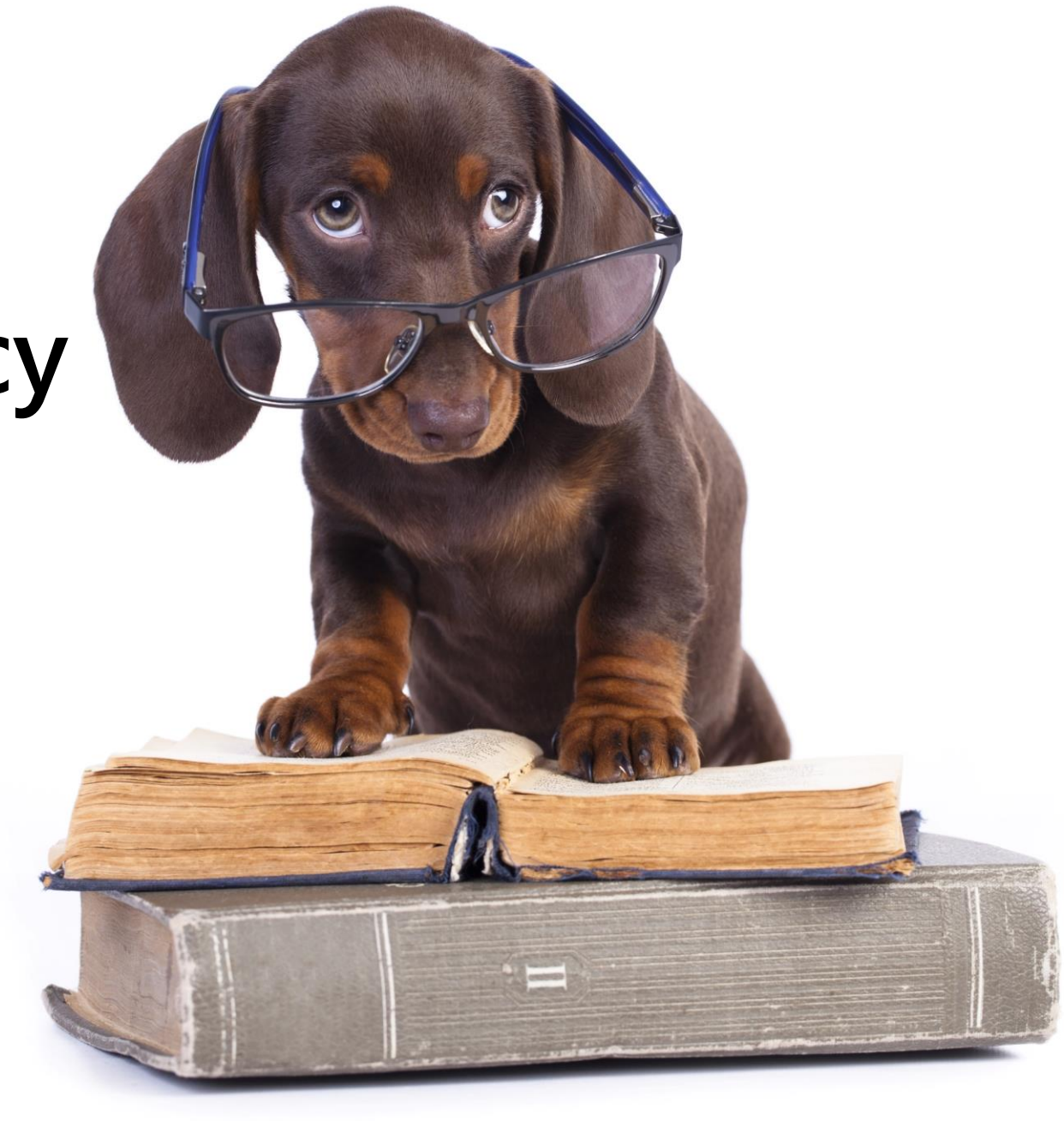
GDPR och E-Privacy för Marknad

Cecilia Arneving Juhlin

2018-01-24



moderamen CONSULTING

Vem är Cecilia?

- CRM
- Analys
- BI
- Produktledning
- Varumärke
- Strategi
- Styrning/Ledning

telenor
ICA
TELE2
Husqvarna
com hem
ERICSSON
IKEA
Danfoss
H&M
SVENSKA SPEL
projectplace
COMVIQ
Sony Ericsson
onninen
INVISIO

moderamen CONSULTING

Jag är inte jurist

moderamen CONSULTING

Agenda

08.30 - Registrering och morgonfika

09.00 - Vad är GDPR och vad är personuppgifter?

10.00 - Paus

10.15 - Fortsättning Genomgång GDPR

11.00 - Varför behandlar företag personuppgifter?

12.00 - Lunch

13.00 - Vad är E-Privacyförordningen (EPR) och vad säger Marknadsföringslagen?

14.00 - Case: Hur Svenska Spel förbereder sig inför GDPR

14.30 - Eftermiddagsfika

14.45 - Workshop kring era egna case

16.15 - Sammanfattning

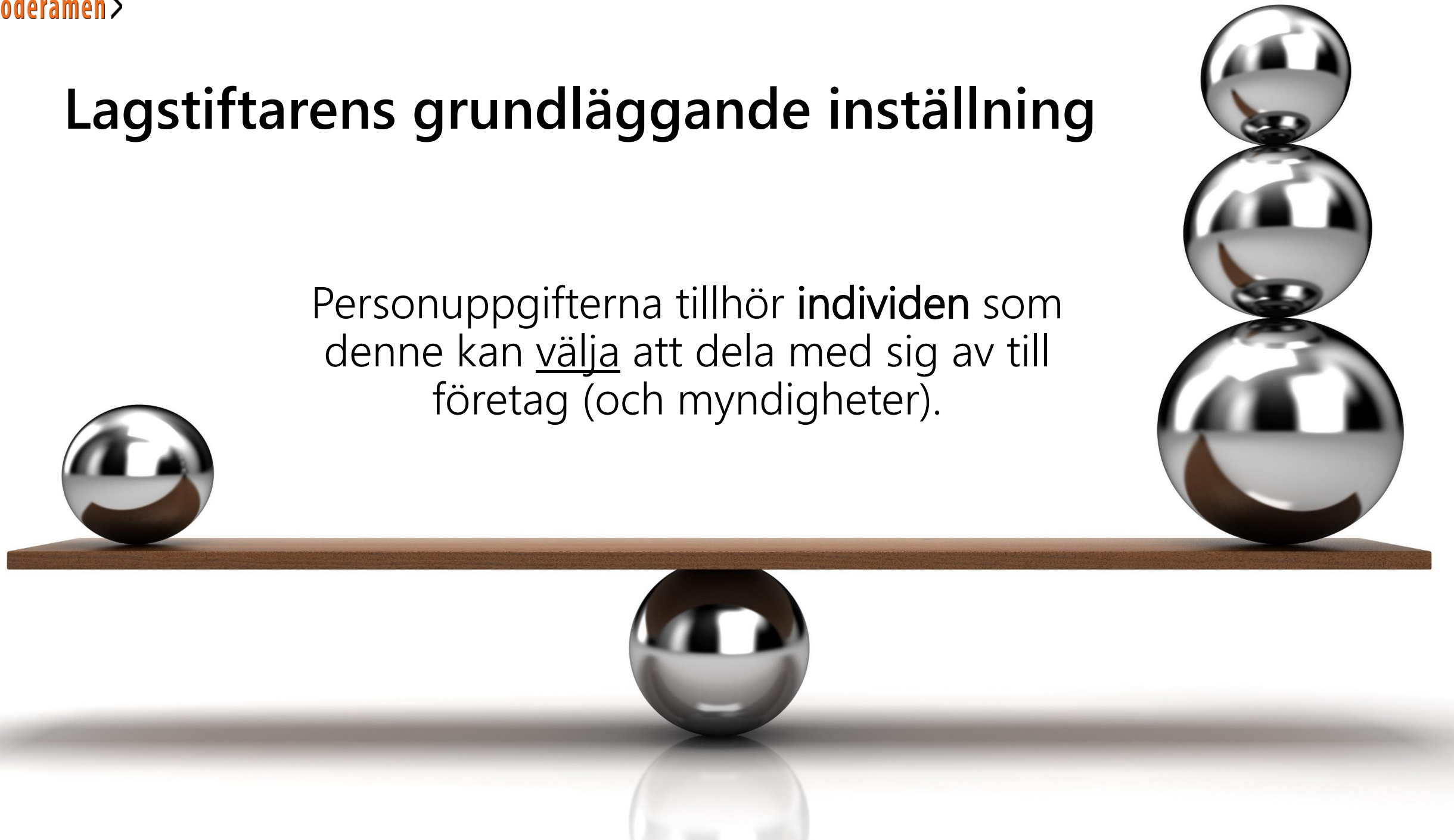
Vad är GDPR?

I stora drag..

- Ny EU-förordning som den 25 Maj 2018 ersätter Personuppgiftslagen (PUL) i Sverige
- Denna strängare lagstiftning har tagits fram på grund av:
  - Nuvarande dataskyddsdirektiv är ifrån 1995..
  - Större risk för kränkning givet digitaliseringen
  - Stärka integritetsskyddet
  - Behov av EU-harmonisering
- Brott mot lagen kan leda till höga ”sanktionsavgifter” på upp till 20 MEURO eller 4% av global årlig omsättning beroende på vilket som är högst.

Lagstiftarens grundläggande inställning

Personuppgifterna tillhör **individen** som denne kan välja att dela med sig av till företag (och myndigheter).



