GDPR
–
Dataskyddsförordningen

torsdagen den 29 mars 2018

Sædén Advisory

Innehåll

- Inledning
- Integritetskontroll?
- Centrala begrepp
- Grundläggande krav
- Laglig grund
- Den registrerades rättigheter
- Känsliga personuppgifter
- Säkerhetsåtgärder
- Nödvändiga dokument
- Integritetskontroll!
- Sanktioner och skadestånd
- Kort om anpassningsprojekt

General data protection regulation - Dataskyddsförordningen

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679

av den 27 april 2016

om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

- Träder i kraft den 25 maj 2018
- Gäller som lag i Sverige
- Ersätter Dataskyddsdirektivet och därmed Personuppgiftslagen (1998:204)
- Syfte att skydda fysiska personer grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter
- 99 artiklar och 173 beaktandesatser som tolkningsstöd

Integritetskontroll?

- Är GDPR tillämplig?
- Är behandlingen förenlig med de grundläggande principerna?
- Finns laglig grund (för vanliga personuppgifter/särskilda kategorier)?
- Iakttas den registrerades rättigheter?
- Har den registrerade informerats?
- Finns ”lämpliga säkerhetsåtgärder” på plats?
- Personuppgiftsbiträden?
- Har instruktioner lämnats till personuppgiftsbiträdet?
- Vid överföring till tredje land – finns laglig grund för överföringen?
- Anmälan, förteckning och/eller dataskyddsombud?

Centrala begrepp

» ”Personuppgift”

personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad *en registrerad*), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

Centrala begrepp

» ”Behandling”

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,

Centrala begrepp

» ”Register”

register: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

Centrala begrepp

» ”Personuppgiftsansvarig”

personuppgiftsansvarig: 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,

Centrala begrepp

» ”Personuppgiftsbiträde”

personuppgiftsbiträde: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

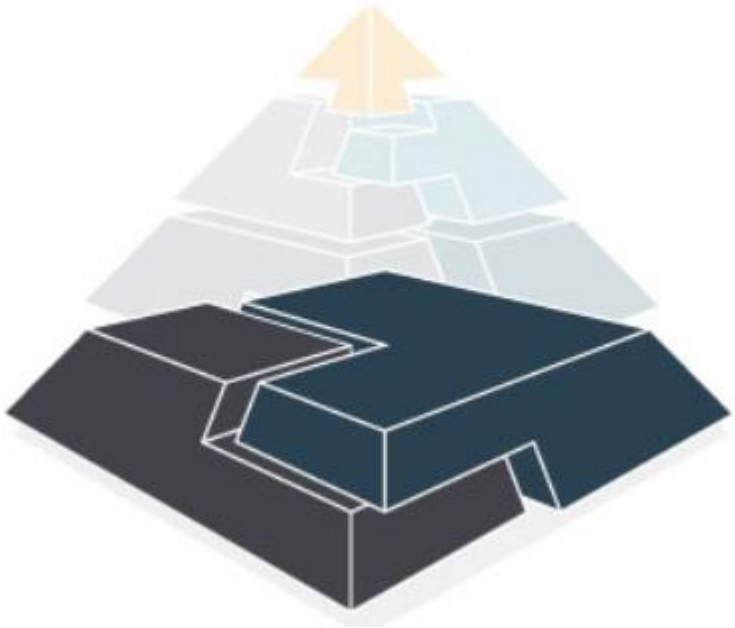
Centrala begrepp

» ”Samtycke”

samtycke av den registrerade: 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,

Grundläggande krav

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekthet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet



… ska genomsyra all personuppgiftsbehandling!

Laglig grund för behandling

Utgångspunkt: personuppgifter får inte behandlas!

