

GDPR

EU:s nya Dataskyddsförordning - *MARKNADSFÖRING*

Utbildning / ERFA Workshop

Wednesday Relations + MarLaw

2017-12-06

Advokatfirman MarLaw
Henrik Palmcrantz

MarLaw

ERFA workshop-deltagare ("Vem är vem?")

- o GDPR projektet på ditt företag
- o Utmaningar ni har på företaget och i projektet
- o Möjligheter ni ser med GDPR
- o Status och hur långt ni kommit

Disposition

09.30 | GDPR for marketing

Inledning om EU:s strategi "Digital Single Market", allmänt om Dataskyddsförordningen (GDPR), grundläggande begrepp, principer för behandling och laglig grund för behandling, informations- och kommunikationskrav, praktiska arbetsmoment, inventering-kategorisering-kartläggning.

10.30 | Fikapaus

10.45 | Fortsättning föredrag och diskussion

Direktmarknadsföring. e-postreklam och CRM-system. Digital marknadsföring, bildhantering och sociala medier.

11.45 | Lunch och nätverksdiskussion

13:00 | Casediskussion. Genomgång vad gör företag

14.45 | Fikapaus

15.00 | Casediskussion Genomgång vad gör företag

16.30 | Avslutning

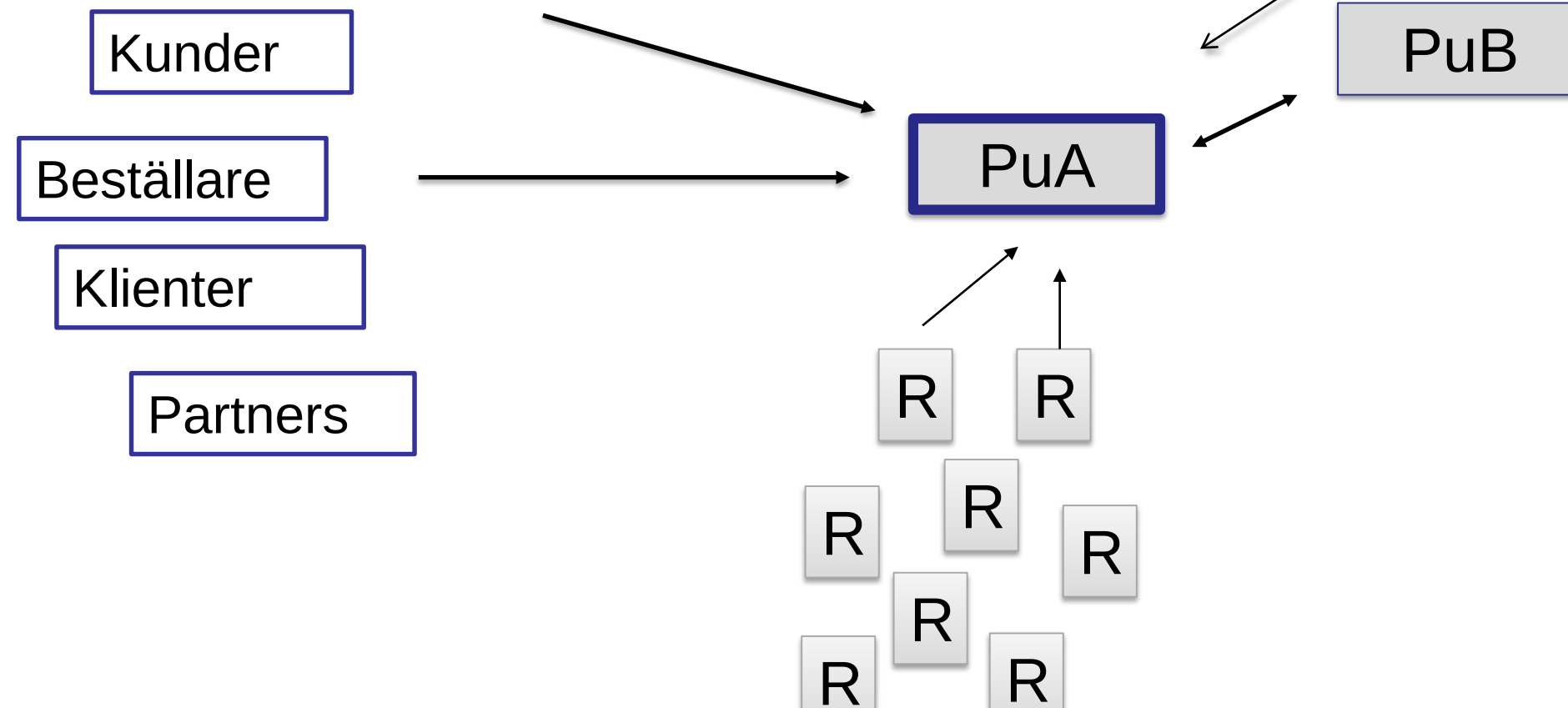
#digitalsinglemarket

Allmänt om GDPR (huvuddrag)