GDPR:S huvudprinciper

- Behandlingen ska vara **Laglig, Rättvis** och **Öppen**
- Det ska finnas tydliga syften med att behandla personuppgifterna (**Ändamålsbegränsning**)
- Kunden ska vara informerad om behandlingen och/eller ha godkänt den (**Samtycke, Fullgörande av avtal, Rättslig förpliktelse, Berättigat intresse** eller **Skydda intresse**)
- Insamlade uppgifter ska vara relevanta och korrekta för syftet (**Uppgiftsminimering och Korrekthet**)
- När anledningen till behandlingen är slutförd ska personuppgiften gallras (**Lagringsminimering/Gallring**)
- Individen ska enkelt kunna få tillgång till vilka personuppgifter som behandlas och varför (**Registerutdrag/dataportabilitet**)
- Uppgifterna ska behandlas på ett säkert sätt (**Integritet och konfidentialitet**)
- Företaget som behandlar personuppgifterna har **Ansvarsskyldighet**

Huvudsakliga skillnader mellan PUL och GDPR

PUL 	GDPR 
Syften med behandling av personuppgifter måste anges (men kan göras sammantaget) under ett ”samlat samtycke” (Praxis)	Aktivt separat samtycke till tydliga syften med behandlingen av personuppgifter måste möjliggöras. Samtycken får inte villkoras • Kunds rätt att neka profilering • Kunds rätt till dataportabilitet
Ingen anmälningsplikt vid läckor/felbehandling	Obligatoriskt att anmäla och informera om läckor av personuppgifter inom 72 timmar
Gäller ej behandling av ”ostrukturerat material”	Gäller även behandling av ”ostrukturerat material”
Generiska PUL-biträdesavtal	Detaljerad dokumentation av dataflöden mellan parter måste komplettera biträdesavtal
Tillsynsmyndigheten måste bevisa att ett företag bryter mot förordningen	Måste kunna bevisa att man är compliant
Inga större finansiella risker att bryta mot PUL (eventuellt varumärkesrisker)	Kännbara finansiella böter kan utdömas vid brott mot förordningen – upp till 4% av global årsomsättning samt skadestånd.

Vad är en personuppgift och vad är ”behandling”?

Vad är en personuppgift enligt förordningen?

”Varje upplysning som avser en identifierad eller identifierbar fysisk person (en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.”

Kort sagt – all typ av data som kan kopplas till en fysisk person på något sätt (även om det är krångligt..)

192.168.0.1

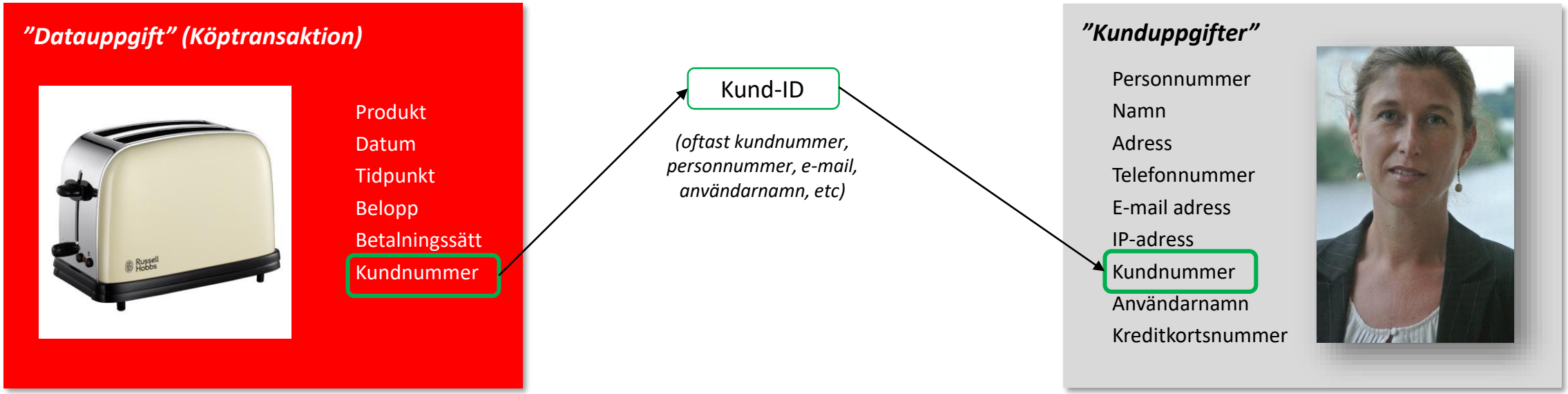
Vad är ”särskilda kategorier av personuppgifter?
(i PUL benämnda ”känsliga personuppgifter”)

”Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden”.

Separat uttryckligt Samtycke krävs.

Förtydligande kring ”personuppgifter”…

Personuppgifter kan därmed innebära antingen en förteckning av information som beskriver vem individen är (”Kunduppgift”) eller en ”datauppgift” (t ex en köptransaktion) som via ett Kund-ID eller ”nyckel” (t ex Kundnummer) kan koppla ”datauppgiften” till en fysisk person.



Alltså, så fort en datauppgift innehåller någon form av kund-ID så blir den en **personuppgift** och faller därmed in under Personuppgiftslagen (PUL) och från Maj 2018 under Dataskyddsförordningen (GDPR)

En datauppgift som är avidentifierad är inte längre en personuppgift

Genom att ta bort ”Kund-ID” från datauppgiften bryts kopplingen till kunduppgifterna och datauppgiften är därmed inte längre en personuppgift.

”Datauppgift” (Köptransaktion)

Produkt
Datum
Tidpunkt
Belopp
Betalningssätt
~~Kundnummer~~
Ålder
Kön
Kommun
Län

Kund-ID

(oftast kundnummer, personnummer, e-mail, användarnamn, etc)

”Kunduppgifter”

Personnummer
Namn
Adress
Telefonnummer
E-mail adress
IP-adress
Kundnummer
Användarnamn
Kreditkortsnummer

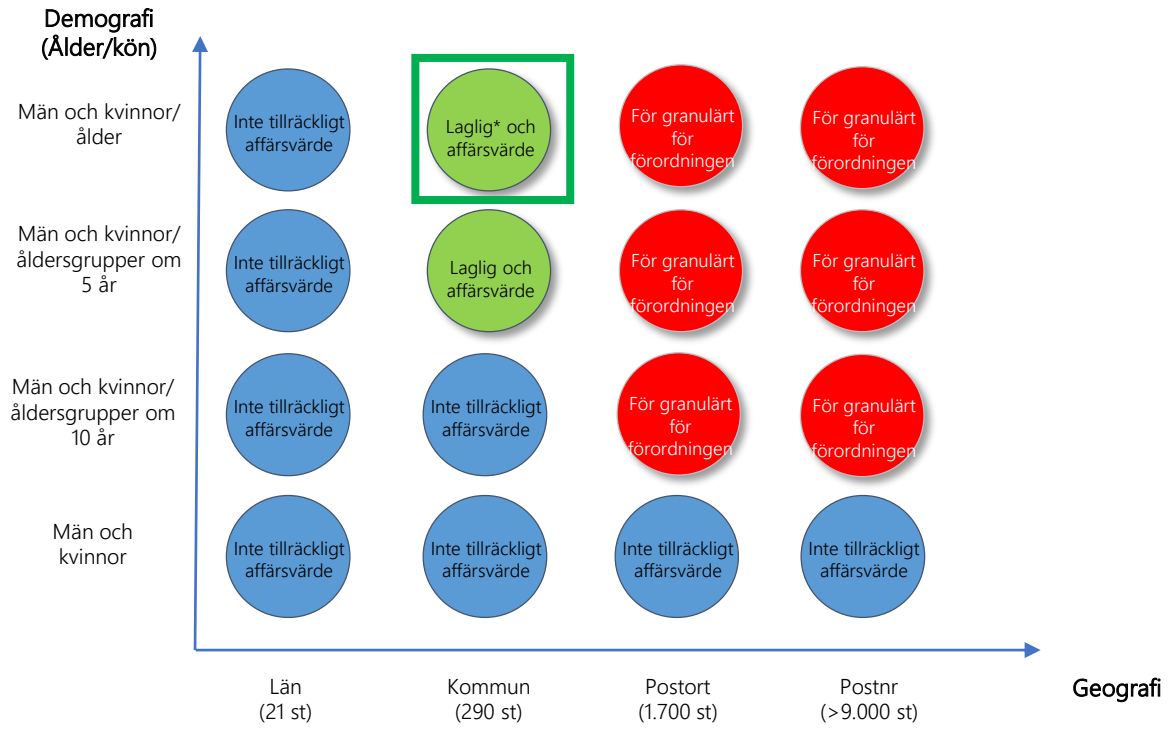
Genom att ta bort Kund-ID men lägga till t ex vissa demografiska och geografiska variabler vid sparandet av datauppgiften kan fortfarande flexibel analys utföras men individen som gjorde köpet kan inte identifieras.

Möjligt resonemang kring avidentifiering

Utgångspunkten vid avidentifiering är att en individ inte ska kunna identifieras baserat på en kombination av datauppgifter som tillsammans pekar ut individen på ett enkelt sätt som t ex genom slagning i öppna register som ratsit.se eller upplysning.se.

Ambitionen skulle därför exempelvis kunna vara att ingen kombination ska innehålla mindre än fem individer i Sverige.

