



GDPR ur verksamhetsperspektiv



Vem är Johan Lindström?

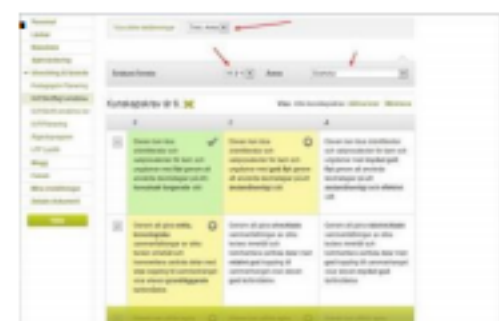


@Aland72



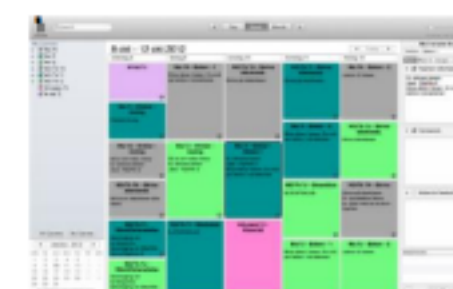
Skolans digitalisering

Inloggning omdömen,
utvecklingsplaner



Information lagras
och flödar mellan
systemen

Inloggning schema



Inloggning digitala prov

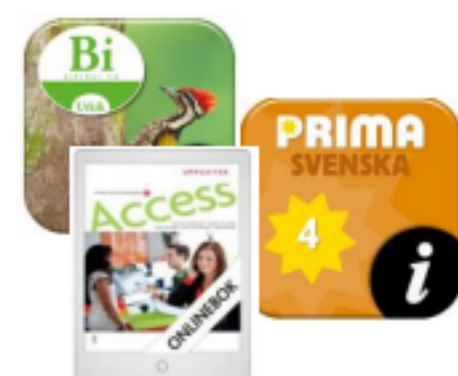


Digitalisering av NP



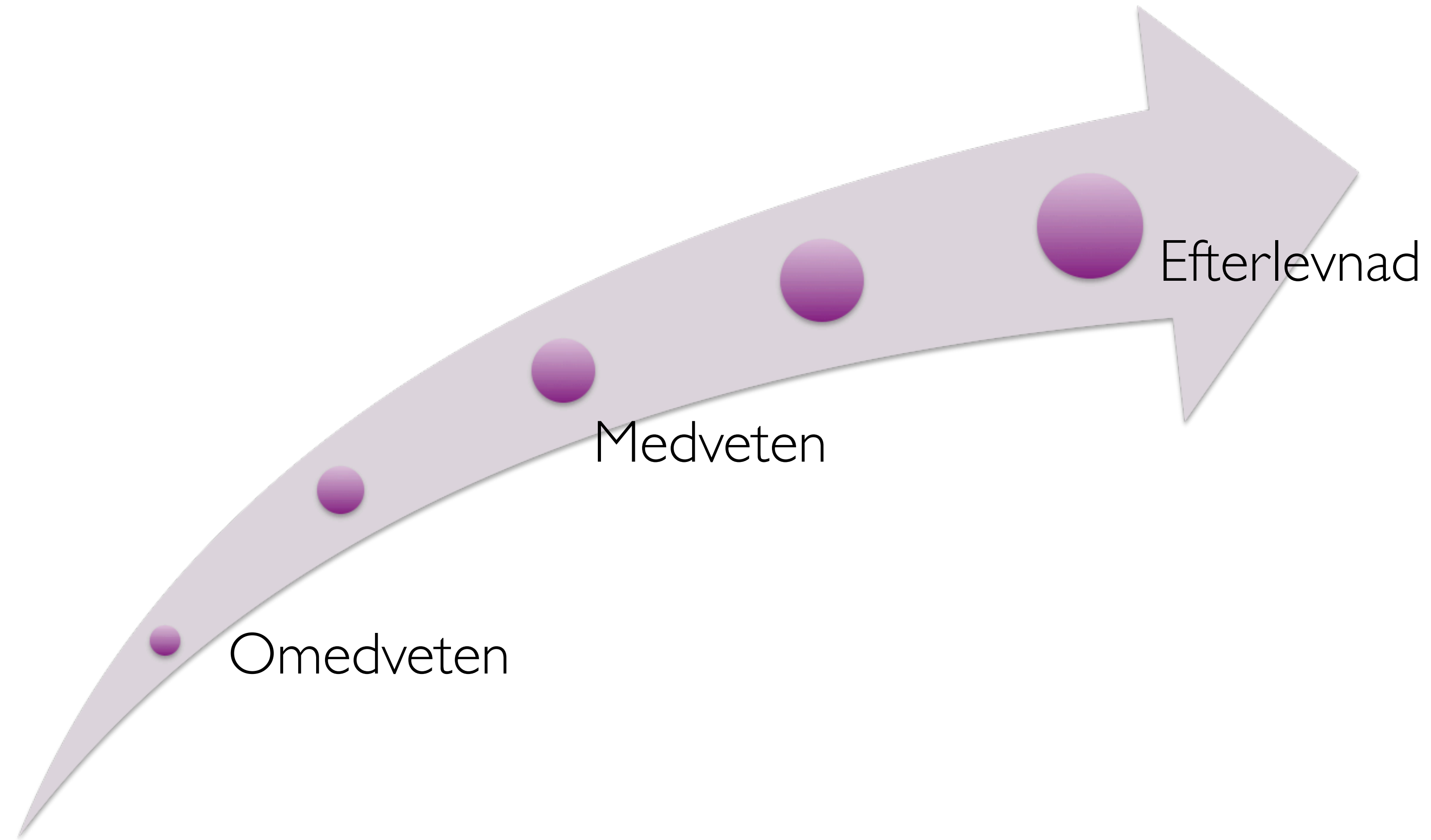
Inloggning
samarbetsytor,
uppgifter, läxor

Inloggning digitala läromedel



Åtkomst till appar.
Inloggning till enhet, nätverk.

GDPR - en utmaning eller möjlighet?