- GDPR – tillämpas (direkt) fr.o.m. 25 maj 2018
- Detaljerad lagstiftningsprodukt (173 skäl, 99 artiklar)
- I grund och botten samma grundläggande principer
- Kodifiering – samt vissa nyheter
- Skärpt reglering
 - tydligare krav på ansvariga
 - utökade krav på dokumentation
 - tydligare rättigheter för registrerade
 - skärpta sanktioner och tillsyn (?)
- Bred tillämplighet
 - ✓ Hela EU + extraterritoriell effekt
 - ✓ Företag, organisationer och myndigheter
 - ✓ Teknikoberoende

Allmänt om GDPR (huvuddrag)

- Skärpt reglering
 - tydligare krav på ansvariga
 - tydligare rättigheter för registrerade
 - skärpta sanktioner och tillsyn (?)



Grundläggande begrepp

□ Personuppgift

varje upplysning som avser en identifierad eller identifierbar fysisk person (Registrerad)...

... varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras...

...särskilt med hänvisning till identifierare som namn, identifikationsnummer, en lokaliseringssuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet (**Art. 4.1**)

Grundläggande begrepp

□ Personuppgift?

- namn.efternamn@privatmail.se
 - påhittatnamn@privatmail.se
 - förnamn@jobbmail.se
 - mail@jobbet.se
- ...
- organisationsnummer
 - företagsadress
 - fast telefon nr till kontoret

Grundläggande begrepp

□ Personuppgift?

- Identifikationsnummer... (t.ex. kundnummer, interna id)
- Lokaliseringsuppgift... (t.ex. platsdata)
- Online-identifikatorer (t.ex. IP-nummer)
- faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet
- ... bilder, registreringsnummer, kundnummer, användarnamn, kontonummer, etc. etc.....

Grundläggande begrepp

☐ Registrerad

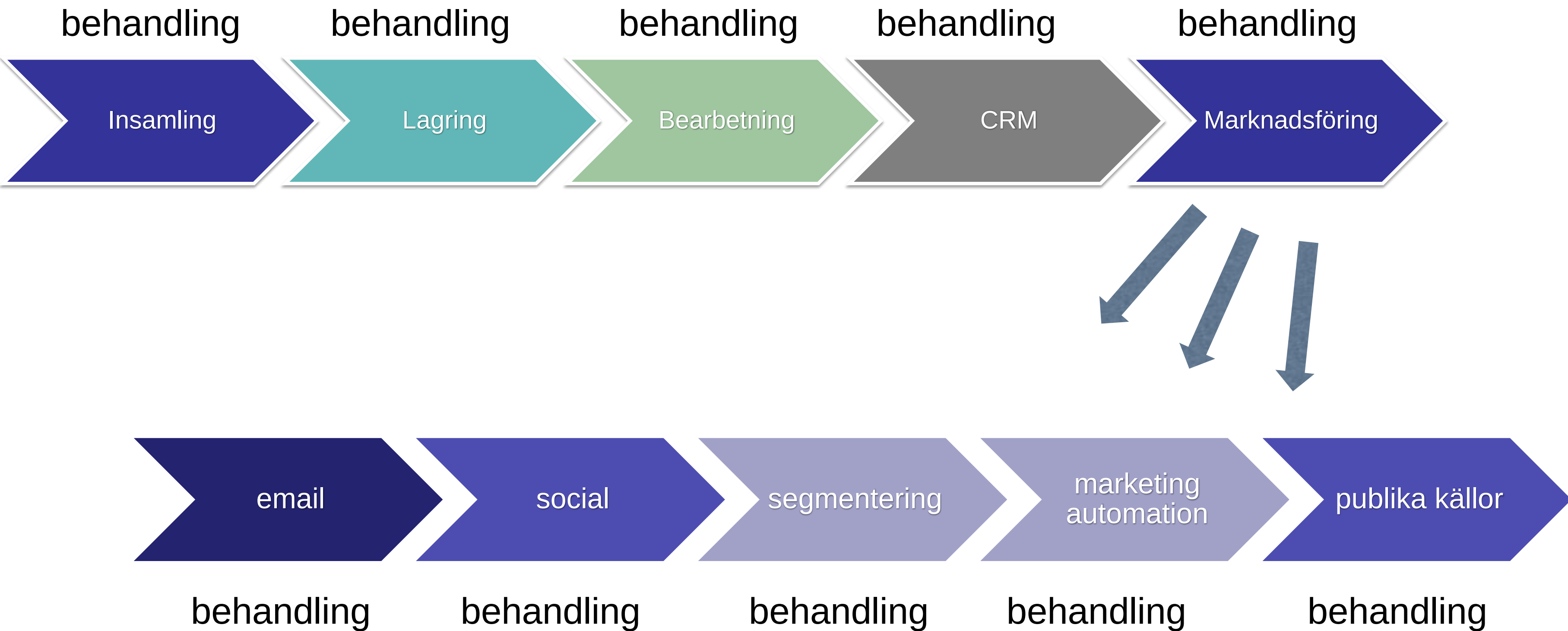
identifierad eller identifierbar fysisk person
som personuppgift avser = Registrerad (R)