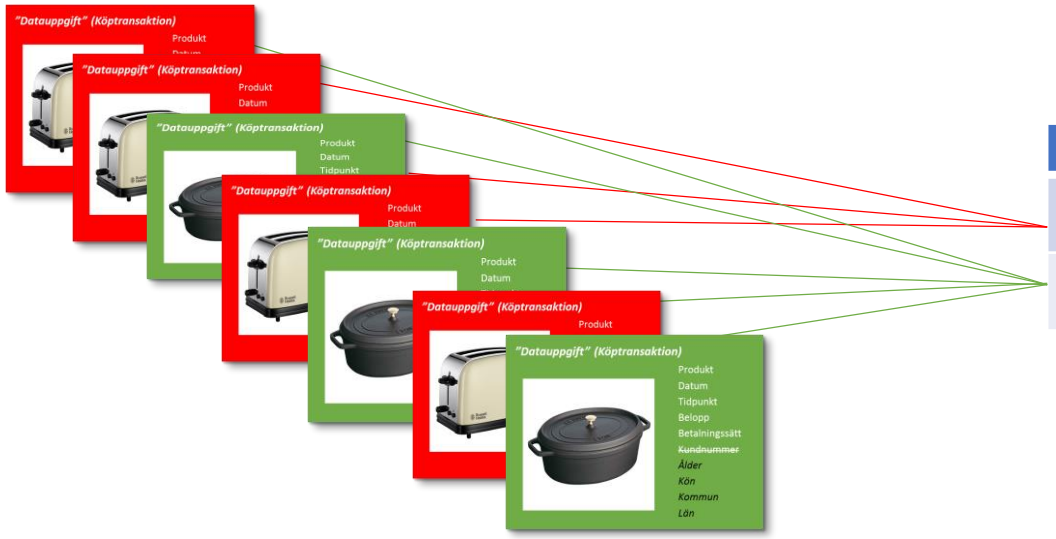
Avidentifiering ska inte blandas ihop med ”pseudonymisering”, då kopplingen finns kvar men kräver översättningssteg för att göra identifieringen.



** Med gruppering om 5 års-gruppering över 80 år*

En datauppgift som är aggregerad är inte längre en personuppgift

För uppföljning av t ex försäljning av en produkt så räknar och summerar man oftast datauppgifterna och sparar resultatet i en ny ”tabell”. På så sätt kan man slänga de underliggande datauppgifterna (personuppgifterna) utan att gå miste om viktig information. På så sätt försvinner spårbarheten till enskilda individer.



2017-02-01	Antal spel	Summa
Brödrost	4 st	950 kr
Gryta	3 st	5600 kr

Traditionell Data Warehouse-teknologi och Big Data-teknologi skiljer sig åt. Traditionell DW jobbar i större utsträckning med aggregering och skapande av nya tabeller för att följa upp förutbestämda KPI:er, medan Big Data behåller data på lägre nivå för att möjliggöra snabb och flexibel ad-hoc analys.

Vad är ”behandling” av personuppgifter?

”Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.”

Kort sagt – **Allt.**

Vad är profilering?

”Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar”

moderamen CONSULTING

Agenda

08.30 - Registrering och morgonfika

09.00 - Vad är GDPR och vad är personuppgifter?

10.00 - Paus

10.15 - Fortsättning Genomgång GDPR

11.00 - Varför behandlar företag personuppgifter?

12.00 - Lunch

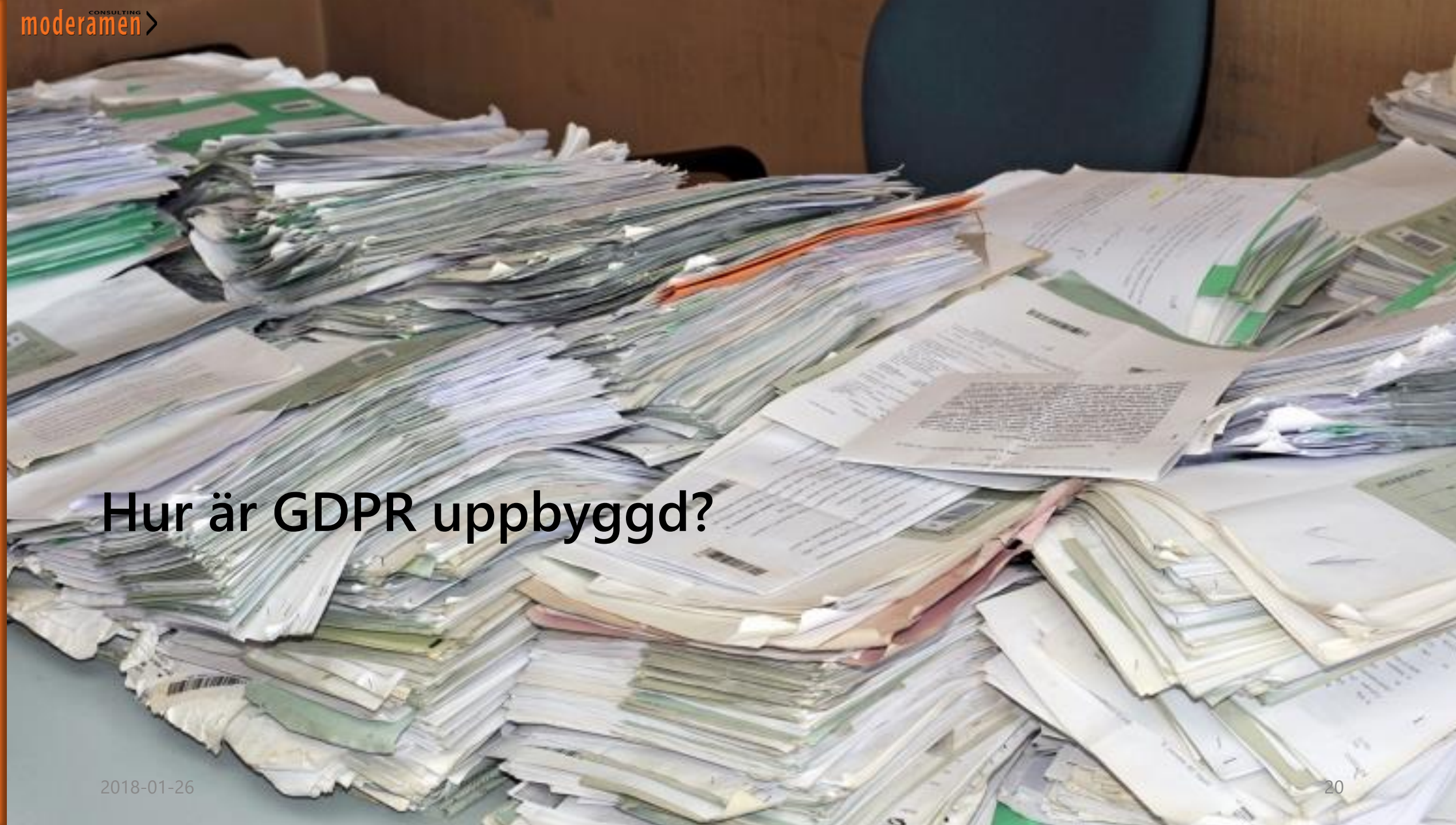
13.00 - Vad är E-Privacyförordningen (EPR) och vad säger Marknadsföringslagen?

14.00 - Case: Hur Svenska Spel förbereder sig inför GDPR

14.30 - Eftermiddagsfika

14.45 - Workshop kring era egna case

16.15 - Sammanfattning



Hur är GDPR uppbyggd?

Dataskyddsförordningen – Struktur

Själva beslutstexten
- 11 kapitel
- 99 artiklar

Bakomliggande beslutsskäl
- 173 stycken
- Ej strukturerade i kapitel

Kap 1: Allmänna bestämmelser
Kap 2: Principer
Kap 3: Den registrerades rättigheter
Kap 4: Personuppgiftsansvariges och personuppgiftsbiträdes skyldigheter
Kap 5: Överföring av personuppgifter till tredjeländer eller internationella organisationer
Kap 6: Oberoende tillsynsmyndigheter
Kap 7: Samarbete och enhetlighet
Kap 8: Rättsmedel, ansvar och sanktioner
Kap 9: Särskilda behandlingssituationer
Kap 10: Delegerade akter och genomförandeakter
Kap 11: Slutbestämmelser

Relevanta kapitel för de flesta företag

- Kap 1: Allmänna bestämmelser
- Kap 2: Principer
- Kap 3: Den registrerades rättigheter
- Kap 4: Personuppgiftsansvariges och personuppgiftsbiträdes skyldigheter
- Kap 5: Överföring av personuppgifter till tredjeländer eller internationella organisationer
- *Kap 6: Oberoende tillsynsmyndigheter*
- *Kap 7: Samarbete och enhetlighet*
- Kap 8: Rättsmedel, ansvar och sanktioner
- Kap 9: Särskilda behandlingssituationer
- *Kap 10: Delegerade akter och genomförandeakter*
- *Kap 11: Slutbestämmelser*

Kapitel 2 – Principer

- Art 5 - Dataskydds principer:
  - Syfte, Ändamålsbegränsning, Uppgiftsminimering, Korrekthet, Lagringsminimering, Konfidentialitet och Integritet
  - Ansvarsskyldighet: kunna visa att förordningen efterlevs = dokumentera, ordning och reda, Personuppgiftsansvarig har bevisbördan för att förordningen efterlevs
- Art 6 - Laglig grund:
  - Samtycke, Fullgörande av avtal, Rättslig förpliktelse, Skydda intresse, Berättigat intresse
- Art 7 - Villkor för samtycke:
  - Höga krav på tydlighet, begriplighet och separation
  - Lika lätt att ge som att återkalla samtycke, rätt att återkalla samtycke när som helst
- Art 8 - Villkor för barns samtycke
  - Målsmans godkännande under 16 år – förslag i Sverige under 13 år
- Art 9 - Behandling särskilda kategorier av personuppgifter:
  - Är i normalfallet förbjuden
  - Kräver samtycke
- Art 10 - Behandling personuppgifter avseende fällande domar brottmål samt överträdelser är i normalfallet förbjuden. Annan lag kan dock trumfa, t ex Penningtvättslagen

