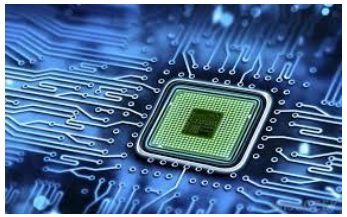

!NSATT

DATASKYDDSFÖRORDNINGEN

GDPR – GENERAL DATA PROTECTION REGULATION



Börjar tillämpas 25 maj 2018

!NSATT

DATASKYDDSFÖRORDNINGEN

GDPR – GENERAL DATA PROTECTION REGULATION

20 mEUR

4%
AV GLOBAL ÅRSOMSÄTTNING

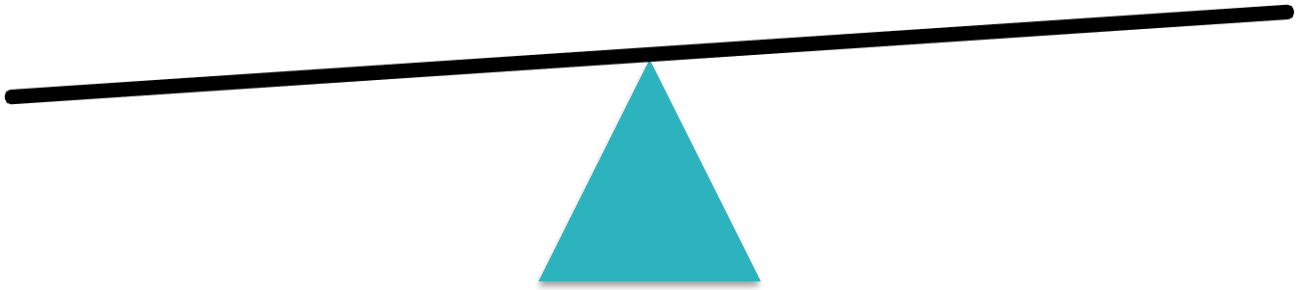
- Gäller även personuppgiftsbiträden
- Skadestånd från registrerad

!NSATT

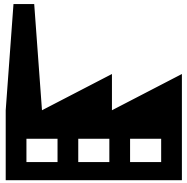

Personnummer
Namn
PERSONUPPGIFTER
Lokalisering
Foto
Ort + antal barn
IP-adress

!INSATT

TEKNISKA OCH ORGANISATORISKA SKYDDSÅTGÄRDER



!INSATT



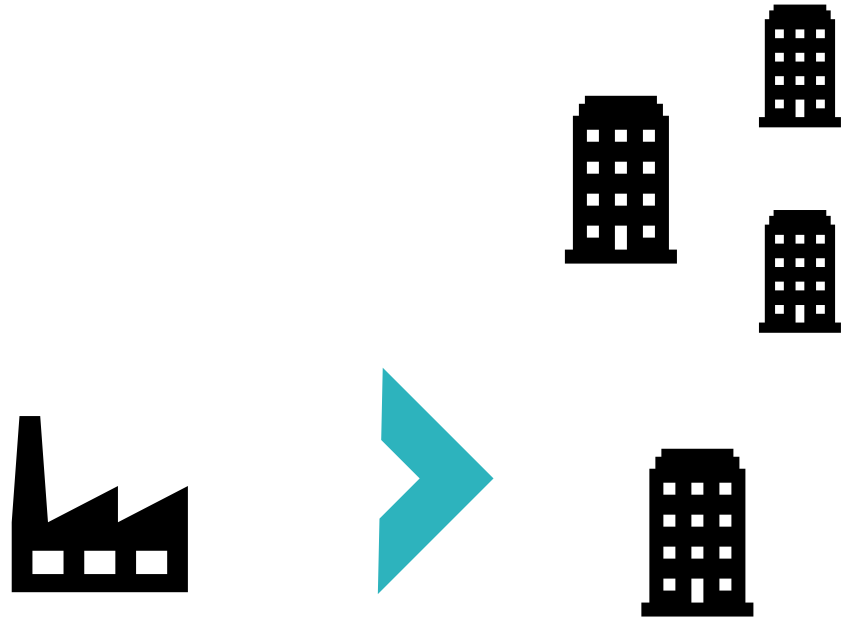
PERSONUPPGIFTSANSVARIG

Personuppgiftsansvarig

- Juridisk person
- Bestämmer ändamål och medel för behandlingen
- Kan vara gemensamt

”Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.” Art 24

!INSATT



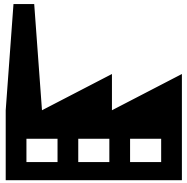
PERSONUPPGIFTSANSVARIG

PERSONUPPGIFTSBITRÄDE

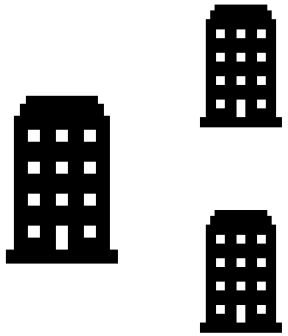
UNDERBITRÄDE

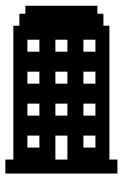
DATASKYDDSOMBUD

Myndigheter
Övervakning
Känsliga uppgifter



PERSONUPPGIFTSANSVARIG





PERSONUPPGIFTSBITRÄDE

UNDERBITRÄDE

Principer för behandling av personuppgifter

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
  - Uppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål
  - Uppgifterna får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål
- Uppgiftsminimering
  - Uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet
- Korrekthet
  - Alla uppgifter ska vara korrekta, i annat fall ska de raderas eller rättas
- Lagringsminimering
  - Uppgifter får inte sparas längre än nödvändigt
- Integritet och konfidentialitet
  - Krav på säkerhet vid behandling inklusive skydd mot obehörig behandling och förlust

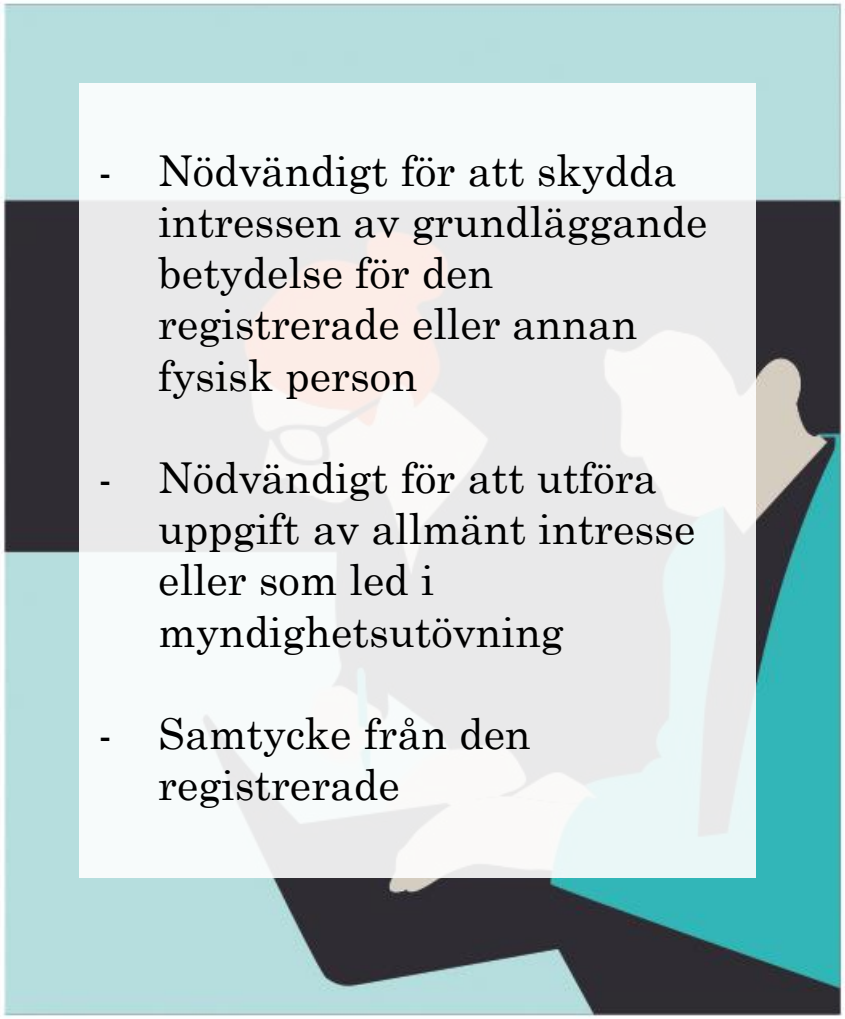
!INSATT

När är behandling tillåten?

