skyddet av den personliga integriteten och att god sed iakttas i kreditupplysnings- och inkassoverksamhet. Datainspektionen kan inleda tillsyn i två olika spår – utifrån en riskbaserad, i förväg fastställd tillsynsplan eller med anledning av händelser i omvärlden. För att använda våra resurser så effektivt som möjligt prioriterar vi granskningar som bedöms få störst effekt för enskildas rättigheter i form av regelefterlevnad och lärande, både hos den verksamhet som granskas och hos andra myndigheter, företag och organisationer.

Tillsynsplan

Tillsynsplanen avser verksamhetsåren 2019 – 2020, men uppdateras årligen. Planen omfattar ett antal prioriterade områden där Datainspektionen identifierat att det finns särskild risk för att den enskildes rättigheter kan komma att kränkas och att det därför är särskilt viktigt att dessa behandlingar blir föremål för tillsyn.

Den riskbaserade tillsynen väljs utifrån tre aspekter där särskilda risker kan identifieras:

- Prioriterade rättsområden
- Specifika branscher eller verksamheter
- Nya företeelser

Årets prioriterade områden har identifierats genom de klagomål och personuppgiftsincidenter som inkommit till Datainspektionen, erfarenheter från tidigare genomförd tillsyn, generell omvärldsbevakning och utifrån aktuella regelförändringar. Utifrån dessa källor sker också löpande under året urvalet av vilka faktiska tillsynsobjekt som blir föremål för tillsyn

Datainspektionens tillsyn

- 2018-06-08: DI undersökte om 400 myndigheter och företag utsett dataskyddsombud. Varningar utdelas.
- 2018-06-11: Googles hantering av rätten att bli glömd.
- 2018-10-19: Generell översyn över samtycke som legal grund.
- 2018-12-03: SL-kontrollanters kroppsburna kameror.
- 2018-12-18: Kameraövervakning i omklädningsrum/vagnhall på brandstationer.
- 2019-01-21: Googles användning av GPS-data.
- 2019-02-21: Gymnasieskolas användning av ansiktsigenkänning för närvarokontroll.
- 2019-02-25: Privatpersoners kameraövervakning.
- 2019-03-04: 1177 Vårdguidens brister i krav på vidtagande av säkerhetsåtgärder.
- 25 mars 2019: Vårdgivares, universitetssjukhus och nätläkares (Kry) säkerhetsåtgärder för begränsning av tillgång till patientjournaler.
- 2019-04-01: Klarnas profilering baserat på köphistorik.

Incidenter 2018 (i Sverige)

2300 anmälda incidenter

DEL 2 - Vanligaste bristerna vid översyn av GDPR-compliance

Setterwalls findings

Personuppgiftsansvarig, personuppgiftsbiträde eller gemensamt ansvariga?

Rollfördelningen ICO/WP29/DIs översyn.

Ensam bestämmer ändamålen (varför) och medlen (hur).

Glidande skala mellan hur mycket hur/varför som krävs.

Biträdet har friheten att bestämma HUR viss behandling ska utföras. Inte bedöma varför uppgifterna samlas in och vilka.

Nivå av självständighet - teknisk kompetens för att göra ett urval/bedömning/för att utföra uppdraget.

T.ex. rekryteringsbolag – när HR anlitar

Advokatbyråer/revisionsbyråer

Hur är det med (resurs) konsulter?

- Agerar på instruktioner/ledning
- Saknar egen teknisk utrustning
- Delar inte något med arbetsgivaren

Information till de registrerade / transparens – Röd tråd

Tillräckligt tydlig information för att förstå, för respektive behandling:

- Ändamålet – specificera (FoU)
- Behandlingen – koppla flera till ett ändamål
- Typ av uppgift – ej för breda, inga t.ex., såsom, etc.
- Rättslig grund – inte flera
- Lagringsperioden – koppla till uppgiften/behandling
- Generalisera INTE inom respektive del

Olika uppgifter som ska lämnas ut

Rättighet	Grund	Grund	Grund	Övrigt
Data-portabilitet	Samtycke	Enligt avtal		Om automatiserad behandling
Invändningar	Intresseav-vägning (inkl. profilering)	Direkt marknads-föring	Allmänt intresse	Rätt ska uttryckligen meddelas, redovisas tydligt, klart och åtskilt
[…]				

Exempel på informationsbrister

- **Behandlingen**

”Personuppgifterna behandlas **i huvudsak för** att uppfylla… skyldigheter enligt lag. I samband med bolagsstämma används uppgifterna också för registrering, upprättande av röstlängd för bolagsstämman och, i förekommande fall, stämmoprotokoll”.