1

Dokumentera det som ska dokumenteras

2

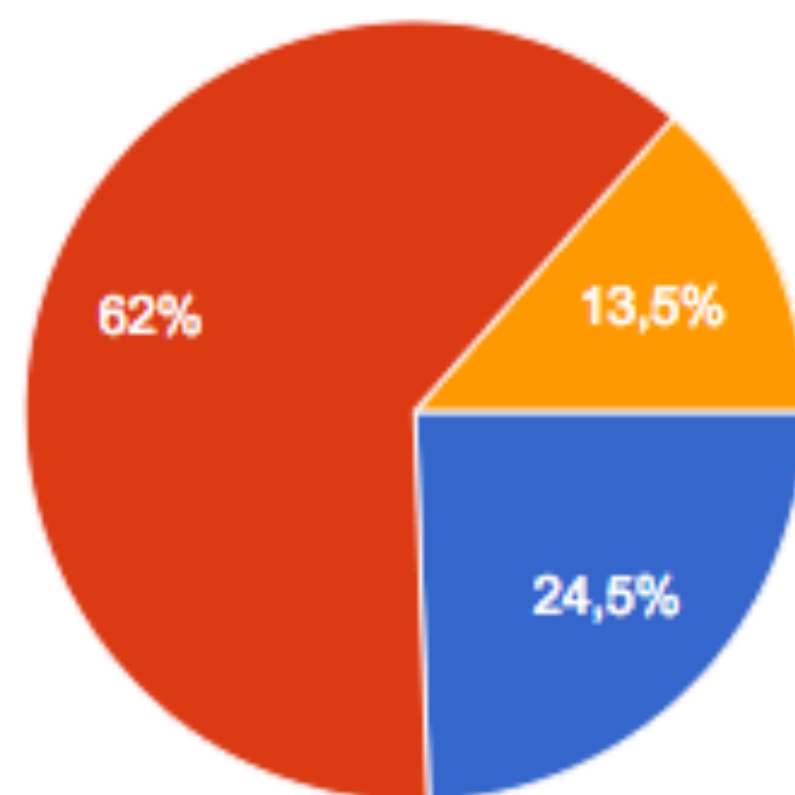
Säkerställa att all personal dagligen lever upp till GDPR



Kartläggning 274 personer som jobbar i skola i en kommun

Känner du till vad skolkopieringsavtalet är?

274 svar



- Ja, jag har full koll på vad skolkopieringsavtalet är
- Jag har hört om det, men är osäker på vad det innebär
- Nej, skolkopierings-vad???



Vad skulle du/dina kollegor svara om du/de fick följande frågor?

Kopieringsavtal; vad gäller vid kopiering av

- analoga verk
- digitala verk

Känner du till vad Creative Commons (CC) är?

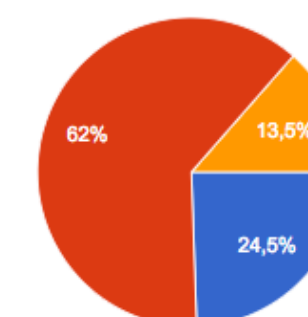
Vet du hur man hittar bilder med en viss CC-licens?

Vet du vad som gäller (digitala molntjänster) för att leva upp till GDPR?



Känner du till vad skolkopieringsavtalet är?

274 svar



- Ja, jag har full koll på vad skolkopieringsavtalet är
- Jag har hört om det, men är osäker på vad det innebär
- Nej, skolkopierings-vad???



1995 - Personuppgiftslag (i Sverige)





Användarvillkoren så omfattande att "ingen" läser dem

Spotify Användningsvillkor

Gäller från och med 27 oktober 2016

- 1 Inledning
- 2 Ändringar av Avtalen
- 3 Användning av Spotify
- 4 Rättigheter vi ger dig
- 5 Tredjepartsapplikationer
- 6 Användargenererat innehåll
- 7 Rättigheter du ger oss
- 8 Användarriktlinjer
- 9 Intrång och anmälan av Användarinnehåll
- 10 Begränsningar i och ändringar av Tjänsten
- 11 Märkeskonton
- 12 Spotifys Support Community
- 13 Kundtjänst
- 14 Exportkontroll
- 15 Betalningar, uppsägning och ångerrätt
- 16 Avtalstid och uppsägning
- 17 Garanti och friskrivning
- 18 Begränsningar
- 19 Tredje parts rättigheter
- 20 Fullständigt avtal
- 21 Ogiltighet och avstående från rättigheter
- 22 Överlåtelse
- 23 Försäkran att hålla skadeslös
- 24 Val av lag, obligatoriskt skiljeförfarande och forum
- 25 Kontakta oss

Hej och välkommen till våra Användningsvillkor. Det här är viktigt och påverkar dina juridiska rättigheter.

USER LICENSE AGREEMENT

Last version: 17.08.2017

ATTENTION! BY DOWNLOADING, COPYING, INSTALLING THE GAME CLIENT SOFTWARE AND/OR OTHERWISE USING DRACONIUS GO: CATCH A DRAGON!, YOU CONFIRM THAT YOU HAVE READ, UNDERSTOOD AND AGREED TO BE BOUND BY THE FOLLOWING TERMS AND CONDITIONS AS WELL AS ANY OTHER DOCUMENTS ASSOCIATED WITH THIS USER AGREEMENT, WITHOUT ANY RESTRICTIONS, AND THAT YOU OBLIGE TO ABIDE BY THIS USER AGREEMENT AND BEAR RESPONSIBILITY FOR VIOLATING IT.

Please read the Draconius GO: Catch a Dragon! Game End User License Agreement (hereinafter – the "User Agreement", "Agreement") attentively, since it regulates Your (hereinafter – the "User") usage of the game Draconius GO: Catch a Dragon! (hereinafter – the "Game") and all of its Resources. The End User License Agreement terms and conditions, and all links that it may contain, are important and shall be subject to compulsory execution. If You do not agree to be bound by the following terms and conditions, You are forbidden from downloading and playing the Game.

