

2018 ATEA
BOOT
CAMP

Välkommen

Atea

GDPR - Undvik att det blir en
dagslända och gör det till er vardag!

Föreläsare:

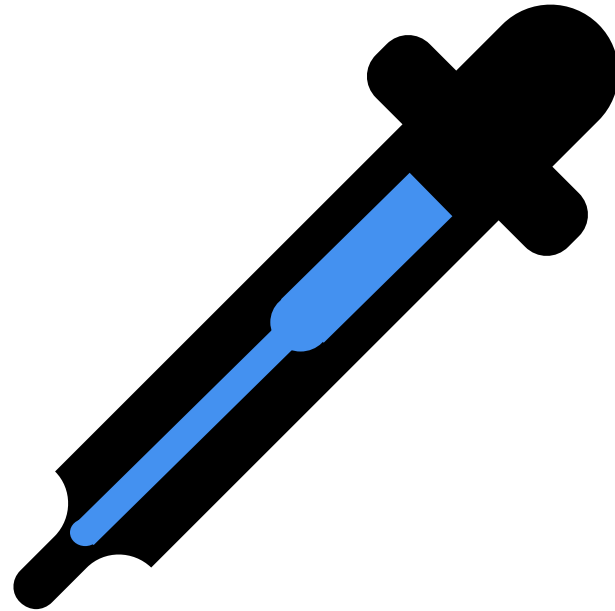
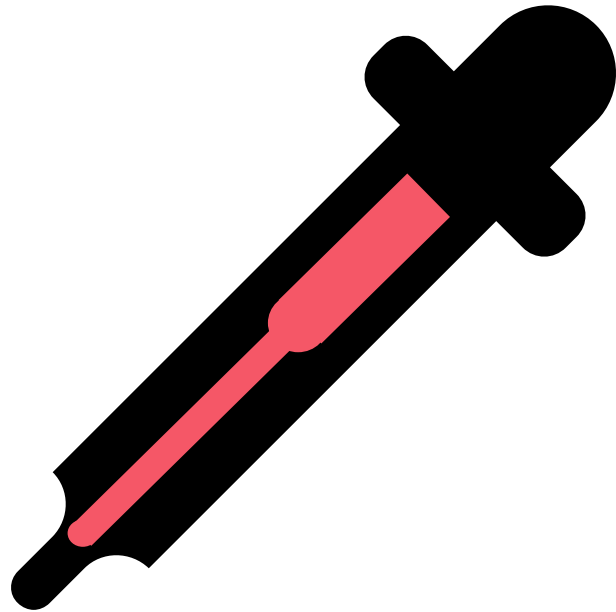
Carl-Magnus Brandt, Atea



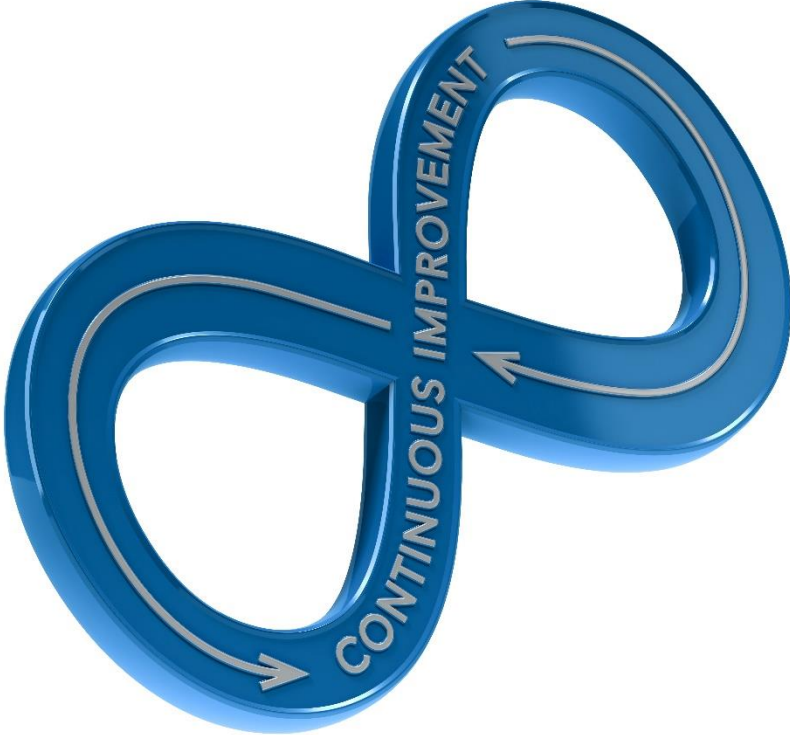
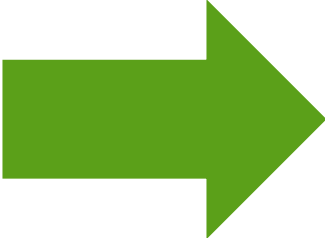
Start with the end in mind