Grundläggande begrepp

□ **Behandling**

en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej...

... såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring
(Art. 4.2)



Grundläggande begrepp

□ Personuppgiftsansvarig (PuA)

en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter;

... om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt
(Art. 4.7)

Grundläggande begrepp

❑ Personuppgiftsbiträde (PuB)

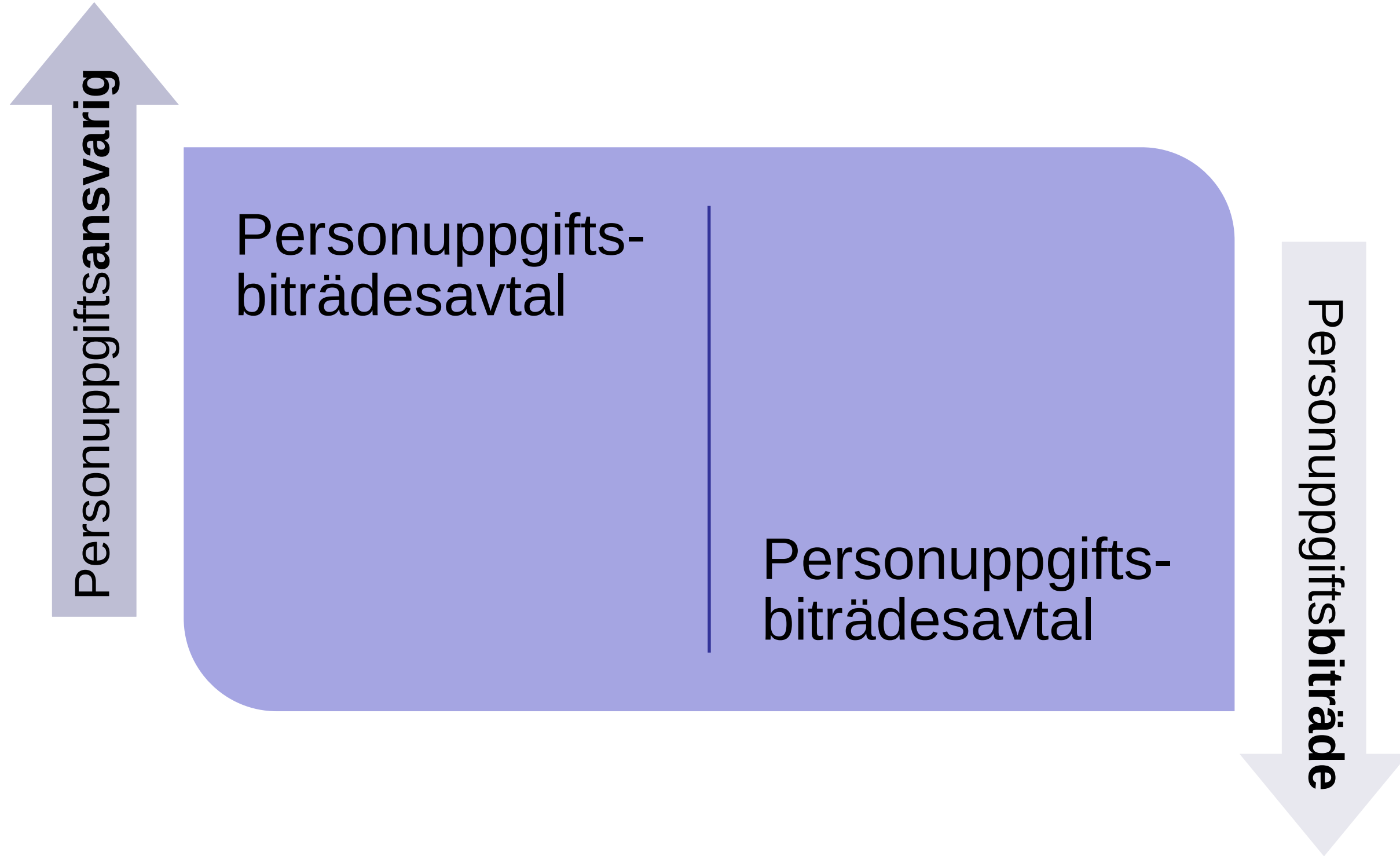
en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning
(Art. 4.8)