- **Typ av uppgift**

”När du surfar på vår webbplats, tar direktkontakt med … eller på annat sätt lämnar personuppgifter till oss, samlar vi in och behandlar dessa personuppgifter. Personuppgifterna som behandlas **består främst av** kontaktuppgifter samt teknisk information om ditt besök på vår webbplats som samlas in via vår användning av cookies, som beskrivs längre ner i denna policy. För att prenumerera på pressmeddelanden och/eller finansiella rapporter behöver du lämna din e-postadress till oss. … använder inte din e-postadress för andra ändamål än att skicka pressmeddelanden och finansiella rapporter som du valt att prenumerera på”.

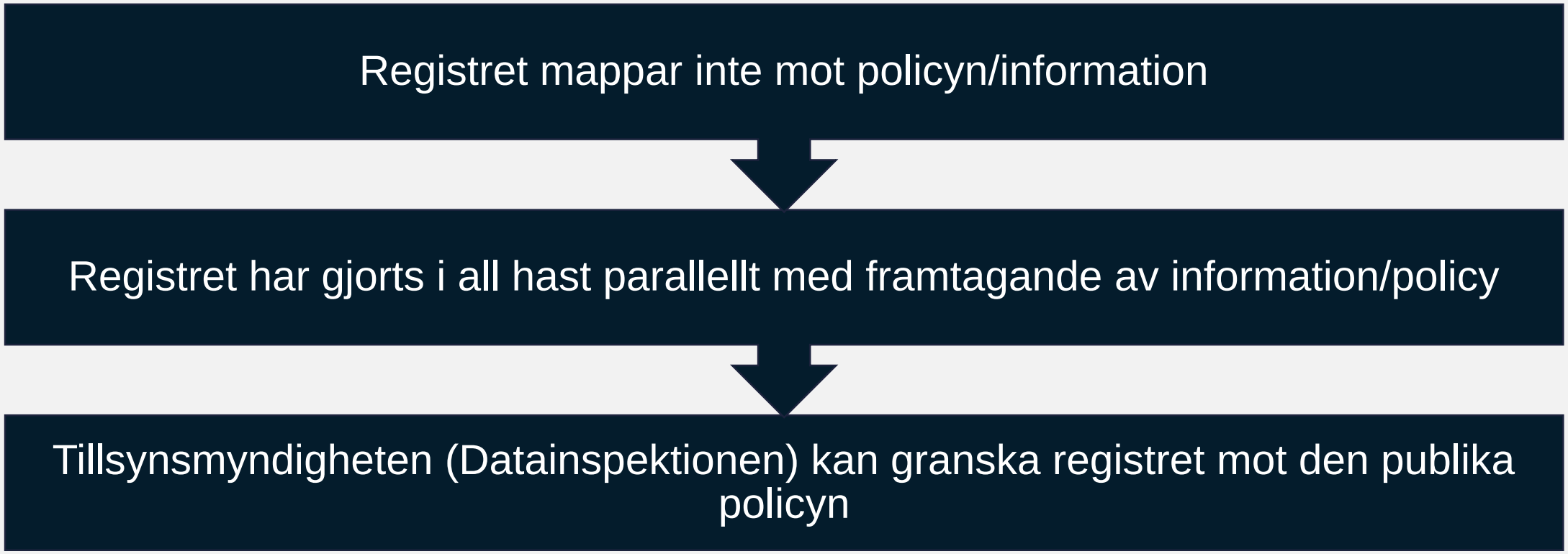
- **Rättslig grund**

”Vår rättsliga grund för ovan behandlingar är att förbereda och **fullgöra avtal och fullgöra rättsliga förpliktelser**. Om personuppgifterna är känsliga, behandlar vi dina personuppgifter för **att fastställa, göra gällande och försvara rättsliga anspråk** samt för att vår behandling är nödvändig för ett viktigt **allmänt intresse** enligt de lagar och regler som gäller för vår verksamhet”.