Om inte…

- Samtycke
- Fullgörande av avtal
- Fullgörande av rättslig förpliktelse
- Skydda enskilds grundläggande intressen
- Utföra uppgift av allmänt intresse
- Intresseavvägning

Laglig grund för behandling

- Samtycke
  - Stora krav på hur det är utformat
  - Vad händer om det återkallas?
  - Styrkeförhållandet - beroendet
  - Måste vara välinformerat

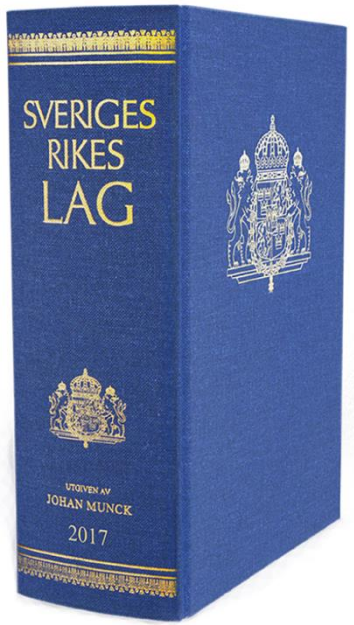
Laglig grund för behandling

- Fullgörande av avtal
  - Ofta den lämpligaste grunden
  - Den registrerade har störst förståelse för den anledningen
  - En början och ett slut

Laglig grund för behandling

» Fullgörande av rättslig förpliktelse, t ex

- bokföringslagen,
- kollektivavtal,
- penningtvättslagen,
- patientdatalagen,
- förelägganden från domstol och
- skattelagstiftning.



Laglig grund för behandling

- Intresseavvägning/berättigat intresse
  - Den personuppgiftsansvariges intresse ska väga tyngre än den registrerades rättigheter och friheter.
  - Svår bedömning, ledning får sökas i Datainspektionens praxis.
  - Några exempel: marknadsföring, publicering på intranät, säkerhet.
  - Om den enskilde motsätter sig behandling väger det tungt till dennes fördel.

Registrerades rättigheter

- Rätt till information, art 13-14
- Rätt till registerutdrag, art 15
- Rätt till rättelse, art 16
- Rätt att bli bortglömd, art 17
- Rätt till begränsning av behandling, art 18
- Rätt till dataportabilitet, art 20
- Rätt att göra invändningar, art 21

Känsliga uppgifter

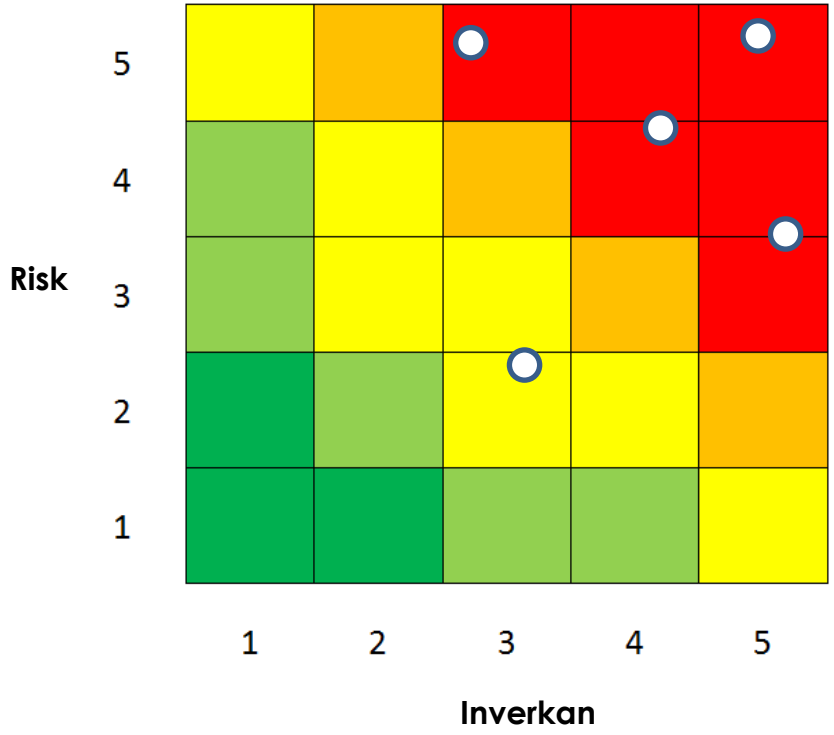
1. Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter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