Grundläggande begrepp

- ☐ Personuppgiftsansvarig (PuA)
- ☐ Personuppgiftsbiträde (PuB)

Dubbelt och delat ansvar...

PuA ska endast anlita PuB som ger *tillräckliga garantier* om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas
(Art. 28.1)



Principer för behandling

- ☐ Laglighet, korrekthet och öppenhet
- ☐ Ändamålsbegränsning
- ☐ Uppgiftsminimering
- ☐ Korrekthet (personuppgifter)
- ☐ Lagringsminimering
- ☐ Integritet och konfidentialitet
- ☐ PuA ansvarar för och ska kunna visa att detta efterlevs
("ansvarsskyldighet" → *dokumentationsskyldighet*)

Laglig grund för behandling

☐ **Samtycke** från registrerad

☐ Nödvändigt för att fullgöra **avtal**

☐ Nödvändig för att fullgöra en **rättslig förpliktelse**

☐ Nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person

☐ Nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning

☐ Nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts **berättigade intressen**, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter,

- särskilt när den registrerade är ett barn
- (gäller ej myndigheter i fullgörande av sina uppgifter)

Principer för behandling + Laglig grund för behandling =

... ett grundläggande arbete för PuA / PuB

☐ Inventering

☐ Kategorisering

☐ Kartläggning

☐ Motivering (*rättfärdigande*)

Initialt praktiskt arbete

☐ Inventering →

✓ En mängd uppgifter hittas
(Art. 4 GDPR, "*indirekt
identifieras...*")

☐ Kategorisering →
(*personuppgifter*)

✓ Uppgifterna delas in i logiska
kategorier (beroende på
behandling)

☐ Kategorisering →
(behandling)

✓ Olika behandlingar, olika lagliga
grunder, etc.

☐ Kartläggning →

✓ Var skickas uppgifter? PuB,
utomlands?

Grundläggande begrepp

❑ "Särskilda kategorier" (av personuppgifter)

Behandling av personuppgifter som avslöjar:

Ras, etniskt ursprung, politiska åsikter, religiös övertygelse, filosofisk övertygelse, medlemskap i fackförening, behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa, uppgifter om en fysisk persons sexualliv eller sexuella läggning
ska vara förbjuden
(Art. 9.1)

Undantag: Uttryckligt samtycke, fullgöra skyldighet/rättighet inom arbetsrätt/socialt skydd, skydda grundläggande intressen, inom ramen för berättigad verksamhet (om lämpligt skydd), uppgifter tydligt offentliggjorda av registrerad

Ostrukturerad personuppgiftsbehandling?

❑ "missbruksregeln" (PUL)

Nu gällande undantag, personuppgifter i ostrukturerat material:
"...Ostrukturerad behandling får utföras så länge behandlingen inte innebär en kränkning (missbruk) av den registrerades personliga integritet."

- Upphör att existera under GDPR (!)
- Innebär att GDPR tillämpas för all behandling
- Även ostrukturerat material (mail, sociala medier, etc.)

... sociala medier? ... mail?

- Innebär ofta PU-behandling i ostrukturerad form
- Nuvarande missbruksregeln

På vilken grund kan PU i sociala medier behandlas efter den 25 maj 2017?

Avtal / Berättigat intresse / Intresseavvägning?

- Avvägning om lämplig användning av social...
- Uppgiftsminimering...?
- Informationstext...?