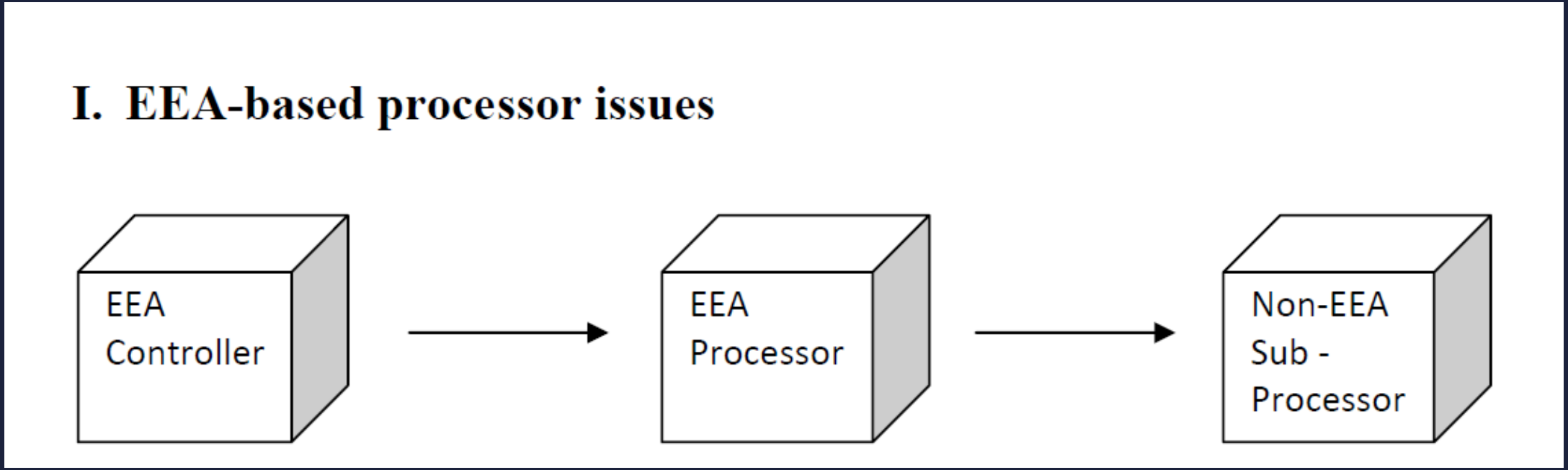
- **Lagringstiden**

”Vi spar dina personuppgifter **så länge de behövs**”.

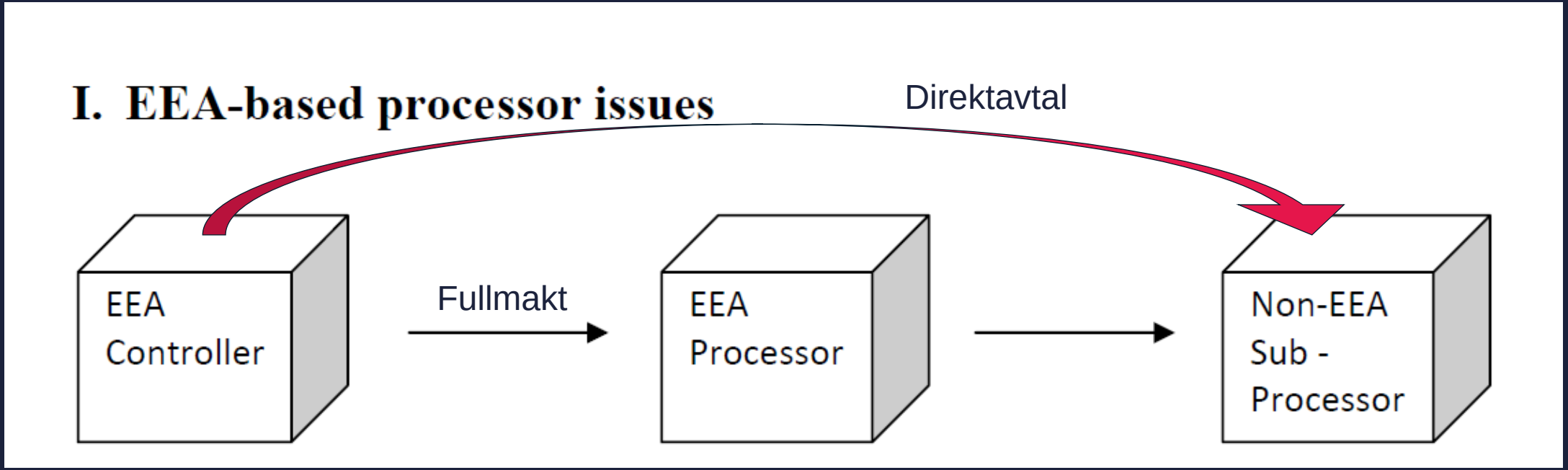
Art 30 registret - vilka ändamål som angivits



Biträdet måste vara i 3e land (ej bara underbiträdet)



Data exporter / data importer



Forts.