Den registrerades rättigheter

Kap 3 – Den registrerades rättigheter
Rätten till information

- Art 12-14 - Rätten till information:
- Information ska lämnas självmant
- Information på begäran (registerutdrag) inom en månad
- Mer omfattande information:
  - Uppdatera information till registrerade (t ex Policy för behandling av personuppgifter)
  - Kontaktuppgifter till dataskyddsombud
  - Behandlingens rättsliga grund
  - Om berättigat intresse; vilka intressen som ligger bakom behandlingen
  - Hur länge uppgifter behandlas och hur denna tid fastställs
  - Nya rättigheter, t.ex. dataportabilitet
  - Rätten att återkalla samtycke, i de fall där behandlingen grundas på samtycke
  - Rätt att klaga hos tillsynsmyndighet
  - Om den registrerades tillhandahållande av uppgifterna är lagstadgat eller avtalat krav
  - Om det förekommer automatiserat beslutsfattande, inbegripet profilering

Kap 3 – Den registrerades rättigheter
Rätten till tillgång, rättelse och radering

- Art 15 - Rätten till tillgång (Registerutdrag inom 1 månad)
  - Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat
  - Måste även ange ändamål med behandlingen, samtliga PUL-biträden, lagringstid, grund för automatiserat beslutsfattande inkl profilering (logiken bakom), etc
- Art 16 - Rätten till rättelse
  - ”Utan onödigt dröjsmål”..
- Art 17 - Rätten till radering. ”Rätten att bli glömd”
  - Samtycke dras tillbaka eller behandlingen har bedömts olaglig
  - Om uppgifterna inte längre är nödvändiga för ändamålet eller om laglig grund för fortsatt behandling saknas

Kap 3 – Den registrerades rättigheter
Rätten till begränsning, dataportabilitet och invändningar

- Art 18 - Rätten till begränsning
  - Kunden kan välja begränsning istället för radering om den vill.
  - Oftast sker detta under någon form av bestridande från kunden, t ex inkorrekta uppgifter, olaglig behandling, etc
- Art 19 – Anmälningsskyldighet till samtliga mottagare
  - Om kunden begär rättelse eller begränsning av behandling ska även samtliga PU-biträden meddelas och göra justeringar i den mån det är möjligt
- Art 20 - Rätten till dataportabilitet
  - Gäller när behandlingen grundar sig på samtycke eller på avtal, samt är automatiserad
  - Personuppgifter som rör den registrerade och som registrerade tillhandahållit
  - Strukturerat, allmänt använt och maskinläsbart format
- Art 21 - Rätt att göra invändningar
  - Alltid rätt att invända mot direktmarknadsföring, inbegripet profilering för dessa ändamål. Behandlingen ska då upphöra
  - Den registrerade ska informeras om rätten att göra invändningar vid första kontakt

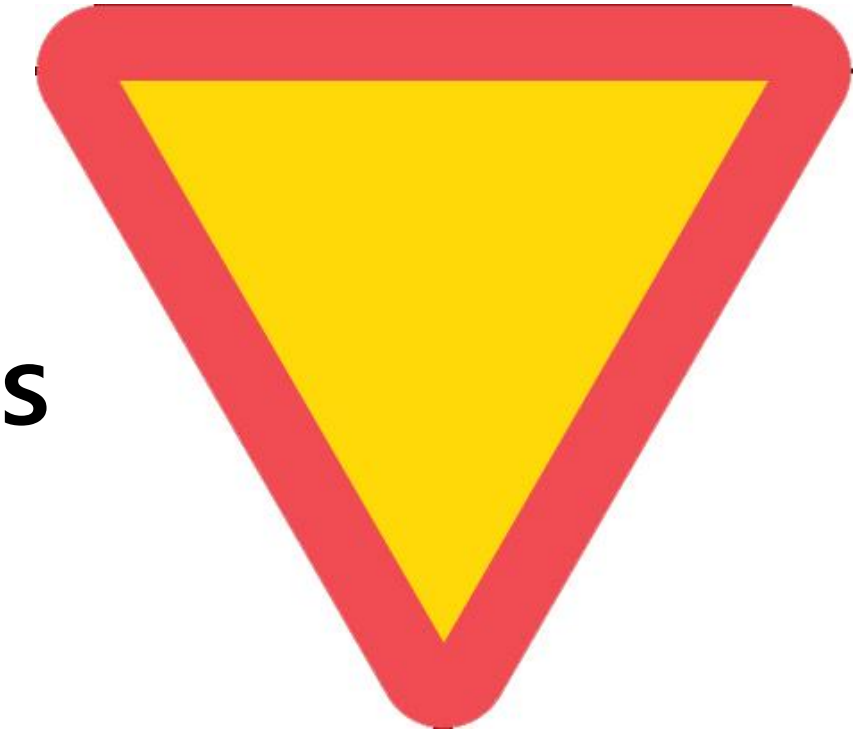
Kap 3 – Den registrerades rättigheter
Rätt att neka profilering

- Art 21-22 - Automatiserat individuellt beslutsfattande, inbegripet profilering
- Definition av profilering:

"Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar"

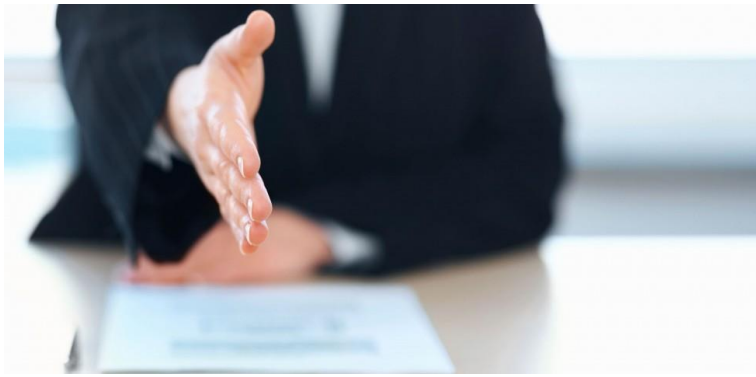
- Kund ska kunna neka profilering om detta inte baseras på:
  - Fullgörande av avtal
  - Samtycke

Personuppgiftsansvariges skyldigheter



Kap 4 - Personuppgiftsansvariges skyldigheter
- Eget ansvar samt biträdens

- Art 24 - Den personuppgiftsansvariges ansvar
  - Genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandling utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.
- Art 25 - Inbyggt dataskydd och dataskydd som standard (Privacy by design)
  - Säkerställandet av ***Principerna*** vid all form av produkt-, tjänste- och systemutveckling
- Art 28 – Personuppgiftsbiträden
  - Ett personuppgiftsbiträdesavtal ska minst innehålla
    - Skriftliga instruktioner från den ansvarige
    - Tillgänglighet och sekretess hos de som arbetar hos biträdet
    - Skyldighet för biträdet att vidta säkerhetsåtgärder
    - Hur och om underbiträden får anlitas, samt lista över vilka dessa är
    - Biträdet ska bistå den ansvarige att säkerställa de registrerades rättigheter
    - Incidentrapportering
    - Bestämmelser rörande radering vid avtalets upphörande
    - Insyn och revision



Kap 4 - Personuppgiftsansvariges skyldigheter
- Register, Dataskyddsombud och Uppförandekod

- Art 30 - Register över behandling
  - Kan även vara bra för andra syften, t ex systemförvaltning
  - Gäller både ansvariga och biträden
- Art 37-39 – Dataskyddsombud
  - Om kärnverksamheten behandlar personuppgifter i stor omfattning
  - Denne ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd
  - Kan vara en anställd eller kan köpas som tjänst från extern
- Art 40-42 Uppförandekod och certifiering
  - Branscher kan utarbeta praxis och standarder samt möjlighet till certifiering efter godkännande av tillsynsmyndigheter