Informations- och kommunikationskrav

De registrerades rättigheter



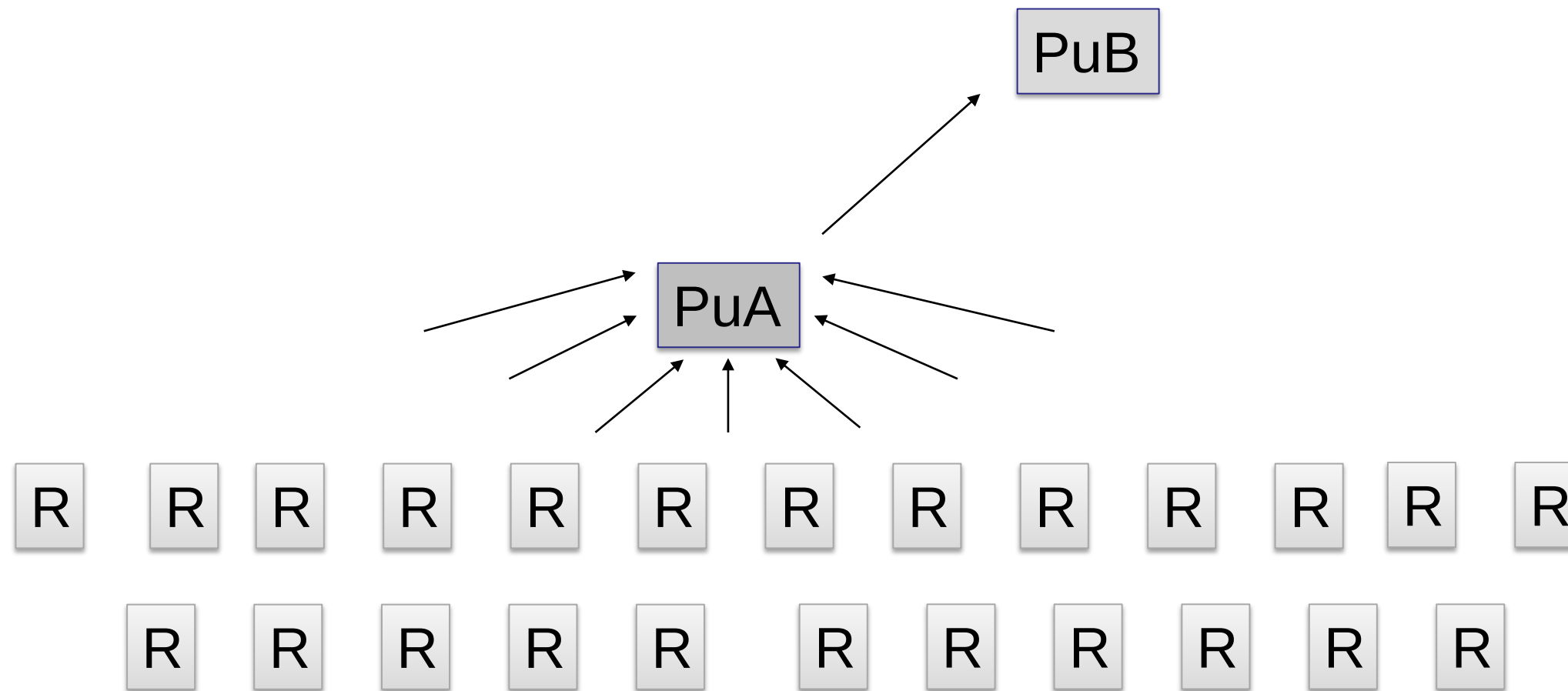
”transparens & insyn”



Skyldigheter för PuA/PuB

Information till vem?

Art. 4 *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad)... ("**R**")



Informations- och kommunikationskrav

- Art. 12.1

PuA ska vidta lämpliga åtgärder för att till Registrerade tillhandahålla all information och kommunikation avseende behandling...

... i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk...

Informations- och kommunikationskrav

- Art. 13.1

PuA ska när personuppgifterna erhålls till R lämna information om

- a) Identitet, kontaktuppgifter, företrädare för PuA
- b) Kontaktuppgift DSO
- c) Ändamål och rättslig grund för behandling
- d) Berättigade intressen (om intresseavvägning som grund)
- e) Mottagare av personuppgifter
- f) Överföring till annat land

Informations- och kommunikationskrav

- Art. 13.2

Ytterligare info för att "säkerställa rättvis och transparent behandling"

- a) Lagringsperiod alternativt kriterier för att fastställa sådan period
- b) Rätt till tillgång, rättelse, radering, begränsning av behandling, rätt att invända mot behandling samt rätt till dataportabilitet
- c) Rätt att återkalla samtycke
- d) Rätt att inge klagomål till en tillsynsmyndighet (Di)
- e) Huruvida tillhandahållandet av personuppgifter är lagkrav, krav enligt avtal, nödvändigt för att ingå avtal, etc.
- f) Förekomst av automatiserat beslutsfattande, profilering samt meningsfull information om logiken bakom, betydelse och följder av sådan behandling för R

Informationskrav – Praktiska arbetsmoment

- ✓ Upprätta text/personuppgiftpolicy som täcker all information
- ✓ Anpassa text(er)/policydokument till specialfall
- ✓ Se över i vilka situationer källan är R och inte
- ✓ Lämpligt format (skriftlig, om lämpligt elektroniskt)
- ✓ ...kom ihåg att efterleva test/policydokument över tid!