- Huvudregel: Förbjudet, men med en mängd undantag.
- Ställer alltid högre krav.
- Endast i undantagsfall och då endast med stöd av samtycke eller nödvändigt för att…
- Utöver de "vanliga känsliga" – uppgift om brott, personnummer, "integritetskänsliga uppgifter"

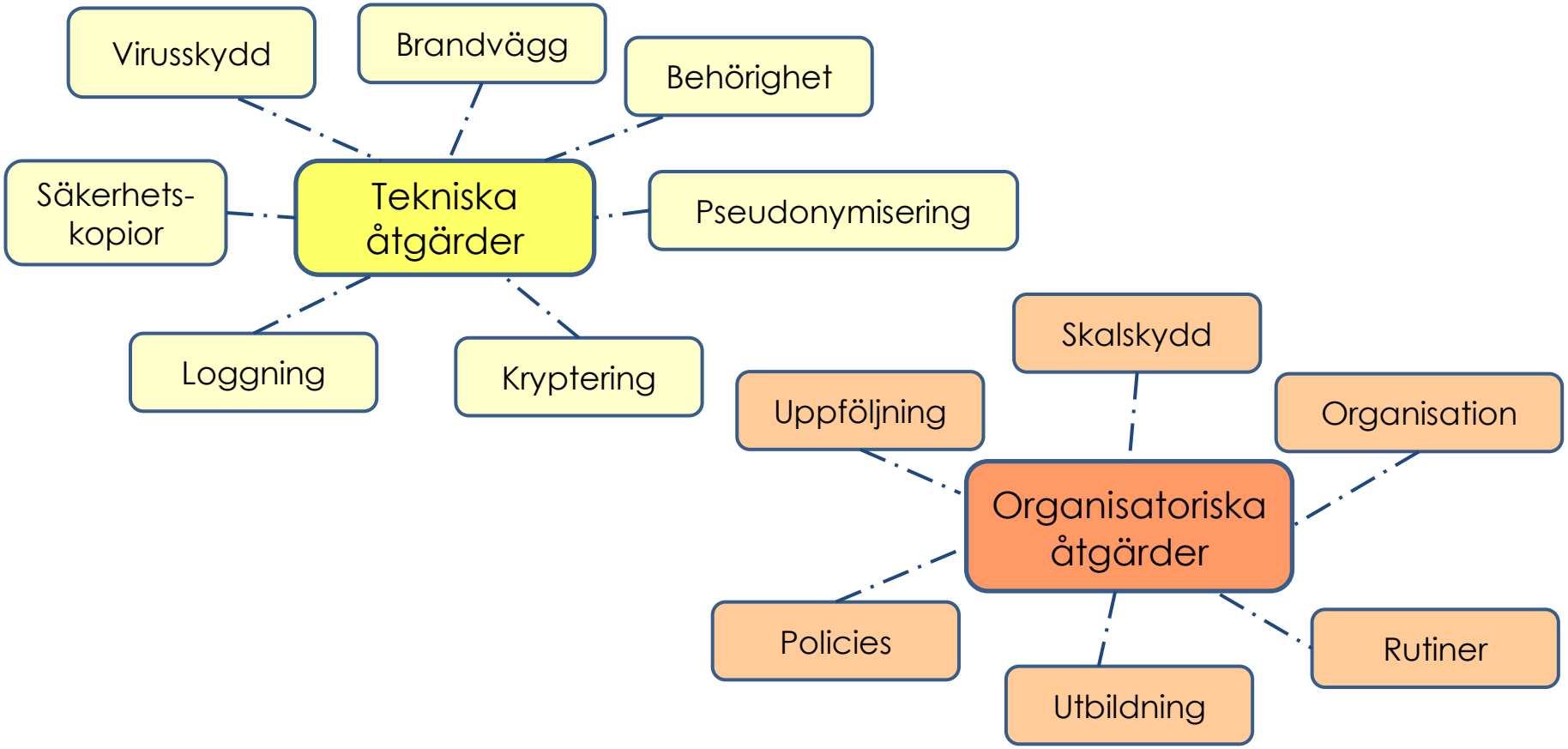
Vanliga uppgifter | **Personnummer** | **Integritetskänsliga uppgifter** | **Uppgifter om brott** | **Skyddade uppgifter** | **Känsliga uppgifter**