In order to play the Game and save Your progress in the Game, You may be asked to register an account (hereinafter – the "Account"). By entering the Game and registering an Account or otherwise using the Game, You confirm that You are 13 years old or older. and agree to be bound by the terms

Accept

Decline

USER LICENSE AGREEMENT

that regulate the procedure and terms for concluding public agreements and adhesion contracts. The User shall not violate the local laws of his/her country of residence. The User is solely responsible for any non-compliance with these norms.

14.5. Within a period of two weeks of accepting the terms of the Agreement, the User can terminate it in writing (e.g. fax, email) without giving any reason.

Notice of termination of the Agreement should be sent to: support@draconiusgo.com or using the form on the Game's Website.

When requesting termination of the agreement, the User's name and Account name should be written in the subject line.

14.6. To ensure the correct functioning of the Game, it is important that any errors or problems that the User discovers are confidentially reported to the technical support team directly so that they may be resolved as quickly as possible. The User can report errors in the Game by contacting Us at support@draconiusgo.com or through a form on the Game's Website.

15. Licenses used

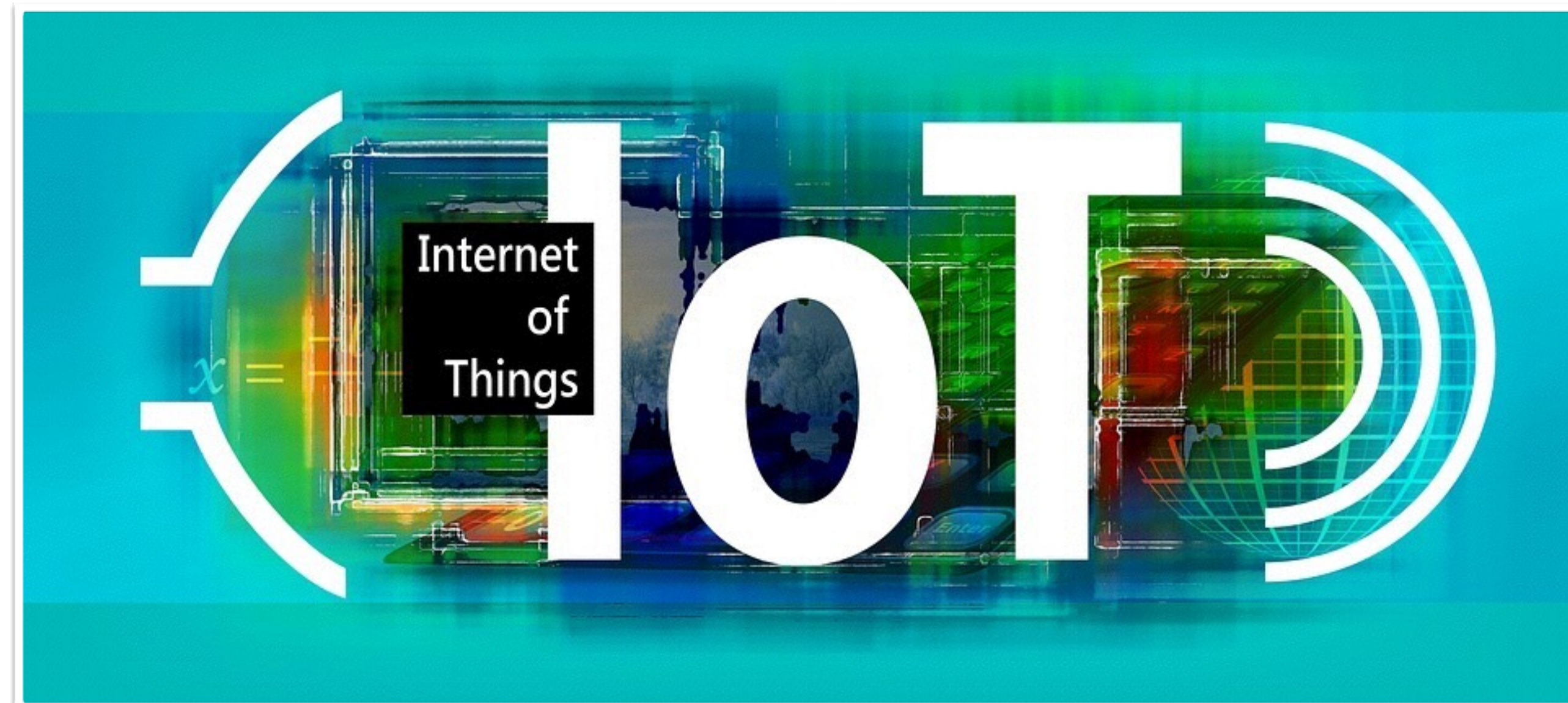
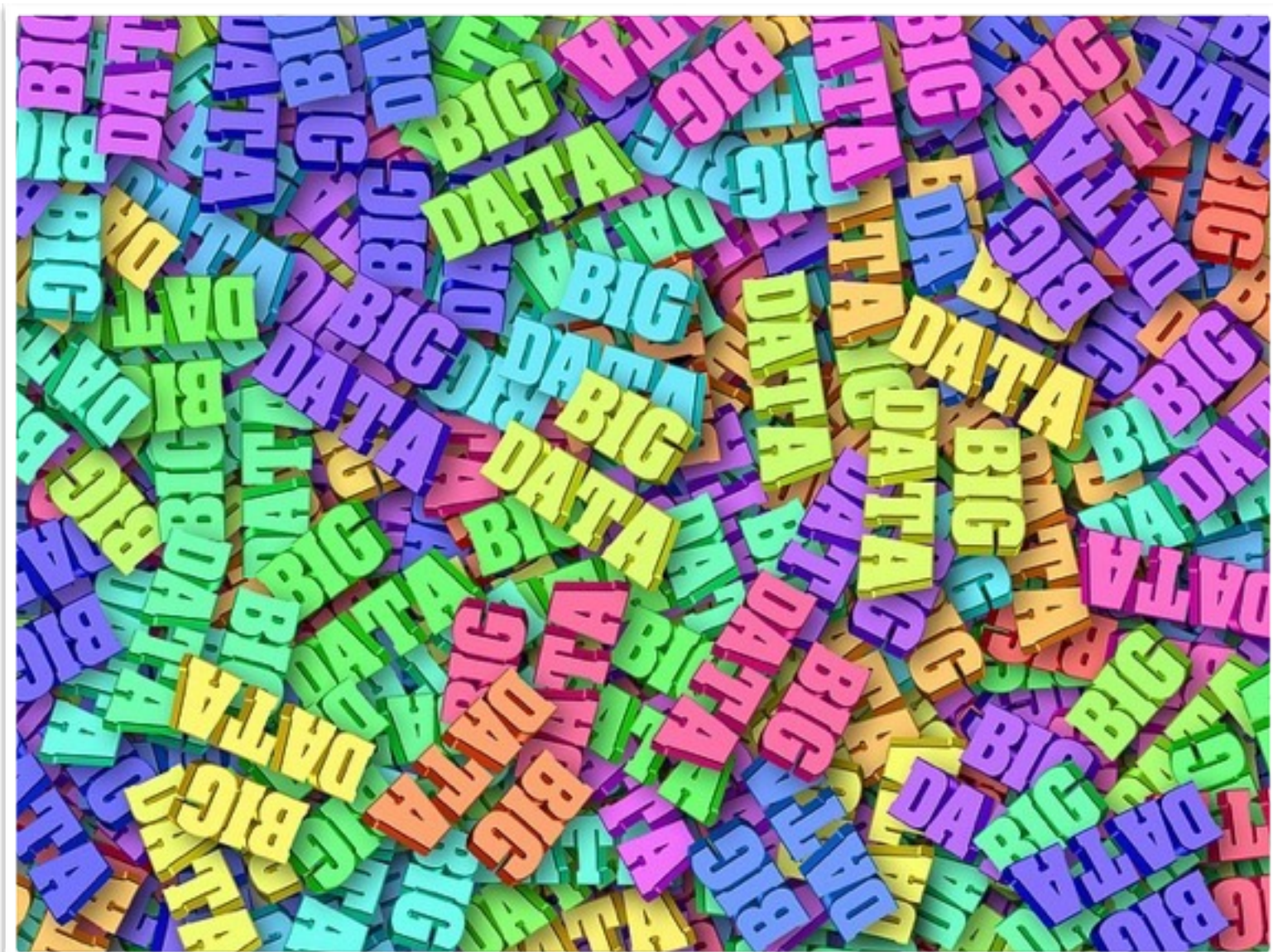
15.1. The list of licenses for free software used for the Game is available at:

<https://draconiusgo.com/policy/licenses-and-notifications>.

Accept

Decline

I dag - helt andra krav





Juridik - GDPR

JURIDIK



Man gör först och i efterhand får man veta om man gjort rätt/fel



Vad är GDPR?

GDPR = **G**eneral **D**ata **P**rotection **R**egulation
(Dataskyddsförordningen på svenska)

GDPR ersätter tidigare regelverk

En harmonisering av lagstiftningen inom EU



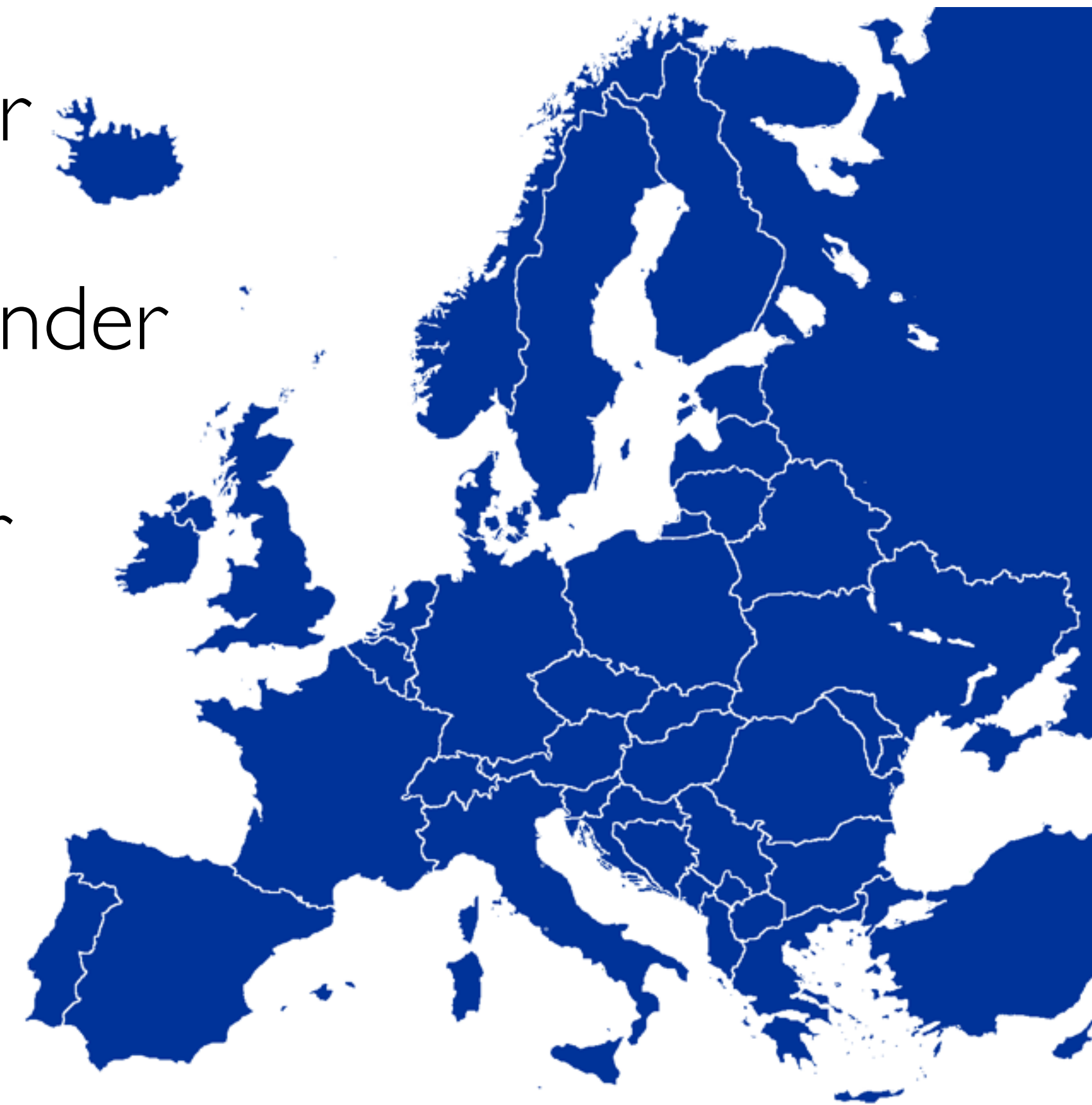


Syfte med GDPR?