Kap 4 - Personuppgiftsansvariges skyldigheter
- Samarbete med tillsynsmyndighet

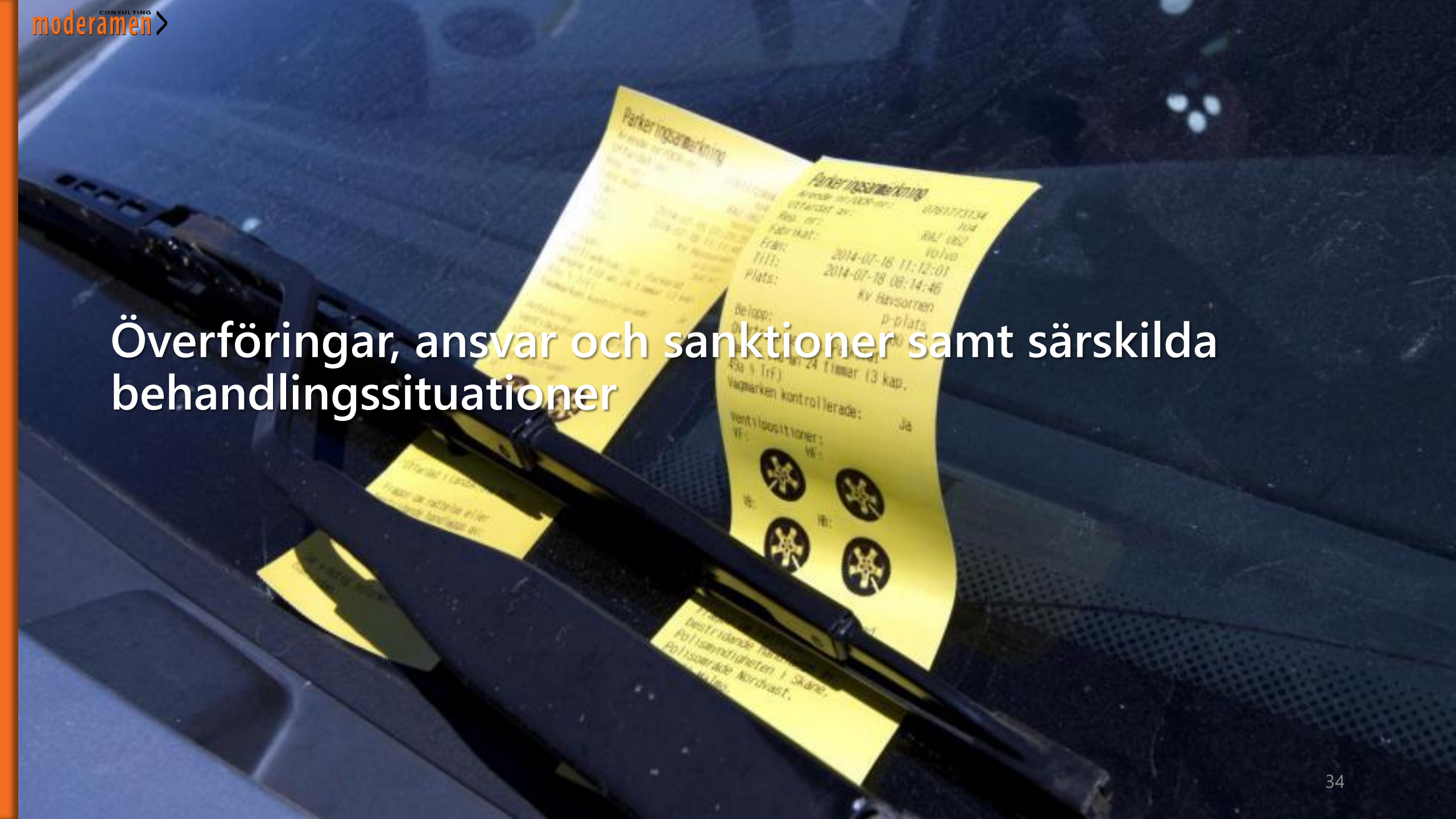
- Art 31 - Samarbete med tillsynsmyndigheten
- Art 35-36 - Konsekvensbedömning avseende dataskydd samt föregående samråd
  - Nya projekt som kan utgöra särskild risk för den registrerades fri- och rättigheter (stor mängd uppgifter, känsliga pers uppg)
  - Innan behandling påbörjas (samråda med DI)
- Art 33-34 - Anmälan/information på grund av en personuppgiftsincident
  - Om inte osannolikt att incidenten medför risker för enskildas fri- och rättigheter = anmäla till DI inom 72 h
  - Om incidenten kan leda till att personer utsätts för allvarliga risker såsom diskriminering, id-stölder, bedrägerier eller finansiella förluster måste även de registrerade informeras om händelsen så att de kan vidta nödvändiga åtgärder

Datainspektionen

Kap 4 - Personuppgiftsansvariges skyldigheter
- Säkerhet och utbildning

Art 32 - Säkerhet i samband med behandlingen

- Ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt:
  - a) pseudonymisering och kryptering av personuppgifter,
  - b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
  - c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
  - d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.
- Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför
- Anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism får användas för att visa att kraven i den här artikeln följs.
- Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige



Överföringar, ansvar och sanktioner samt särskilda behandlingssituationer

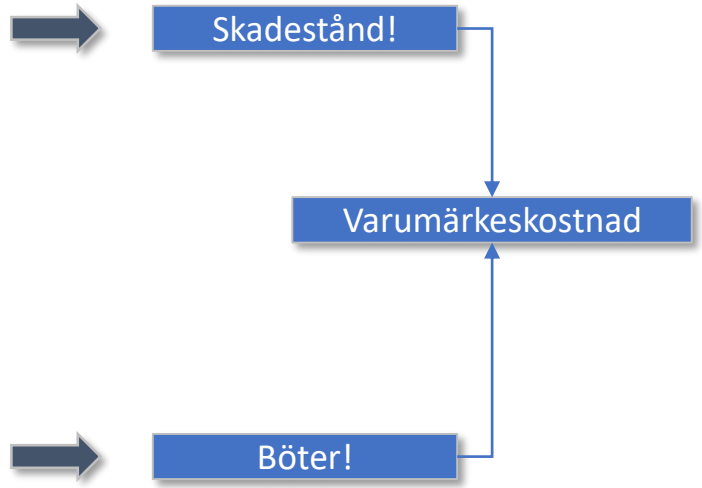
Kap 5- Överföringar till andra länder

- Art 44 - Allmän princip för överföring av uppgifter
  - Ingen idé att försöka kringgå förordningen genom att skicka ut personuppgifterna utanför EU för behandling, GDPR gäller oavsett
- Art 45 - Överföring på grundval av ett beslut om adekvat skyddsnivå
  - Tillsynsmyndigheten tillhandahåller listor med länder som är OK. Då behövs inget ytterligare tillstånd.
- Art 46 - Överföring som omfattas av lämpliga skyddsåtgärder
  - Lista med krav som måste vara uppfyllda för att överföra till tredjeländer som inte redan är OK enligt tillsynsmyndighetens lista.

Andorra
Argentina
Bailiwick of Guernsey
Färöarna
Isle of Man
Israel
Jersey
Kanada (beroende på bransch)
Nya Zeeland
Schweiz
Uruguay
(USA)

Kap 8 - Ansvar och sanktioner

- Art 79 - Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig
- Art 80 - Företrädande av registrerade
  - Den registrerade ska ha rätt att ge ett organ, en organisation eller sammanslutning utan vinstsyfte i uppdrag att lämna in ett klagomål för hans eller hennes räkning.
- Art 82 - Ansvar och rätt till ersättning
  - Varje person som har lidit skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan.
  - Om en personuppgiftsansvarig eller ett personuppgiftsbiträde har betalat full ersättning för den skada som orsakats ska den ha rätt att från de andra som medverkat vid samma behandling återkräva den del av ersättningen som motsvarar deras del av ansvaret för skadan.
- Art 84 – Sanktioner från tillsynsmyndigheter
  - Två prislappar:
    - 20 miljoner EUR eller 4 % av totala globala årsomsättningen (De grundläggande principerna för behandling, inklusive villkoren för samtycke, Registrerades rättigheter, Överföring av personuppgifter till en mottagare i ett tredjeland)
    - 10 miljoner EUR eller 2 % av totala globala årsomsättningen (Registerförteckning, Konsekvensbedömning, Dataskyddsombud, Lämpliga säkerhetskrav, Personuppgiftsincident)



Kap 9 - Särskilda behandlingssituationer

- Art 87 - Behandling av nationella identifikationsnummer
  - Dataskyddsförordningen ger medlemsstaterna möjlighet att bestämma särskilda villkor för när ett nationellt identifieringsnummer, det vill säga ett personnummer eller samordningsnummer, får behandlas.
  - Frågan om hur personnummer och samordningsnummer ska regleras i svensk rätt har hanterats av Dataskyddsutredningen som har föreslagit att sådana uppgifter ska få behandlas bara om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Förslaget motsvarar tidigare bestämmelse i personuppgiftslagen (PUL).
  - Även om personnummer inte nämns som ”särskilda kategorier” i artikel 9 så betraktar Datainspektionen dem som extra känsliga.

moderamen CONSULTING

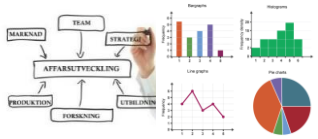
Agenda

08.30 - Registrering och morgonfika
09.00 - Vad är GDPR och vad är personuppgifter?
10.00 - Paus
10.15 - Fortsättning Genomgång GDPR
11.00 - Varför behandlar företag personuppgifter?
12.00 - Lunch
13.00 - Vad är E-Privacyförordningen (EPR) och vad säger Marknadsföringslagen?
14.00 - Case: Hur Svenska Spel förbereder sig inför GDPR
14.30 - Eftermiddagsfika
14.45 - Workshop kring era egna case
16.15 - Sammanfattning

Varför behandlar företag personuppgifter för kunder?

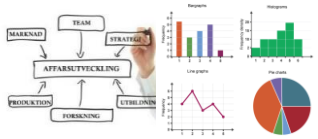
Huvudsakliga syften med att behandla personuppgifter för kunder i ett företag

Annan lagstiftning och/eller myndighetsbeslut!

Affärssyfte	Leverans av tjänst/Försäljning	Kundservice *(Ärendehantering och support)*	Marknadsföring *(CRM och digital anpassning)*	Undersökningar *(Marknadsunder-sökningar, NPS, etc)*	Analys/BI *(Uppföljning, ad-hoc analys, modellering)*	System-förvaltning *(systemtest, back-up, etc)*	Motverka brott *(mot penning-tvätt/fusk)*
							
Målsättning	Leverera det kunden beställt och få betalt	Hjälpa kunden få ut mer av befintlig tjänst	Få kunden att köpa mer (nu eller senare)	Ta reda på vad marknaden/ kunder tycker	Följa upp och utveckla affären	Säkerställa god leverans från IT-system	Motverka brott
Exempel på behandling	• Ordermottagning • Kontohantering • Leverans • Fakturering • Betalning • Vem ska ha bonuspoängen?	• Besvarande av kundförfrågningar per telefon och mail. • Personalisering av kundupplevelse med syfte att ge bättre service. • Inspelningar av kundservice-samtal • Registerutdrag	• Urval och utskick av direktmarknadsföring (CRM). • Personalisering av kundupplevelse på web, app med syfte att få kunden att köpa mer • Datadrivna digitala mediaköp (t ex adserving)	• Insamling och sammanställning av data för att förstå t ex, konsumtionsmönster, kundnöjdhet, attityder och/eller preferenser	• Hur går försäljningen? • Vilka produkter och segment går bäst? • Modellering. Vilka kundgrupper skulle gilla en ny produkt?	• Behandling av personuppgifter i testmiljöer och back-uper	• Anmälan och utredningsstöd till brottsbekämpande myndigheter. • Motverkande av fusk och bedrägerier (beroende på myndighetsbeslut)

Hur påverkas detta av GDPR?