- **Krav**
- Vem är part till avtalet?
- Är del av avtalet inte tillämpligt?
- Koncernen / användare / konsulter

STANDARDAVTALSKLAUSULER ("registerförare")

Standardavtalsklausuler enligt artikel 26.2 i direktiv 95/46/EG för överföring av personuppgifter till registerförare i tredjeländer med otillräckligt uppgiftsskydd

Namn på den uppgiftsutförande organisationen: .....

Adress: .....

Tfn .....; Fax .....;E-postadress: .....

Övriga uppgifter som krävs för att identifiera organisationen:

.....

("Uppgifts**utföraren**")

och

Namn på den uppgiftsinförande organisationen: .....

Adress: .....

Tfn .....; Fax .....;E-postadress: .....

Övriga uppgifter som krävs för att identifiera organisationen:

.....

("Uppgifts**införaren**")

var och en "part", tillsammans "parterna".

Koncerninterna avtal

Krav

- Det koncerninterna avtalet ska innehålla en separat bilaga för respektive personuppgiftsansvarig/-biträderelation

Tillvägagångssätt

- Vikten av att kartläggning av behandling innan ett koncerninternt avtal kan fyllas i
- Bifoga dokument som redogör för matris över behandlingarna mellan koncernbolagen.

Bolag	Behandling		
PuA / PuB	1	2	3
1			
2			
3			

Biträdesavtal

Krav

- Hur avtalet ingåtts – undertecknat?
- Motstående mallar?
- Många leverantörer vs. många kunder.
- Utskick utan ifylld bilaga/instruktion – anpassad instruktion för varje avtal.
- Ensidiga ändringar – praxis enligt vissa branscher – ej för GDPR.
- Möjlighet att begränsa ansvaret.

Biträdesavtal

- Identifiera viktiga leverantörer baserat på:
  - uppgifternas **känslighet,**
  - **volym** av uppgifter och/eller registrerade,
  - **3e landsöverföring**, och
  - **Leverantörens utsatthet** baserat på storlek eller allmänhetens intresse av granskning av tillsynsmyndighet (t.ex. Microsoft och andra stora välkända IT-leverantörer).
- **Prioritera** leverantörer – ta fram åtgärdsplan.
- Rutin för att prioritera nya leverantörer.

Tillvägagångssätt

Samtycke

Krav – giltigt samtycke ska vara:

Frivilligt,
Specifikt,
Informerat, och
Otvetydigt.

Problematik

Samtycket är för brett (inhämtas för deltagande i flera eller framtida projekt - uppfyller därmed ej transparenskravet)

Samtycke från anställd

Krav
Ett samtycke måste lämnas frivilligt för att vara en rättslig grund för behandling.

Problematik
Det beroendeförhållande som föreligger mellan anställd och arbetsgivare gör det problematiskt att visa att samtycket är lämnat frivilligt.

Samtycke för profilering

- Hur har uppgifterna samlats in?
- Cookies
- Genom kundklubb/kundförhållande
- Kundklubb – avtal som rättslig grund?
- Graden av profilering

Vad innefattar samtycket?

- Vilka uppgifter
- Ändamålet profilering
- Ändamålet marknadsföring
- Ändamålet delning

Whistleblowing-funktion

Krav
Det ska finnas tydliga instruktioner som begränsar whistleblowing-funktionen till de begränsningar som finns.

Tillvägagångssätt

- Riktlinjer hur whistleblowing får användas.
- Undersök tekniska möjligheter att begränsa rapportering i WB-systemet

Samtal med Telia Sveriges Dataskyddsombud Ida Mazzenga

Konsekvensbedömning

Sannolikt hög risk för registrerades rättigheter och friheter?

<u>Nio kriterier, bl.a:</u>

Användning av ny teknik eller nya organisatoriska lösningar.

Uppgifter i stor omfattning.

Uppgifter om personer som befinner sig i ett underläge/beroendeställning och därför är sårbara, t.ex. anställda.

<u>Utgångpunkt</u>

Om två eller fler kriterier är uppfyllda ska en konsekvensbedömning göras!