Skydda fysiska personer vid behandling av personuppgifter

Skapa smidigt flöde av personuppgifter mellan medlemsländer

Öka enskilda individers kontroll över sina personuppgifter





EU-nivå - Europeisk myndighet



Nationell nivå - tillsynsmyndighet



EU-nivå - Europeisk myndighet
(European Data Protection Board)

Rådgivande för att harmonisera mellan EU-länderna

Publicera material (riktlinjer, best practice etc) för
att det ska bli en enhetlig tillämpning av GDPR inom EU



Ta emot anmälningar om överträdelser

Bestämna **sanktionsavgifter** vid överträdelser

Samarbeta med andra dataskyddsmyndigheter inom EU



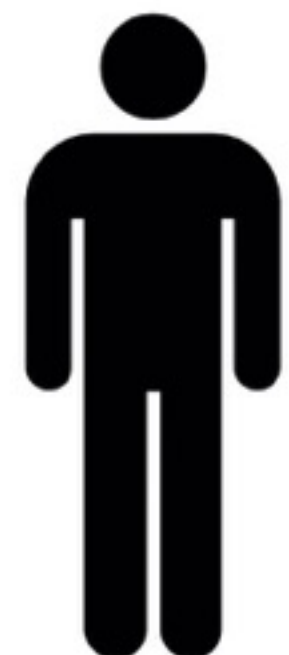
Nationell nivå - tillsynsmyndighet
i Sverige: Datainspektionen
(namnbyte till Integritetsskyddsmyndigheten
eller dataskyddsmyndigheten)



3 roller som ska finnas



Dataskyddsbud



Personuppgiftsansvarig



Personuppgiftsbiträde



Dataskyddsbud

Alla **myndigheter** måste ha ett ombud (anställd eller konsult)

En person kan vara ombud för flera myndigheter

Rollen förstärks/ökade krav:

- **Rätt kompetens**
- Självständighet
- Resurser

I uppgifterna ingår att

- **informera** och **ge råd** till personuppgiftsansvarig och biträde
- övervaka efterlevnad
- ta emot klagomål från registrerade
- fungera som kontaktperson för tillsynsmyndigheten



Personuppgiftsansvarig

Utökade skyldigheter för personuppgiftsansvarig

Skyldighet att föra **register** över ändamål med behandlingar övergår från ombud till personuppgiftsansvarig (art 30)

Ostrukturerad behandling ska också förtecknas, d v s alla dokument man har där personuppgifter ingår behöver **gallras** och **det som sparas ska förtecknas!**

Rutiner för att utreda, dokumentera och rapportera incidenter (till tillsynsmyndigheten) ska finnas
(undantag om det är osannolikt att incidenten medför risk för enskilda)



Personuppgiftsbiträde

Personuppgiftsbiträdet får ett självständigt **skadeståndsansvar** gentemot de registrerade

Företag eller fysisk person

Personuppgiftsbiträdet skyldig att hålla ett **register** över kategorier av behandlingar (art 30)



Personuppgiftsbiträdesavtal



Kommunen

Personuppgiftsansvar

Personal

Molntjänstleverantör

biträder kommunen när
det gäller personuppgifter

ex Google (Suite)
eller O365

Ett **personuppgiftsbiträdesavtal** upprättas mellan kommunen och molntjänstleverantören