Annan lagstiftning och/eller myndighetsbeslut!

	Leverans av tjänst/Försäljning *(Fullgörande av avtal)*	Kundservice *(Ärendehantering och support)*	Marknadsföring *(CRM och digital anpassning)*	Undersökningar *(Marknadsunder-sökningar, NPS, etc)*	Analys/BI *(Uppföljning, ad-hoc analys, modellering)*	System-förvaltning *(systemtest, back-up, etc)*	Motverka brott *(mot penning-tvätt/fusk)*
Affärssyfte							
							
Målsättning	Leverera det kunden beställt och få betalt	Hjälpa kunden få ut mer av befintlig tjänst	Få kunden att köpa mer (nu eller senare)	Ta reda på vad marknaden/ kunder tycker	Följa upp och utveckla affären	Säkerställa god leverans från IT-system	Motverka brott
Laglig grund	• Fullgörande av avtal • Berättigat intresse • Samtycke	• Fullgörande av avtal	• Samtycke (Opt-in) • Berättigat intresse; (Opt-out)	• Berättigat intresse (Opt-out)	• Berättigat intresse (om avidentifierat)	• Berättigat intresse	• Andra lagar och myndighetsbeslut
Gallring	Definitioner av tjänsterna styr gallringen av personuppgifter.	Basera huvudregel på hur gamla uppgifter som kunder brukar fråga om.	• Baserat på information i samtycke. • Huvudregel ett år efter avslutad kundrelation för kommunikation. • 2-3 år för datauppgifter/ transaktioner i pågående relation	• Baserat på information i tydligt samtycke	Avidentifiering och aggregering vid inläsning till analysmiljö.	Vid driftsättning bör personuppgifterna raderas i testmiljön samt back-uper skrivas över.	• Penningtvättslagen spara detaljerad data i minst 5 år. • Enligt myndighets-beslut i övrigt

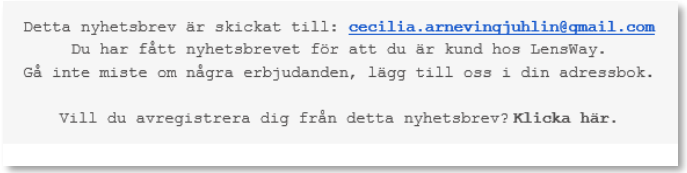
Skillnad mellan Samtycke och Berättigat intresse

Samtycke (”Opt-in”)

- Personen måste aktivt slå på knappen/kryssa i rutan
- Samtycken får inte villkoras

Berättigat intresse (”Opt-out”)

- T ex information i allmänna villkor
- Kund måste få chans att säga nej senast vid första tillfället av behandlingen (helst vid registrering)
- Förikryssade rutor är inte att rekommendera



moderamen CONSULTING

Agenda

08.30 - Registrering och morgonfika
09.00 - Vad är GDPR och vad är personuppgifter?
10.00 - Paus
10.15 - Fortsättning Genomgång GDPR
11.00 - Varför behandlar företag personuppgifter?
12.00 - Lunch
13.00 - Vad är E-Privacyförordningen (EPR) och vad säger Marknadsföringslagen?
14.00 - Case: Hur Svenska Spel förbereder sig inför GDPR
14.30 - Eftermiddagsfika
14.45 - Workshop kring era egna case
16.15 - Sammanfattning

moderamen CONSULTING

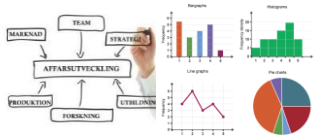
Agenda

08.30 - Registrering och morgonfika
09.00 - Vad är GDPR och vad är personuppgifter?
10.00 - Paus
10.15 - Fortsättning Genomgång GDPR
11.00 - Varför behandlar företag personuppgifter?
12.00 - Lunch
13.00 - Vad är E-Privacyförordningen (EPR) och vad säger Marknadsföringslagen?
14.00 - Case: Hur Svenska Spel förbereder sig inför GDPR
14.30 - Eftermiddagsfika
14.45 - Workshop kring era egna case
16.15 - Sammanfattning

Vad betyder detta för oss på Marknad?

Huvudsakliga syften med att behandla personuppgifter för kunder i ett företag

Annan lagstiftning och/eller myndighetsbeslut!

Affärssyfte	Leverans av tjänst/Försäljning	Kundservice *(Ärendehantering och support)*	Marknadsföring *(CRM och digital anpassning)*	Undersökningar *(Marknadsunder-sökningar, NPS, etc)*	Analys/BI *(Uppföljning, ad-hoc analys, modellering)*	System-förvaltning *(systemtest, back-up, etc)*	Motverka brott *(mot penning-tvätt/fusk)*
							
Målsättning	Leverera det kunden beställt och få betalt	Hjälpa kunden få ut mer av befintlig tjänst	Få kunden att köpa mer (nu eller senare)	Ta reda på vad marknaden/ kunder tycker	Följa upp och utveckla affären	Säkerställa god leverans från IT-system	Motverka brott
Exempel på behandling	• Ordermottagning • Kontohantering • Leverans • Fakturering • Betalning • Vem ska ha bonuspoängen?	• Besvarande av kundförfrågningar per telefon och mail. • Personalisering av kundupplevelse med syfte att ge bättre service. • Inspelningar av kundservice-samtal • Registerutdrag	• Urval och utskick av direktmarknadsföring (CRM). • Personalisering av kundupplevelse på web, app med syfte att få kunden att köpa mer • Datadrivna digitala mediaköp (t ex adserving)	• Insamling och sammanställning av data för att förstå t ex, konsumtionsmönster, kundnöjdhet, attityder och/eller preferenser	• Hur går försäljningen? • Vilka produkter och segment går bäst? • Modellering. Vilka kundgrupper skulle gilla en ny produkt?	• Behandling av personuppgifter i testmiljöer och back-uper	• Anmälan och utredningsstöd till brottsbekämpande myndigheter. • Motverkande av fusk och bedrägerier (beroende på myndighetsbeslut)

Vilka lagar och regler förutom GDPR styr hur man får jobba med datadriven marknadsföring?

Personuppgiftslagen (PUL)
Dataskyddsförordningen (GDPR)

Laglig grund:
Samtycke

Lagen om Elektronisk kommunikation (LEK)
E-Privacy förordningen (EPR)

Marknadsföring
(CRM och digital anpassning)

Få kunden att köpa mer (nu eller senare)

Marknadsföringslagen

SWEDMA

Etiska regler
Branschstandard
God sed

(Andra lagar, myndighetsbeslut eller branschregler)

PUL respektive GDPR om direktmarknadsföring

PUL

- **11 §** Personuppgifter får inte behandlas för ändamål som rör direkt marknadsföring, om den registrerade hos den personuppgiftsansvarige skriftligen har anmält att han eller hon motsätter sig sådan behandling.

GDPR

Artikel 21 - Rätt att göra invändningar

2. Om personuppgifterna behandlas för direkt marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

3. Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

Marknadsföringslagen om direktmarknadsföring

Obeställd reklam

- 19 § En näringsidkare får vid marknadsföring till en fysisk person använda elektronisk post, telefax eller sådana uppringningsautomater eller andra liknande automatiska system för individuell kommunikation som inte betjänas av någon enskild, bara om den fysiska personen har samtyckt till det på förhand.
- Har näringsidkaren fått den fysiska personens uppgifter om elektronisk adress för elektronisk post i samband med försäljning av en produkt till personen, gäller inte kravet på samtycke enligt första stycket om,
    1. den fysiska personen inte motsatt sig att uppgiften om elektronisk adress används i marknadsföringssyfte med användande av elektronisk post,
    2. marknadsföringen avser näringsidkarens egna, likartade produkter och
    3. den fysiska personen klart och tydligt ges möjlighet att kostnadsfritt och enkelt motsätta sig att uppgiften används i marknadsföringssyfte när den samlas in och vid varje följande marknadsföringsmeddelande.
- 20 § Vid marknadsföring med elektronisk post ska meddelandet alltid innehålla en giltig adress till vilken mottagaren kan sända en begäran om att marknadsföringen ska upphöra. Detta gäller även vid marknadsföring till en juridisk person.

Etiska regler för marknadsföring via e-post (B2B och B2C)

1. Relevant budskap för mottagaren
2. Avanmälan (Opt-Out)
3. Adresskälla
4. Adressinsamling
   - Syfte med insamling
   - Säkerhet och integritet
   - Matchning eget kundregister mot köpta/hyrda adresser
   - Hyr/köp – säkerställa samtycke och källa
5. Registervård
6. Tydliga avtal mellan parter
7. Överföring av register till andra länder

Vad innebär detta för prospekts?