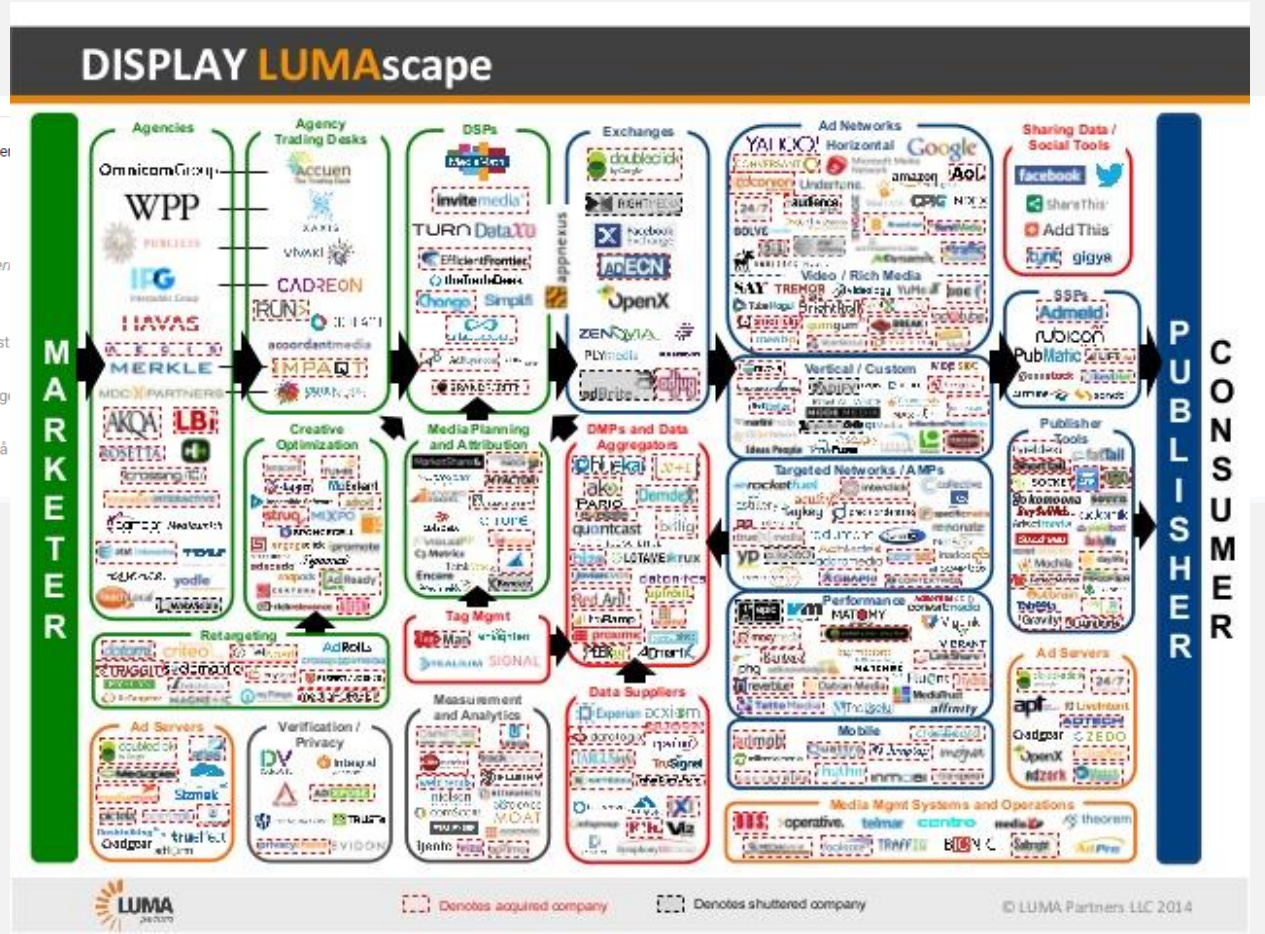
Cookies – vilka används

Inställningar för datadelning

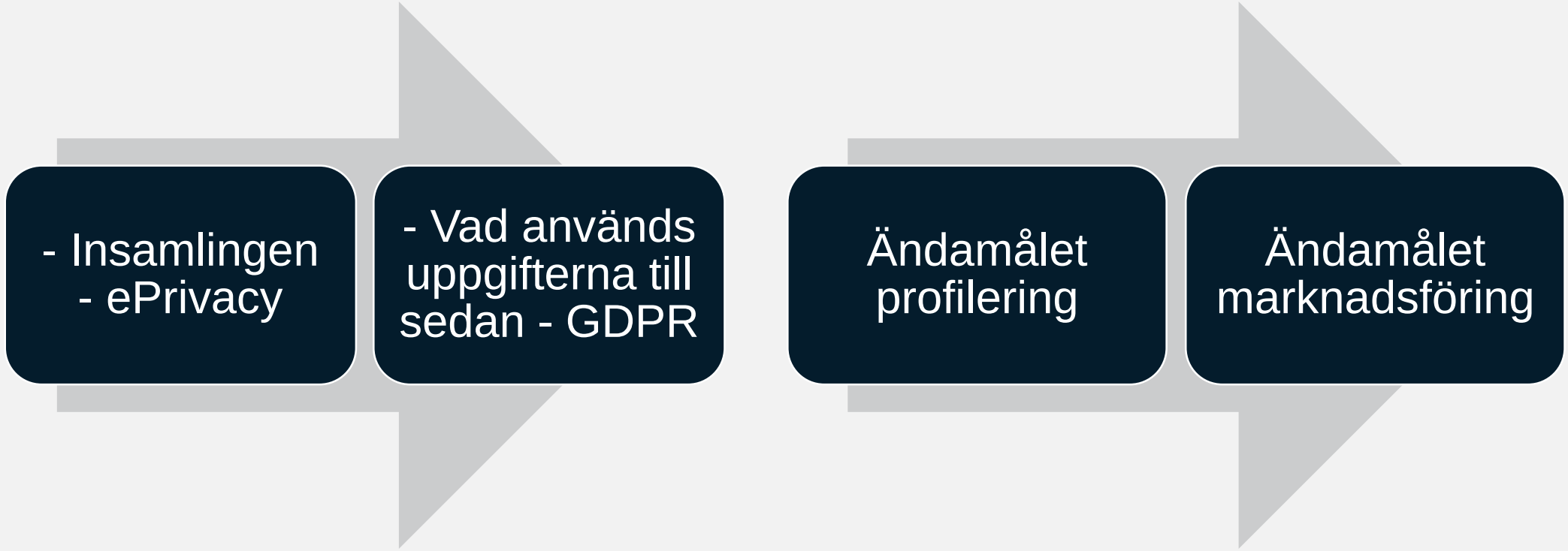
Data som du samlar in, bearbetar och lagrar med hjälp av Google Analytics ("Google Analytics-data") är säker och konfidentiell. Der
sekretesspolicy.

Med alternativen för datadelning kan du ange hur informationen i Google Analytics ska delas med andra. Läs mer.

- [x] Produkter och tjänster från Google REKOMMENDERAS
  Dela Google Analytics-data med Google och bidra till att förbättra Googles produkter och tjänster. *Om du inaktiverar detta alter*
  inställningarna. Visa exempel
- [x] Benchmarking REKOMMENDERAS
  Bidra med anonym data till en samlad datamängd för funktioner som benchmarking och publiceringar som kan hjälpa dig först
- [x] Teknisk support REKOMMENDERAS
  Ge vid behov Googles tekniska supportansvariga åtkomst till din Google Analytics-data och ditt Analytics-konto så att de kan g
- [x] Kontospecialister REKOMMENDERAS
  Ge Googles marknadsföringsspecialister och säljspecialister åtkomst till din Google Analytics-data och ditt Analytics-konto, så
  på Google.



Cookies – ändamålet



Kontakt

Johanna Persson

ASSOCIATE

T: +46 31 701 17 68
M: +46 72 529 32 64
E: Johanna.Persson@Setterwalls.se

HUVUDSAKLIGEN VERKSAM INOM

IT-rätt & dataskydd / Life Sciences / Immaterialrätt, marknadsrätt & mediarätt / Kommersiella avtal / IT, teknologi & telekom / Compliance & investigations

Bobi Mitrovic

SPECIALIST COUNSEL, ADVOKAT

T: +46 31 701 17 55
M: +46 73 270 61 40
E: Bobi.Mitrovic@Setterwalls.se

HUVUDSAKLIGEN VERKSAM INOM

Compliance & investigations / Immaterialrätt, marknadsrätt & mediarätt / IT-rätt & dataskydd / Kommersiella avtal / Fordonsindustri / IT, teknologi & telekom / Life Sciences

SINCERELY.
WE MEET AGAIN!