Personuppgiftsbiträdesavtal

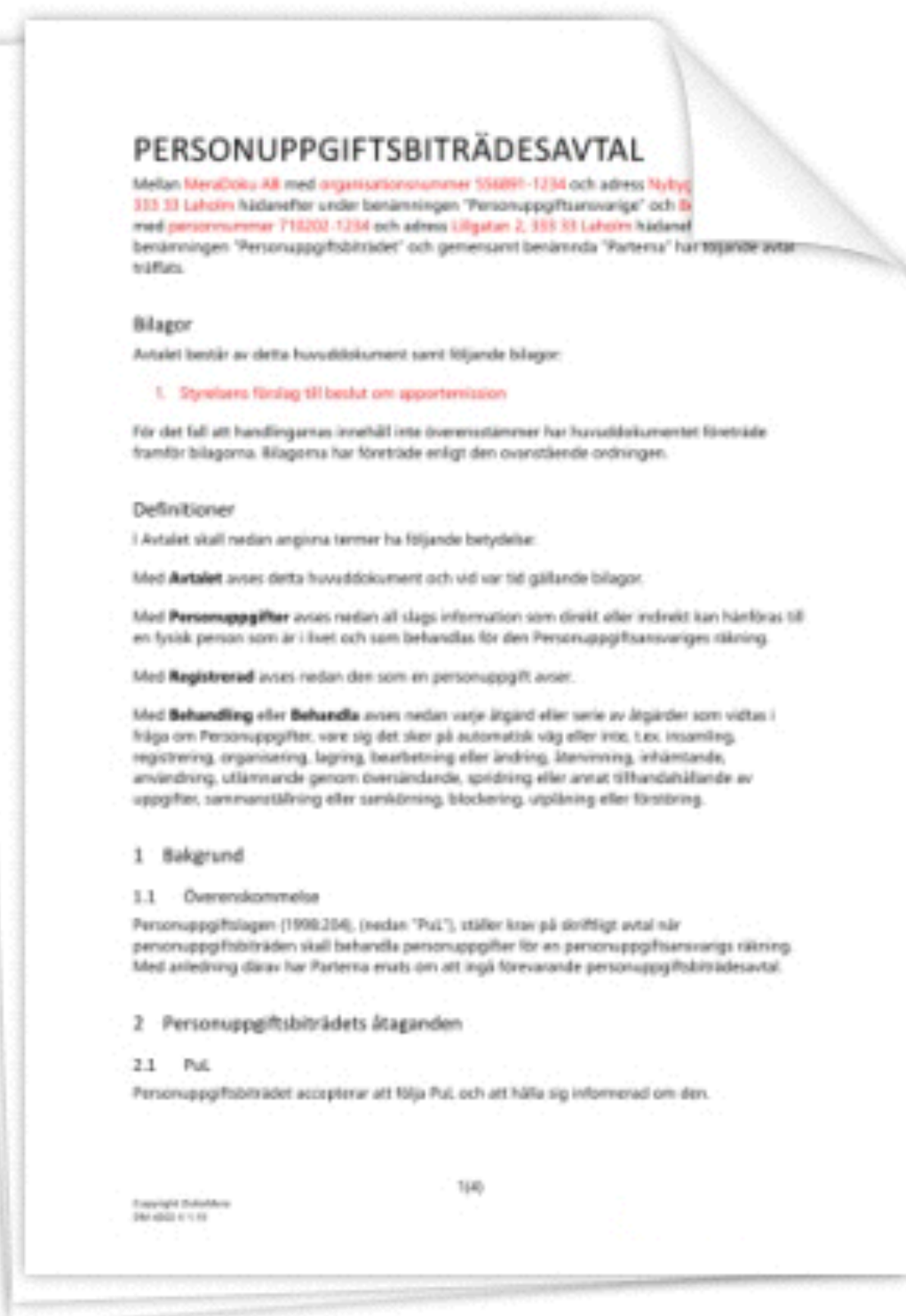


Avtalet säkerställer att GDPR och andra **lagar följs**

Risk- och sårbarhetsanalys krävs

Ju **känsligare data** som hanteras,
desto **högre krav** finns på inloggning och kryptering

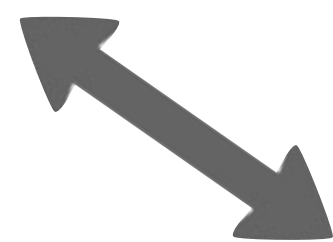
Personuppgiftsbiträdesavtal krävs för **alla**
molntjänster som hanterar personuppgifter



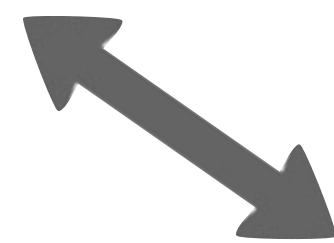


Översikt

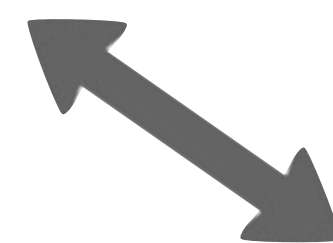
EU-nivå
Europeisk myndighet



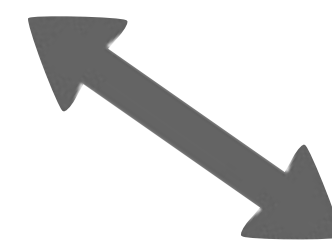
Nationell nivå
Tillsynsmyndighet



Myndighetsnivå
Dataskyddsombud



Verksamhetsnivå
Personuppgiftsansvarig



Personuppgiftsbiträde



Personliga data som måste skyddas

All information som kan relateras till en individ, oavsett om det gäller individens yrkesliv, privatliv eller offentliga liv.

- Namn
- Användarnamn
- Lösenord
- Fotografi
- E-post adress
- Datorns IP-adress
- Webhistorik med cookies
- Inlägg på sociala medier
- Information kopplat till individens finansiella, ekonomiska eller medicinska situation
- Information som kan leda till mobbning eller diskriminering av individen
- Data som kan användas för identitetsstöld

PUL:

All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet räknas enligt personuppgiftslagen som personuppgifter. Även bilder (foton) och ljudupptagningar på individer som behandlas i dator kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas som personuppgifter om de kan kopplas till fysiska personer.



Definitionen av personuppgifter breddas

Definitionen av personuppgifter breddas, nu inkluderas även data som behandlar



Genetisk information



Psykisk hälsa



Kulturell tillhörighet



Ekonomi



Social tillhörighet



Missbruksregeln försvinner

I personuppgiftslagen finns en förenklad regel för behandling av personuppgifter i löpande text och enkla listor, **missbruksregeln**. Den innebär kort och gott att man får behandla uppgifter i vissa situationer så länge det **inte är kränkande** för någon. Den här regeln **försvann** när GDPR började gälla.

Det påverkar hur vi hanterar t ex listor med personuppgifter



Principer för behandling av personuppgifter

Laglighet,
korrekthet

Ändamåls-
begränsning

Uppgifts-
minimering

Lagrings-
minimering

Integritet och
Konfidentialitet



Personal

Vilka program/appar/tjänster/webbapplikationer använder ni?

Vet ledningen om svaret på frågan ovan?

Hur samlas data in i var och en av dessa?

GDPR-säkrade? Finns avtal med leverantör?



”Privacy”



”Privacy by design”

Man tar i beaktande när man skapar en tjänst att datan ska skyddas

”Privacy by default”

De striktaste inställningarna ska vara standard när det gäller personlig data



Konkreta exempel

- Fritextfält i formulär
- "Sjuk" som frånvaroorsak
- Inloggning via internet
- Hur länge får uppgifterna sparas?
- Information om vad som registreras
- Får alla läsa om alla barn/elever?

www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/skolor/checklista-for-hantering-av-personuppgifter/

Känslig uppgift: <http://www.datainspektionen.se/Documents/diverse/forfragan-kanslig-personuppgift.pdf>



Konkreta exempel

- Fritextfält i formulär



Konkreta exempel

- "Sjuk" som frånvaroorsak



Konkreta exempel

- Inloggning via internet



Konkreta exempel

- Hur länge får uppgifterna sparas?