Minst ett av följande villkor måste vara uppfyllt

- Nödvändigt för att kunna fullfölja ett avtal med den registrerade
- Nödvändigt för att fullgöra en rättslig förpliktelse
- Intresseavvägning

- Nödvändigt för att skydda intressen av grundläggande betydelse för den registrerade eller annan fysisk person
- Nödvändigt för att utföra uppgift av allmänt intresse eller som led i myndighetsutövning
- Samtycke från den registrerade



Känsliga personuppgifter

Huvudregel : förbjudna uppgifter

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska och biometriska uppgifter
- Hälsa
- Sexualliv/sexuell läggning

- Fällande domar i brottmål

Undantag

- Uttryckligt och specifikt samtycke
- Arbetsrätt/socialt skydd
- Fysiskt/rättsligt förhindrad
- Verksamhet med politiskt/filosofiskt/religiöst/fackligt syfte
- Tydligt offentliggjorts av den registrerade
- Rättsliga anspråk
- Viktigt allmänt intresse (lagstöd)
- Hälso- och sjukvård/Social omsorg (lagstöd)
- Folkhälsan (lagstöd)
- Arkivändamål /forskning (lagstöd)

!INSATT

Samtycke

”Frivilligt, specifikt, informerat och otvetydigt medgivande”

Skriftlig eller muntlig

Personuppgiftsansvarig ska kunna visa att samtycke finns

Särskiljas från övriga frågor

Klart och tydligt språk

Lika lätt att återkalla

Tillgång

Begränsad behandling

Dataportabilitet

Rättelse

De registrerades rättigheter

Invända mot automatiserat beslutsfattande

Radering

Information

Invända mot viss typ av behandling, inkl profilering

!NSATT

IT-säkerhet

”Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.” Art 32

…inbegripet, när det är lämpligt

- Pseudonymisering och kryptering
- Förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft
- Förmåga att återställa tillgängligheten i rimlig tid
- Ett förfarande för att regelbundet testa effektiviteten av åtgärderna

!NSATT

Personuppgiftsincident

= säkerhetsincident som leder till förstöring, förlust, obehörigt röjande eller obehörig åtkomst

- Anmäls till Datainspektionen inom 72 timmar om det inte är osannolikt att det medför en risk för fysiska personers rättigheter och friheter
- Om sannolikt hög risk ska den registrerade informeras
- Alla incidenter ska dokumenteras
- Personuppgiftsbiträde ska genast underrätta den personuppgiftsansvarige

Rutiner för hur incidenter hanteras.
Hur meddelas de registrerade

!INSATT

Inbyggt dataskydd

Inbyggt dataskydd
Privacy by design
Säkerhet och integritet ska vara med redan vid planering och utveckling

- Behörigheter
- Undvika fritextfält
- Uppgiftsminimering
- Logg
- Anonymisering när det går
- Hög säkerhet
- Funktioner för autentisering
- Möjligt att kryptera
- Möjligt att gallra
- Automatisk radering
- Möjligt att hantera de registrerades rättigheter

Kan komma tydligare riktlinjer från Kommissionen

!INSATT

Dataskydd som standard

Dataskydd som standard

Privacy by default

Systemet ska styra mot det som är minst integritetskränkande
Bara nödvändiga uppgifter ska användas

- Aktivt val att dela uppgifter
- Grundinställningar så att inte mer info än nödvändigt samlas in eller visas
- Arbetsflöde som styr rätt

!INSATT

Vad behöver göras?

Register över behandlingen, art 30

- Är behandlingen laglig? Vad grundas den på?

Personuppgiftsansvarig
Ändamål
Beskrivning av registrerade
Kategorin av personuppgifter
Vem uppgifter lämnas ut till
Överföring till tredje land
Tidsfrister för radering
Tekniska och organisatoriska säkerhetsåtgärder

Personuppgiftsbiträde
Vilka man agerar biträde för
De kategorier av behandling som har utförts
Överföring till tredje land
Tekniska och organisatoriska skyddsåtgärder

Vilket rättsligt stöd används?
Används missbruksregeln?
Vilken information lämnas?
Hur inhämtas och dokumenteras samtycke?

!INSATT


!NSATT