Tekniska och organisatoriska säkerhetsåtgärder

- Risk- och konsekvensbedömning
- Riskbedömning bör alltid göras
- Värdera risk/inverkan
- Bestäm säkerhetsåtgärder
- Om hög risk – formell konsekvensbedömning ska göras



Tekniska och organisatoriska säkerhetsåtgärder



Nödvändiga dokument

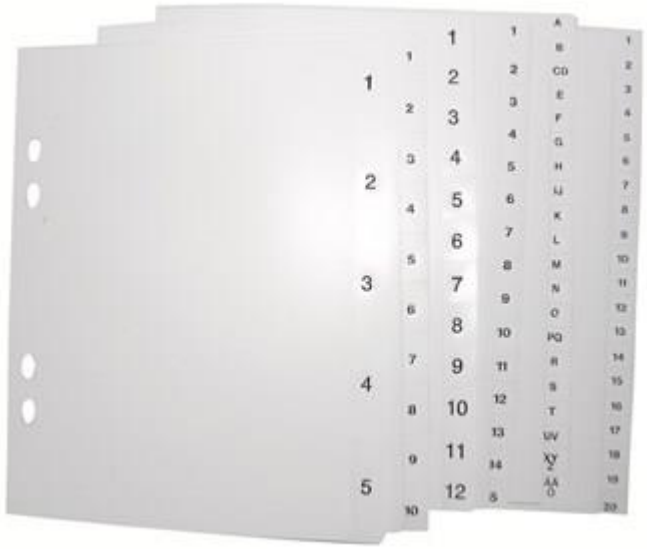
- Information till den registrerade
  - Initial, vid insamlandet
  - Mall för registerutdrag
- Registerförteckning
- Personuppgiftsbiträdesavtal inklusive instruktion
- Policies/Styrdokument

Obligatorisk information till den registrerade

- **Vem** som är personuppgiftsansvarig,
- **Varifrån** uppgifterna hämtats,
- Kontaktuppgifter till eventuellt **dataskyddsombud**,
- **Ändamål** med och **rättslig grund** för behandlingen,
- Vilka eventuella **berättigade intressen** baseras behandlingen på,
- Eventuella **mottagare** av uppgifterna,
- **Hur länge** uppgifterna kommer att sparas,
- Rätt att begära **tillgång, rättelse, begränsning** och **radering**,
- Rätt att **återkalla samtycke**,
- Rätt att **klaga** hos tillsynsmyndigheten,
- Huruvida lämnandet av uppgifterna är **nödvändigt** för lag eller avtal,
- Förekomst av **automatiserat beslutsfattande** och **profilering.**