Konkreta exempel

- Information om vad som registreras



Konkreta exempel

- Får alla läsa om alla barn/elever?



När får man behandla uppgifter om elevens prestationsnivå?

Prestationsuppgifter utgör **känslig information**, men behandlingen har tidigare ansetts **nödvändig** för att uppfylla elevens rätt till utbildning, så **samtycke har inte krävts**.

Hur kommer detta att tolkas under GDPR?
Troligen på samma sätt.



Konkreta exempel

Digitala tjänster som textar i realtid i samband med filminspelning

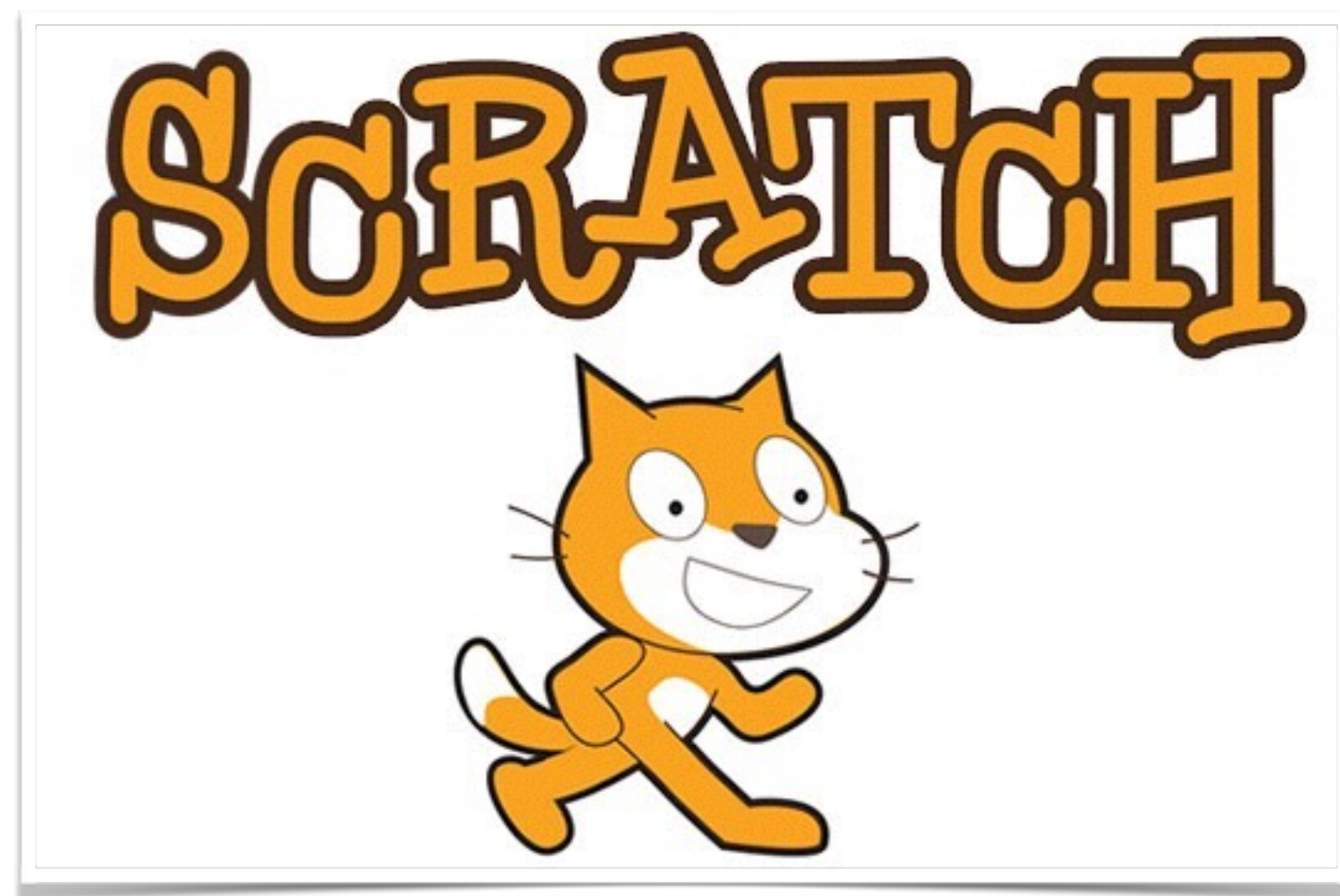
Var hamnar datan? Inom EU? Annars inte ok.

Personal kan inte ha den detaljkollen

Konkreta exempel



Kommer ni att kunna använda dessa digitala tjänster i verksamheten framöver?



Konkreta exempel

Vanliga program och appar kan stoppas

GDPR Populära verktyg för att lära ut programmering kan vara oförenliga med dataskyddsreglerna. De lagrar personuppgifter utanför EU.