Informationskrav – Praktiska arbetsmoment (marknadsföring)

- ✓ Hur når vi ut med rätt information till rätt registrerade?
- ✓ Har vi fått personuppgifterna från en annan källa än de registrerade själva?
- ✓ ... koncis, klart och tydligt, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk...?
- ✓ Är de CRM/marknadsföringsverktyg vi vill använda kompatibla?
(Informations och kommunikationskrav)

Kommunikationskrav

Registrerade har rätt till...

- ☐ Tillgång (registerutdrag – redogörelse över behandling)
- ☐ Rättelse – få felaktiga uppgifter rättade
- ☐ Radering – om laglig grund inte längre finns
("bli glömd")
- ☐ Begränsning – behandlingen upphör i delar
(t.ex. invändning mot intresseavvägning)

... Samtliga kopplade till underrättelseskyldighet

Invändningar – DM (!)

Art. 21.2

R har rätt att när som helst invända mot **behandling för direktmarknadsföring**

(inkluderat profilering i samband med DM)

- Uppgifterna får då inte längre behandlas för DM-ändamål

Senast vid första kontakten med R ska denne informeras om sin rätt att invända...
... redovisas tydligt, klart och åtskilt från annan information.

Kommunikation – (begäran från R) Generella förhållningsregler

HR

- Respektera förfrågan
- Underlätta utövandet av R:s rättigheter
- Utan dröjsmål (tidsfrist 1 mån)
- Kostnadsfritt
- Format (matcha begäran)

U

- Uppenbart ogrundad
- Orimlig/särskilt om repetitiv
- Betvivla identitet – ytterligare info/kontroll
- Uppskov
(komplicerad begäran)

10.30 | Fikapaus

10.45 | Fortsättning föredrag och diskussion

Laglig grund för behandling

☒ Samtycke

☐ Avtal

☐ Rättslig förpliktelse

☐ (Nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person)

☐ Nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning

☒ Intresseavvägning

Samtycke

- Art. 4.11

Varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne

☐ PuA måste kunna visa att samtycke inhämtats korrekt

☐ Samtycket ska särskiljas

☐ Ska gå att återkalla lika enkelt som det lämnades

☐ Frivillighet... (reell möjlighet att tacka nej?)

☐ Informerat – samtyckestext/personuppgiftspolicy

Samtycke – överväganden?

- ☐ Praktiska möjligheter att inhämta giltiga samtycken?
- ☐ Administration (dokumentation)
- ☐ Följder av opt-out?
- ☐ Samtycke (GDPR) vs "informellt samtycke"
- ☐ Möjlighet att förlita sig på annan rättslig grund?