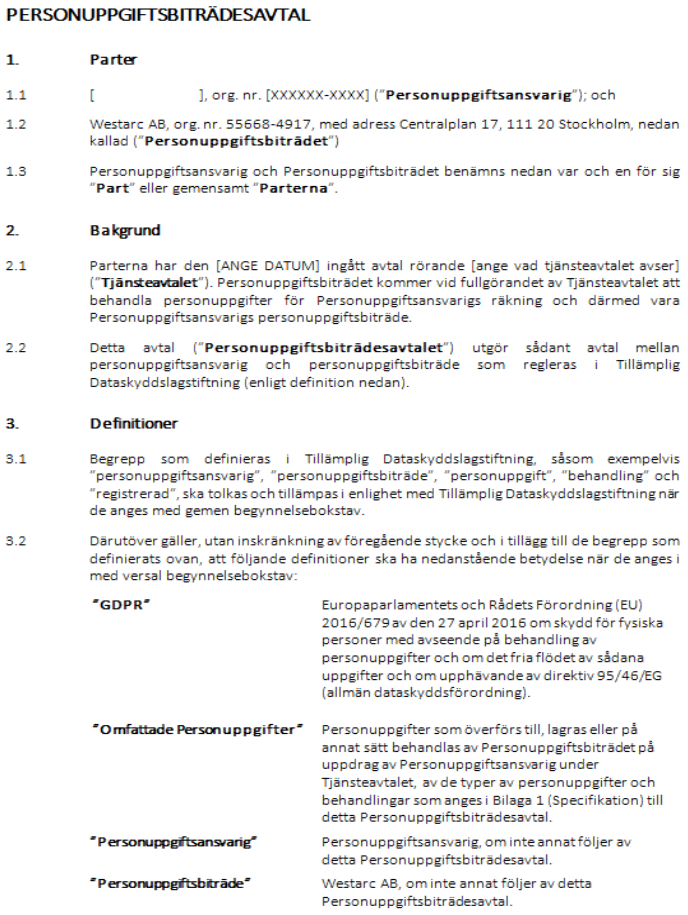
Registerförteckning

- Varje personuppgiftsansvarig ska föra ett register över behandling som utförs under dess ansvar.
- Förteckningen ska innehålla alla uppgifter om vad, var, varför, vart, hur länge, säkerhet m.m.
- Sannolikt ett av de första sakerna Datainspektionen ber om.



Personuppgiftsbiträdesavtal (”DPA”)

- Ska alltid ingås mellan personuppgiftsansvarig och personuppgiftsbiträde
- Lagkrav på innehåll – kan ofta standardiseras
- Instruktioner!
- Löpande dialog



PERSONUPPGIFTSBITRÄDESAVTAL

1. Parter

1.1 [ ], org. nr. [XXXXXX-XXXX] (”**Personuppgiftsansvarig**”); och

1.2 Westarc AB, org. nr. 55668-4917, med adress Centralplan 17, 111 20 Stockholm, nedan kallad (”**Personuppgiftsbiträdet**”)

1.3 Personuppgiftsansvarig och Personuppgiftsbiträdet benämns nedan var och en för sig ”**Part**” eller gemensamt ”**Parterna**”.

2. Bakgrund

2.1 Parterna har den [ANGE DATUM] ingått avtal rörande [ange vad tjänsteavtalet avser] (”**Tjänsteavtalet**”). Personuppgiftsbiträdet kommer vid fullgörandet av Tjänsteavtalet att behandla personuppgifter för Personuppgiftsansvarigs räkning och därmed vara Personuppgiftsansvarigs personuppgiftsbiträde.

2.2 Detta avtal (”**Personuppgiftsbiträdesavtalet**”) utgör sådant avtal mellan personuppgiftsansvarig och personuppgiftsbiträde som regleras i Tillämplig Dataskyddslagstiftning (enligt definition nedan).

3. Definitioner

3.1 Begrepp som definieras i Tillämplig Dataskyddslagstiftning, såsom exempelvis ”personuppgiftsansvarig”, ”personuppgiftsbiträde”, ”personuppgift”, ”behandling” och ”registrerad”, ska tolkas och tillämpas i enlighet med Tillämplig Dataskyddslagstiftning när de anges med gemen begynnelsebokstav.

3.2 Därutöver gäller, utan inskränkning av föregående stycke och i tillägg till de begrepp som definierats ovan, att följande definitioner ska ha nedanstående betydelse när de anges i med versal begynnelsebokstav:

”GDPR”	Europaparlamentets och Rådets Förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
”Omfattade Personuppgifter”	Personuppgifter som överförs till, lagras eller på annat sätt behandlas av Personuppgiftsbiträdet på uppdrag av Personuppgiftsansvarig under Tjänsteavtalet, av de typer av personuppgifter och behandlingar som anges i Bilaga 1 (Specifikation) till detta Personuppgiftsbiträdesavtal.
”Personuppgiftsansvarig”	Personuppgiftsansvarig, om inte annat följer av detta Personuppgiftsbiträdesavtal.
”Personuppgiftsbiträde”	Westarc AB, om inte annat följer av detta Personuppgiftsbiträdesavtal.