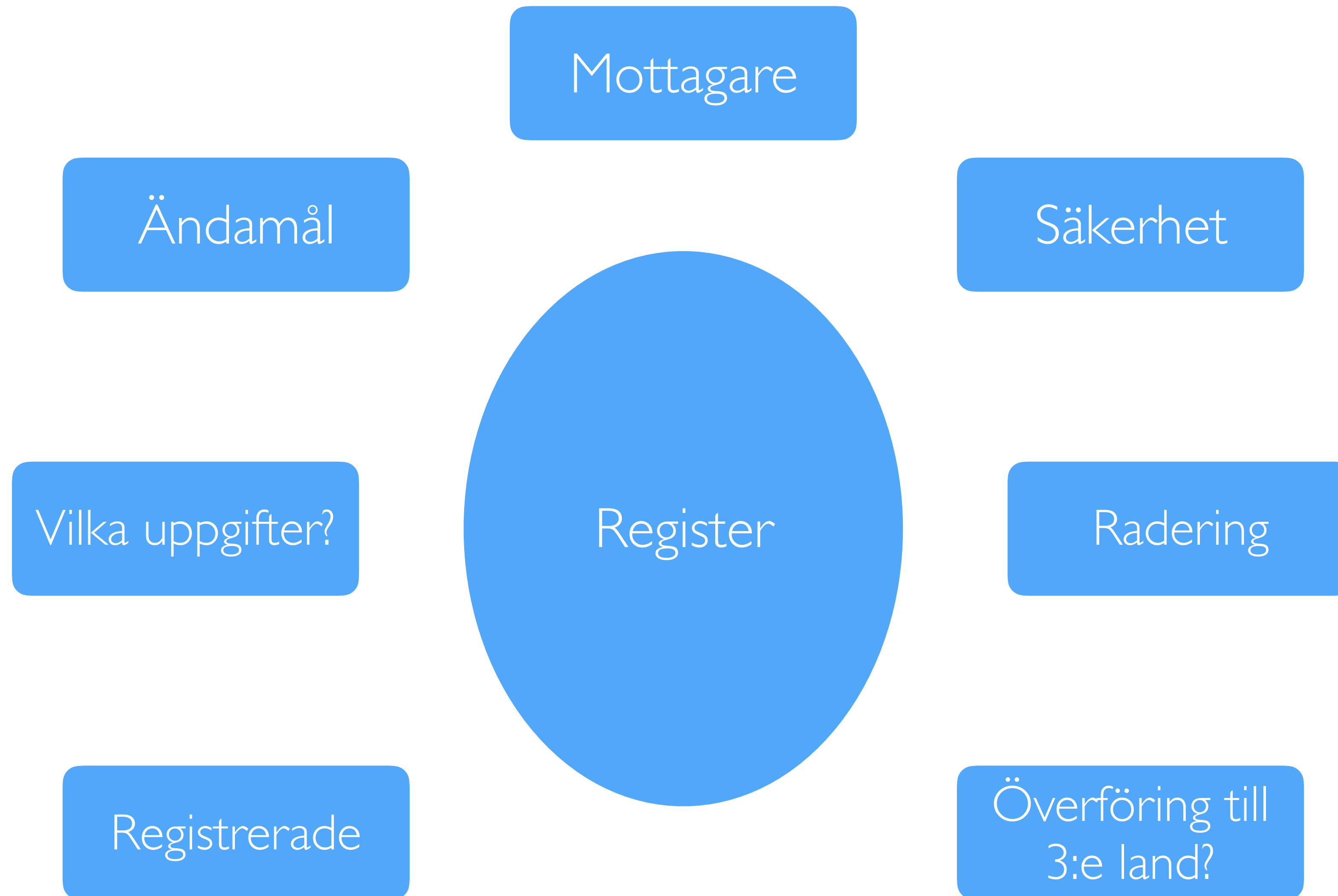


Register

Skyldighet att föra register över ändamålen med behandlingar mm (art 30) övergår från ombudet till den **Personuppgiftsansvariga**

Ostrukturerad behandling ska också förtecknas

Register över register ska finnas





Vad ska ett register över personuppgiftsbehandling innehålla?

- Den personuppgiftsansvariges kontaktuppgifter
- Ändamålen med behandlingen (**varför?**)
- En beskrivning av den eller de kategorier av registrerade som berörs och kategorier av personuppgifter som hänför sig till dem (**vilka och vad?**)
- Mottagarna eller kategorier av mottagare till vilka uppgifterna kan komma att lämnas ut (**till vem?**)
- Om personuppgifterna ska föras över till tredje land
- En allmän beskrivning som gör det möjligt att preliminärt bedöma lämpligheten av de informationssäkerhetsåtgärder som vidtagits för att trygga säkerheten i behandlingen (**säkerhet?**)



GDPR - enkel riskanalys - jämvikt?

Art

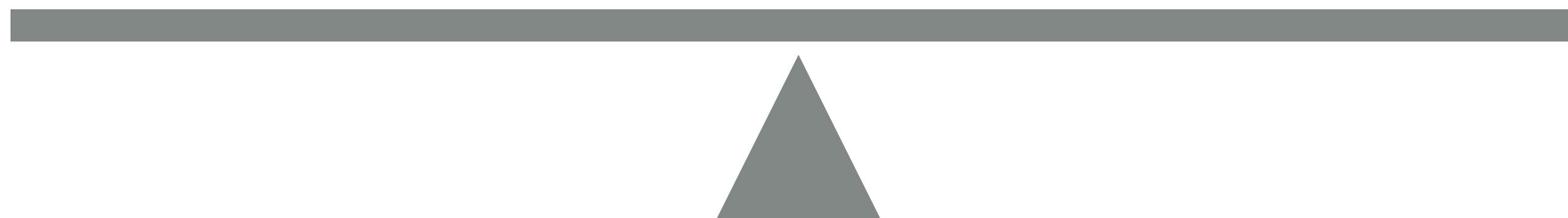
Omfattning

Ändamål

Sammanhang

Risk

Tekniska och
organisatoriska
skyddsåtgärder





GRANSKNING

[OM OSS](#) [KONTAKTA OSS](#) [PRESS](#)

Sök frågor och svar, vägledning och

[OM INTEGRITET](#)

[VÄGLEDNINGAR](#)

[LAGAR & REGLER](#)

[KURSER & FÖRELÄSNI](#)

[Start](#) → [Nyheter](#) → [Datainspektionen inleder första granskningarna enligt GDPR](#)

Publicerad 2018-06-08

Datainspektionen inleder första granskningarna enligt GDPR

Myndigheten undersöker om företag och myndigheter som är skyldiga att utse ett så kallat dataskyddsbud, verkligen har gjort det. Bland annat ska privata vårdgivare, försäkringsbolag och banker granskas.



Bra länkar samt källor

www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/dataskyddsdagen/

www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/

www.datainspektionen.se/Documents/enkel-kurs-dataskydd.pdf

<https://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/dataskyddsforordningenskola.14377.html>

<https://klasa-info.skl.se/>

Google Suite - uppdaterat personuppgiftsbiträdesavtal

https://admin.google.com/terms/apps/3/1/en/dpa_terms.html

www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/skolor/checklista-for-hantering-av-personuppgifter/

www.datainspektionen.se/Documents/diverse/forfragan-kanslig-personuppgift.pdf



Tack för er uppmärksamhet
och lycka till med GDPR!