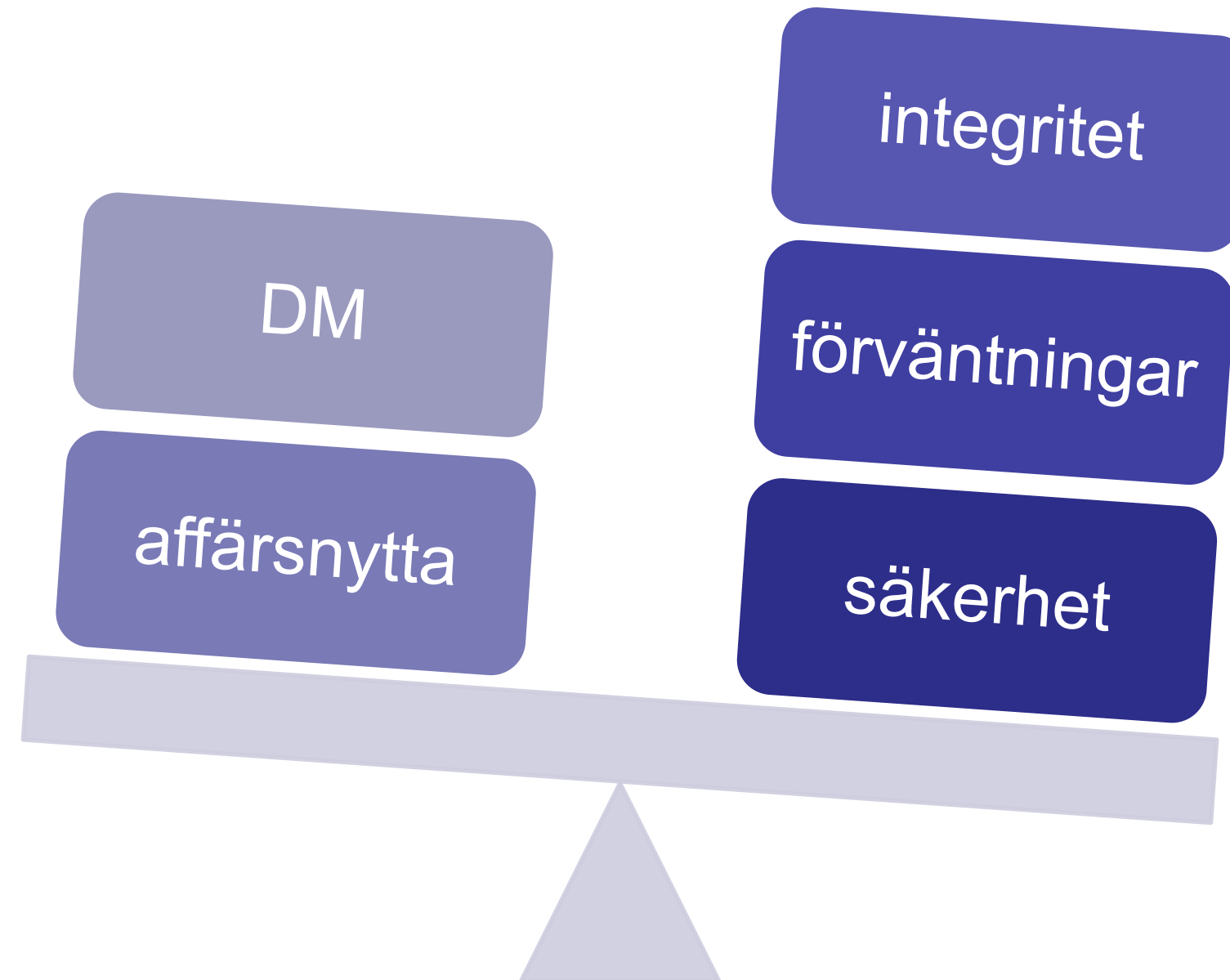
Laglig grund för behandling

- ☐ Samtycke
- ☐ Avtal
- ☐ Rättslig förpliktelse
- ☐ (Nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person)
- ☐ Nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning
- ☐ Intresseavvägning

Intresseavvägning (*berättigat intresse?*)

Behandlingen nödvändig för
ändamål som rör PuA / 3:e P
berättigade intressen

R:s intressen eller
grundläggande
rättigheter/friheter



Intresseavvägning (*berättigat intresse?*)

En personuppgiftsansvarigs berättigade intressen, inklusive intressena för en personuppgiftsansvarig till vilken personuppgifter får lämnas ut, eller för en tredje part, kan utgöra rättslig grund för behandling, på villkor att de registrerades intressen eller grundläggande rättigheter och friheter inte väger tyngre, med beaktande av de registrerades rimliga förväntningar till följd av förhållandet till den personuppgiftsansvarige [...]

Behandling av personuppgifter för direktmarknadsföring kan betraktas som ett berättigat intresse

(Skäl 47)

DM som "berättigat intresse"?

Anses i dagsläget utgöra ett berättigat intresse (SWEDMA)

✓ Opt-out lösning

☐ Inköp av register från tredje part? → Informationsskyldighet?

☐ Om DM/kontakt ej resulterar i kundrelation...

→ Finns annan rättslig grund för behandling? Om inte – radera?

Oavsett "samtycke", "intresseavvägning (eller annan rättslig grund)

- ☐ Hur uppfyller vi Informationskraven enligt GDPR?
- ☐ Hur efterlever vi grundläggande principer enligt GDPR?
(t.ex. ändamålsbegränsning, uppgifts- & lagringsminimering, etc.)
- ☐ Hur *skyddar* vi uppgifterna?