Personuppgiftsincident

- ”En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”.
- Anmälan till Datainspektionen ska ske inom 72 h,
  - ”såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.”
- Information till berörda registrerade vid hög risk för för fysiska personer rättigheter och friheter.
- Personuppgiftsbiträdet ska utan onödigt dröjsmål informera personuppgiftsansvarige efter att ha fått vetskap om incidenten.
- Alla incidenter ska dokumenteras.

Integritetskontroll

- Är GDPR tillämplig?
- Är behandlingen förenlig med de grundläggande principerna?
- Finns laglig grund (för vanliga personuppgifter/särskilda kategorier)?
- Iakttas den registrerades rättigheter?
- Har den registrerade informerats?
- Finns ”lämpliga säkerhetsåtgärder” på plats?
- Personuppgiftsbiträden?
- Har instruktioner lämnats till personuppgiftsbiträdet?
- Anmälan, förteckning och/eller dataskyddsombud?

Sanktioner

» ”Upp till 20 miljoner euro eller 4 % av koncernens globala årsomsättning”, beroende på:

- Svårigheten och omfattningen av överträdelsen: typ av personuppgifter
- Uppsåt eller oaktsamhet
- Vad har man vidtagit för åtgärder
- Tidigare överträdelser och påpekanden från tillsynsmyndigheten
- Samarbete med tillsynsmyndigheten
- Uppförandekoder och certifieringar
- Vinning för bolaget

Skadestånd och rätt att klaga

Artikel 82

Ansvar och rätt till ersättning

1. Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan.

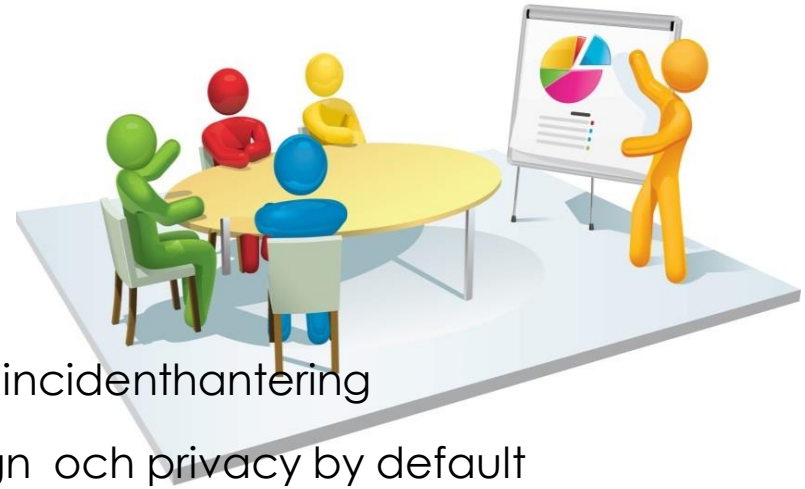
- Den registrerade har rätt att klaga hos Datainspektionen
- Den registrerade kan stämma den personuppgiftsansvarige vid domstol och begära skadestånd.

Ansvar och kontroll

- Personuppgiftsansvarige – ytterst ansvarigt
- Personuppgiftsbiträde – ansvarigt för sin behandling och sitt underbiträde
- Gemensamt ansvar – ofta svår gränsdragning
- Skyldighet att visa att lagen följs
- DPO – Datainspektionens förlängda arm
- Skyldighet att samarbeta med tillsynsmyndigheten (DI)

Kort om anpassningsprojekt

- Vilka personuppgifter behandlar vi? Varför?
- Inventering: identifiera ansvar – ansvarig/biträde. Hur flödar personuppgifter?
- Besluta om prioriteringar
- Nödvändiga avtal
- Nödvändig information
- Dokumentation av behandling
- Nödvändiga processer – registerutdrag, incidenthantering
- Metod och utbildning – privacy by design och privacy by default
- Dataskyddsombud?
- Tredjeland?
- Tekniska och organisatoriska säkerhetsåtgärder



Johan Sædén

johan@saedenadvisory.se
0733-699 656

Sædén Advisory