Brev

- Man får skicka fysiska brev med reklam till privatpersoner genom att köpa adressen från SPAR eller om personen visat aktivt intresse för företagets produkter och tjänster.
- Numera kan man dock spärra sig för adresserad reklam i **SPAR** och **Nix Adresserat**.
- Baseras på Berättigat intresse

Telemarketing

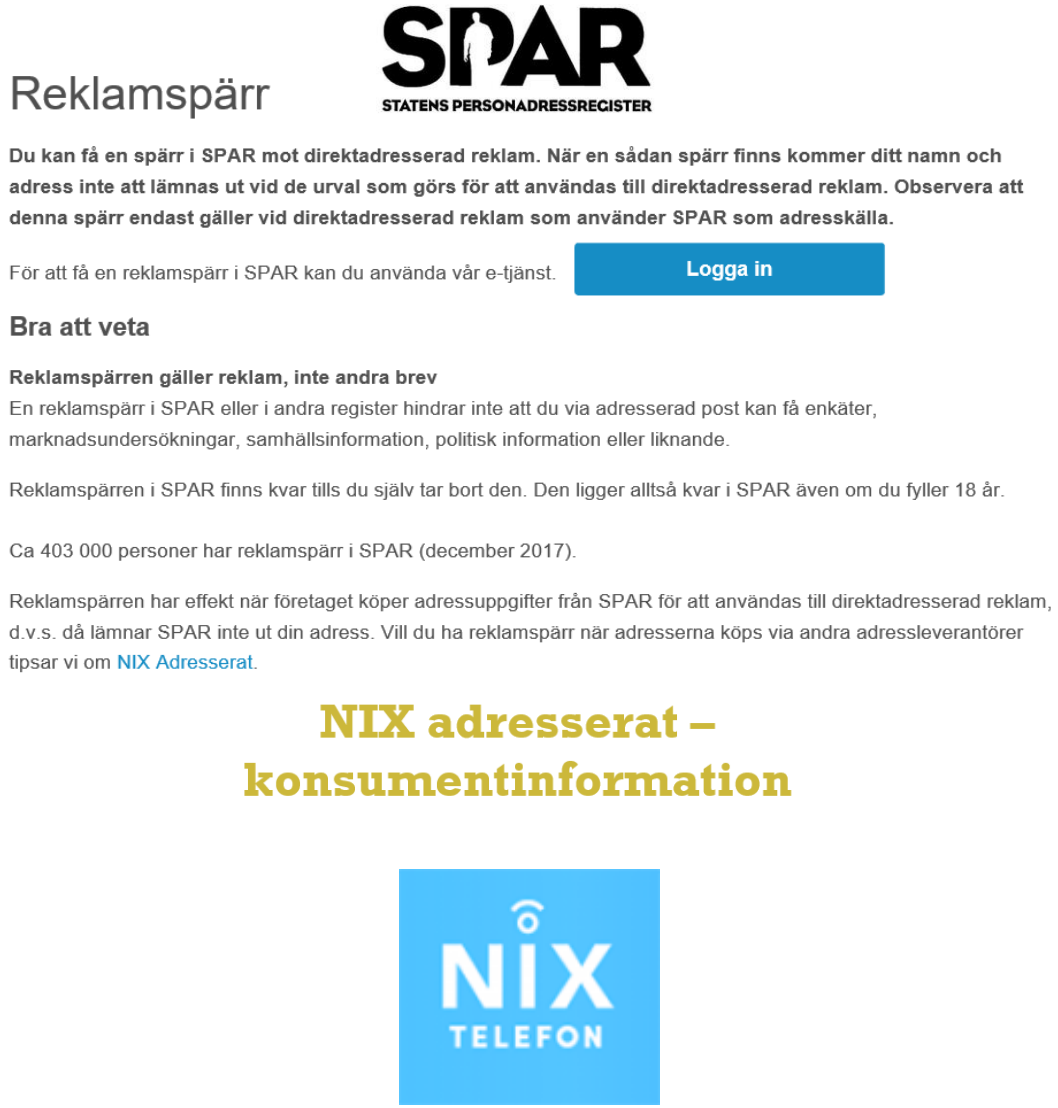
- Man får ringa upp privatpersoner för telemarketing om de inte har spärrat sig i **Nix telefon**
- Baseras på berättigat intresse

E-post

- Man får inte kontakta prospekts med reklam via e-post såvida man inte har först inhämtat samtycke
- Baseras således på samtycke (kan dock vara via förmedlare)

SMS/Textmeddelande

- Betraktas som aggressiv kanal och kräver därmed samtycke



NIX adresserat – konsumentinformation

NIX TELEFON

Vad innebär detta för befintliga kunder?

Brev

- Man får skicka fysiska brev med reklam om egna produkter/tjänster till befintliga kunder om man har informerat om detta i samband med försäljning eller registrering och de inte har avregistrerat sig från utskick tidigare.
- Baseras på Berättigat intresse

Telemarketing

- Man får ringa upp befintliga kunder för telemarketing om egna produkter/tjänster om man informerat om det i samband med försäljning samt att kunden har möjlighet att avsäga sig detta i fortsättningen.
- Baseras på berättigat intresse

E-post

- Man får skicka reklam via e-post till befintliga kunder om egna produkter/tjänster om man informerat om det på samma sätt som ovan samt vid varje tillfälle ger möjlighet för kunden att avregistrera sig (samt enbart om egna produkter/tjänster, etc)
- Baseras på berättigat intresse

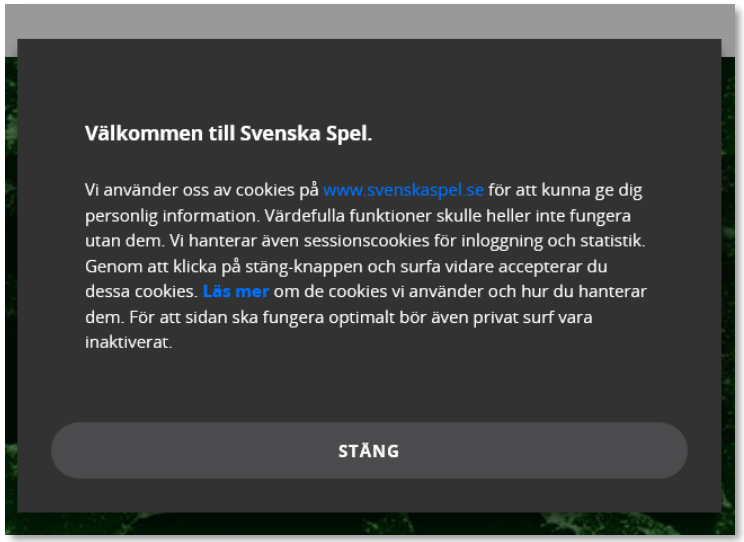
SMS/Textmeddelande

- Man får skicka reklam via e-post till befintliga kunder om egna produkter/tjänster om man informerat om det på samma sätt som ovan samt vid varje tillfälle ger möjlighet för kunden att avregistrera sig (samt enbart om egna produkter/tjänster, etc)
- Baseras på berättigat intresse

Legal information eller annan information som inte kan klassas som reklam får man alltid skicka till befintliga kunder!

Lagen om elektronisk kommunikation (LEK)

- Baseras huvudsakligen på EU E-privacy direktiv från 2002
- Reglerar användningen av elektronisk kommunikation och samtliga telekom- och kabeloperatörer
- I lagen omfattas begreppet elektronisk kommunikation av alla typer av elektroniska kommunikationsnät som telenätet, internet och kabel-TV-nätet.
- Reglerar användningen av cookies
  - Individer måste samtycka till cookies
  - Detta ska göras i enlighet med §3 PUL (individuellt, frivilligt och särskilt)
  - ”Samtycke innebär något förenklat ett medvetet godkännande. PTS har inga regler för exakt hur den tekniska utformningen ska se ut eller fungera för att möjliggöra detta.”
  - Praxis är dock passivt samtycke
- Post och Telestyrelsen är tillsynsmyndighet



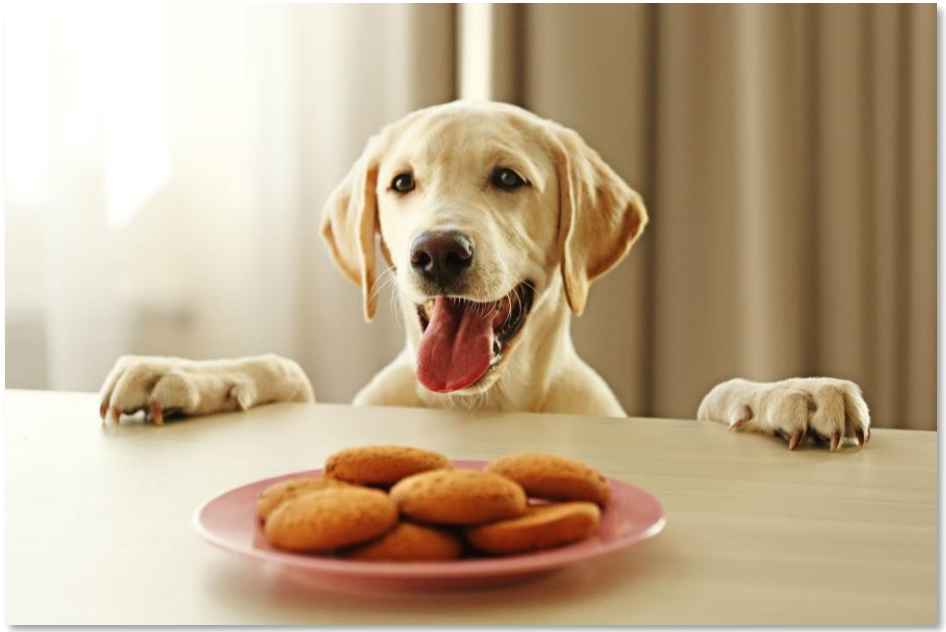
E-privacy förordningen (nya ”Cookie-lagen”)

- Kommer att ersätta LEK (Lagen om elektronisk kommunikation). Dock ej helt klart när detta kommer att ske…
- Applicerbar främst på telekombolag men nu även företag som tillhandahåller kommunikationstjänster (t ex FB Messenger, Gmail, etc)
- Reglerar fortsatt användningen av cookies
  - ”Session” cookies – inget samtycke
  - Förstahandscookies för analys av egen web – inget samtycke
  - Förstahandscookies för personalisering egen web (Samtycke)
  - Tredjepartcookies för marknadsföring (Samtycke)
- Skydd mot skräppost utan samtycke (Finns redan i Sverige)
- Tydligare reglering av telemarketing – Speciella avsändarnummerserier
- En tillsynsmyndighet för alla integritetsfrågor (idag PTS för LEK och Datainspektionen för PUL)

Vad gäller till dess att E-privacyförordningen börjar gälla?