Säkerhetsåtgärder

Art. 32

PuA/PuB ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken...
.. med beaktande av

- ☐ Senaste utvecklingen
- ☐ Genomförandekostnader
- ☐ Behandlingens art, ändamål, omfattning, sammanhang
- ☐ Risk - för fysiska personers rättigheter och friheter
(sannolikhetsgrad och allvar)

Säkerhetsåtgärder

Tekniska

- ✓ Minimera uppgiftsbehandling
- ✓ Inbyggd dataskydd som standard (privacy-by-default)
- ✓ Pseudonymisering
- ✓ Brandvägg, antivirus, uppdaterad mjukvara, backup, kryptering, etc.
- ✓ Åtkomstlogg
- ✓ Tester

Organisatoriska

- ✓ Minimera uppgiftsbehandling
- ✓ Behörighetsstyrning
- ✓ Utbildning/rutiner
- ✓ Säkerhetspolicy
- ✓ Kontroll, avstämning

... (**även**) Fysisk säkerhet

Tillsyn och sanktioner

☐ Datainspektionen (2.0?)

- ✓ Anslag
- ✓ Större ansvarsområde
- ✓ Kontroll från EU (art. 29)

☐ Varje Registrerad får klaga inför Datainspektionen

☐ Registrerad som lidit skada till följd av överträdelse
kan kräva ersättning av PuA/PuB

☐ Allmän domstol (TR, HovR, HD)

Tillsyn och sanktioner

Administrativa sanktionsavgifter

Di har att tillse att sanktion i varje enskilt fall är effektivt, proportionellt, avskräckande

... hänsyn tas till bl.a.

- ☐ Överträdelsens karaktär, svårighet, varaktighet
- ☐ Uppsåt/oaktsamhet
- ☐ Åtgärder för att lindra skada
- ☐ Grad av ansvar med beaktande av säkerhetsåtgärder
- ☐ Tidigare överträdelser
- ☐ Samarbete med myndighet
- ☐ Berörda kategorier uppgifter

Tillsyn och sanktioner

Administrativa sanktionsavgifter

- Art. 83 Sanktionsnivåer (tak)

Upp till 10 000 000 EUR / 2 % av global årsomsättning

Upp till 20 000 000 EUR / 4 % av global årsomsättning

Två nivåer – kopplade till specifika bestämmelser i GDPR

Lägre – bl.a. skyldigheter avseende biträden, privacy-by-design, register, säkerhetsåtgärder, incident, DSO, certifiering.

Högre – bl.a. grundläggande principer, R:s rättigheter, underlåtenhet att rätta sig efter beslut, tredjelandsoverföring,

ePrivacy (förslag till e-integritets**förordning** – 25 maj 2018?)

Reglerar "elektronisk kommunikation"

cookies, metadata, spårningsteknologi online, opt-in, webbläsarinställningar, etc.

Kunskap - Praktiskt (eget) arbete – Extern hjälp

- ❖ Ett grundläggande arbete för PuA / PuB
[även för marknadsföringsavdelningen]
- ❖ Inventering → Kategorisering → Kartläggning
- ❖ Har vi rätt projektgrupp?
- ❖ Följer vi "principer för behandling"
- ❖ Har vi en "laglig grund för behandling"
(per kategori och per behandling)
- ❖ Vilka informationstexter måste vi sammanställa?
- ❖ Vilka avtal har vi (PuB-avtal)? → Upprätta/uppdatera

Kunskap - Praktiskt (eget) arbete – Extern hjälp

Specifikt för marknadsföringsavdelningen

- ❖ Vilka verktyg vill vi använda?
CRM, Marketing Automation, Tracking, Re-targeting, Social, etc.
- ❖ Externa leverantörer av verktyg/plattformar – biträdesavtal? Utomlands?
- ❖ Hur länge sparar vi uppgifter? När måste vi gallra?
- ❖ Hur jobbar marknad inom ramen för ett övergripande GDPR-projekt?
- ❖ Vilka särskilda informationstexter måste vi upprätta?

Initialt praktiskt kartläggningsarbete?

❑ Inventering →

✓ En mängd uppgifter hittas
(Art. 4 GDPR, "*indirekt
identifieras...*")

❑ Kategorisering →
(*personuppgifter*)

✓ Uppgifterna delas in i logiska
kategorier (beroende på
behandling)

❑ Kategorisering →
(behandling)

✓ Olika behandlingar, olika lagliga
grunder, etc.

❑ Kartläggning →

✓ Var skickas uppgifter? PuB,
utomlands?

❑ DPOrganizer

MarLaw



Henrik Palmcrantz

Senior bitr. jurist

Kontaktinformation

Telefon: + 46 76 215 45 43

henrik.palmcrantz@marlaw.se

Advokatfirman MarLaw AB

Sveavägen 31

P.O. Box 3079

103 61 Stockholm

Tel: +46 8 23 07 35

Fax: +46 8 796 75 33