- Måste informera om användningen av cookies och för vilka syften.
- Vid användning av cookiebaserad reklam ska symbolen här bredvid användas på hemsidan enligt Reklamombudsmannen

Villkorade cookiesamtycken för flera syften kan komma att tolkas som olagliga redan under GDPR



Intressebaserad reklam på internet

Intressebaserad marknadsföring på internet, OBA (Online Behavioral Advertising), är reklam baserad på insamling av uppgifter om användares surfande på olika webbplatser från en viss dator. Reklamen baseras på cookies som sätts i din webbläsare från sajter som du surfar på.

Det ska tydligt framgå om du får se reklam på grund av ditt tidigare surfande på nätet. Denna symbol ska visas på sådan reklam:

Om du inte vill se sådan intressebaserad reklam kan du besöka **www.youronlinechoices.com/se/** för att klicka i vilka annonsnätverk du inte vill ta emot reklam ifrån. Denna information sparas som en cookie, så om du rensar dina cookies måste du göra valen på nytt.

Inte all reklam på nätet visas på grund av ditt tidigare surfande, och sådan reklam kommer du se ändå även om du tackar nej till intressebaserad reklam.

http://www.youronlinechoices.com/se/dina-val

moderamen CONSULTING

Agenda

08.30 - Registrering och morgonfika
09.00 - Vad är GDPR och vad är personuppgifter?
10.00 - Paus
10.15 - Fortsättning Genomgång GDPR
11.00 - Varför behandlar företag personuppgifter?
12.00 - Lunch
13.00 - Vad är E-Privacyförordningen (EPR) och vad säger Marknadsföringslagen?
14.00 - Case: Hur Svenska Spel förbereder sig inför GDPR
14.30 - Eftermiddagsfika
14.45 - Workshop kring era egna case
16.15 - Sammanfattning

moderamen CONSULTING

SVENSKA SPEL

Hur Svenska spel förbereder sig för GDPR

Margareta Almbring,
Chef Konto och tjänster

moderamen CONSULTING

Agenda

08.30 - Registrering och morgonfika
09.00 - Vad är GDPR och vad är personuppgifter?
10.00 - Paus
10.15 - Fortsättning Genomgång GDPR
11.00 - Varför behandlar företag personuppgifter?
12.00 - Lunch
13.00 - Vad är E-Privacyförordningen (EPR) och vad säger Marknadsföringslagen?
14.00 - Case: Hur Svenska Spel förbereder sig inför GDPR
14.30 - Eftermiddagsfika
14.45 - Workshop kring era egna case
16.15 - Sammanfattning

moderamen CONSULTING

Agenda

08.30 - Registrering och morgonfika
09.00 - Vad är GDPR och vad är personuppgifter?
10.00 - Paus
10.15 - Fortsättning Genomgång GDPR
11.00 - Varför behandlar företag personuppgifter?
12.00 - Lunch
13.00 - Vad är E-Privacyförordningen (EPR) och vad säger Marknadsföringslagen?
14.00 - Case: Hur Svenska Spel förbereder sig inför GDPR
14.30 - Eftermiddagsfika
14.45 - Workshop kring era egna case
16.15 - Sammanfattning

moderamen CONSULTING

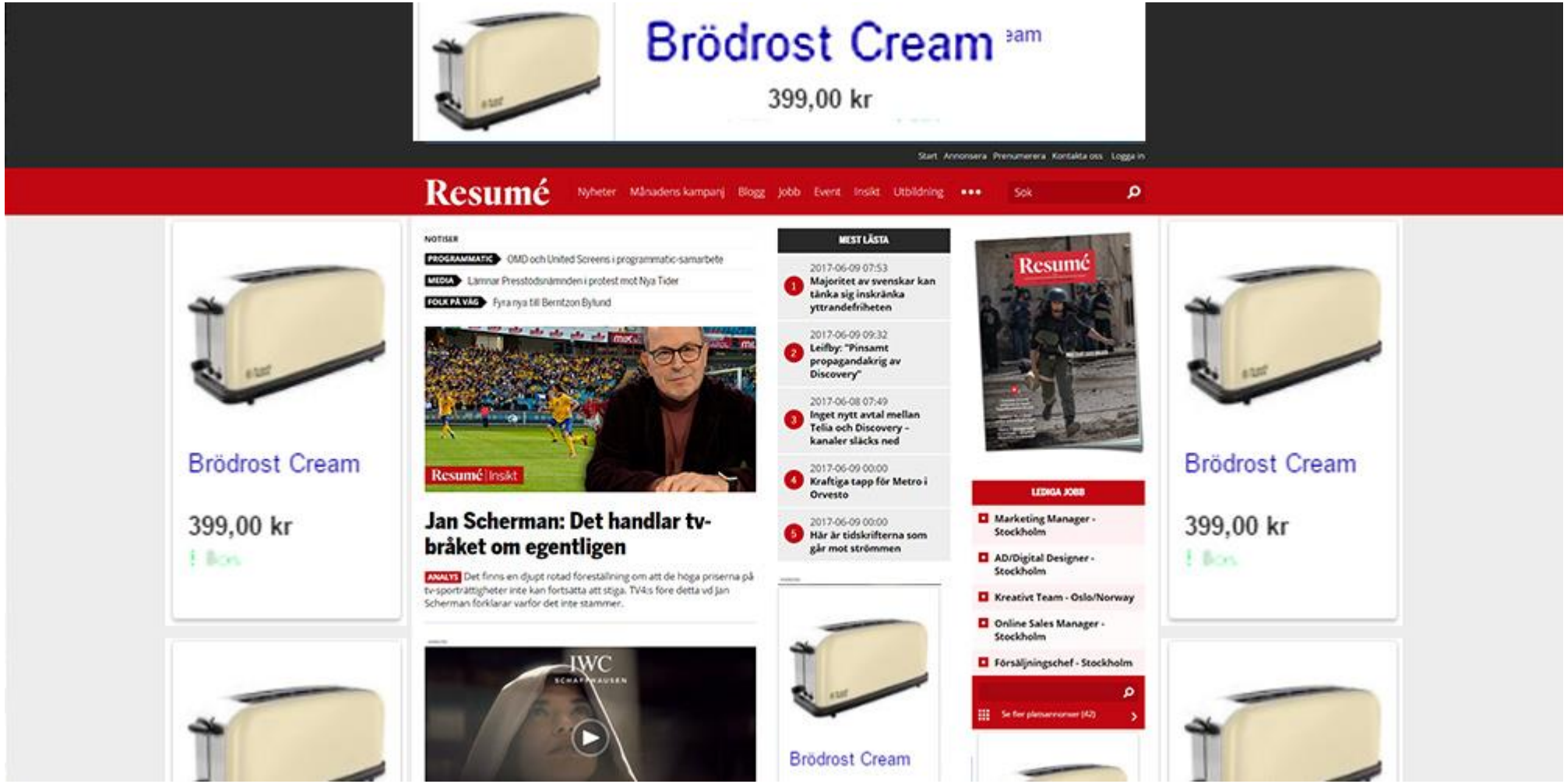
Diskussion era case

moderamen CONSULTING

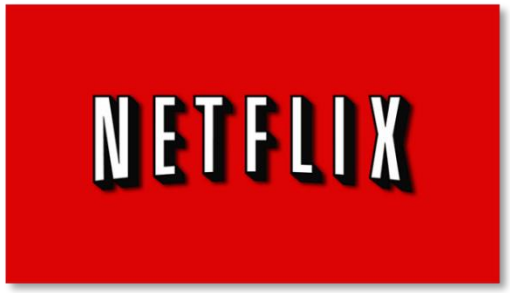
Avslutningsvis

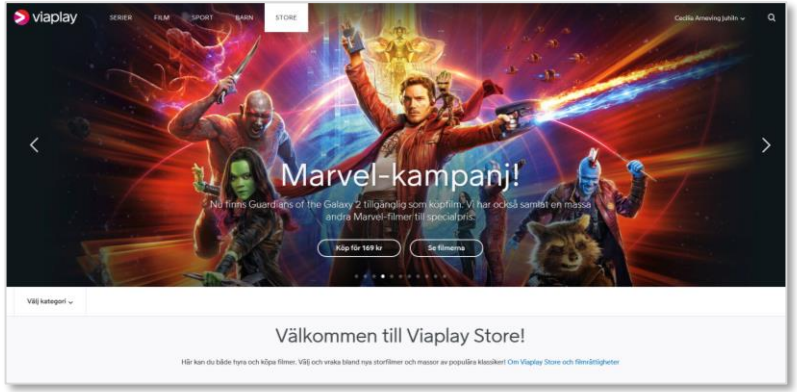
moderamen CONSULTING

Vi måste gå ifrån det här...



…till att tänka så här!





Vad är den generella kundupplevelsen som vi vill leverera till kunder som inte vill dela med sig av sitt data?

Vad är den **delvis** personaliserade kundupplevelsen som vi vill leverera till kunder som vill dela med sig av sitt data med vissa begränsningar?

Vad är den **helt** personaliserade kundupplevelsen som vi vill leverera till kunder som vill dela med sig av sitt data för alla syften?

moderamen CONSULTING

Tack för er uppmärksamhet och lycka till!