ATEA

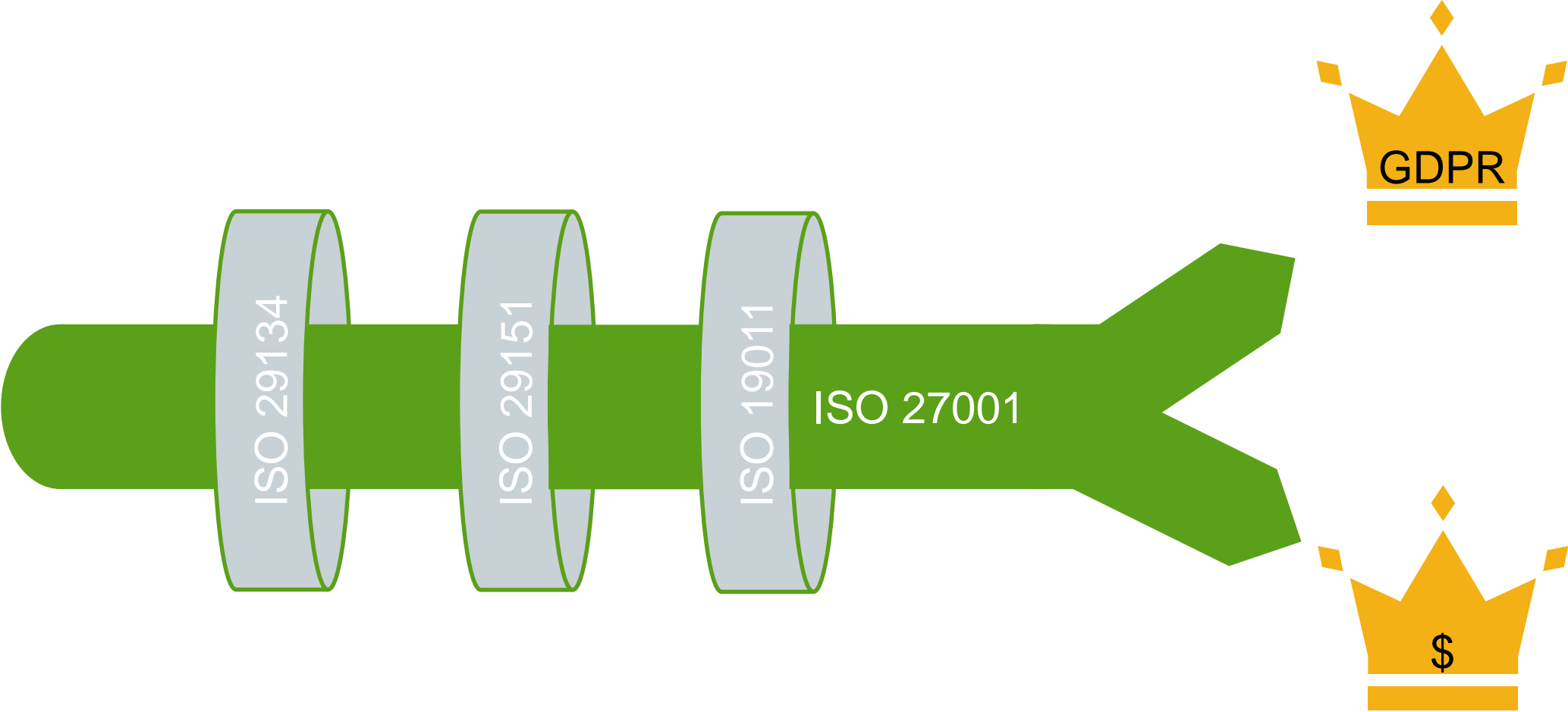
Hur mår ert GDPR-projekt idag?



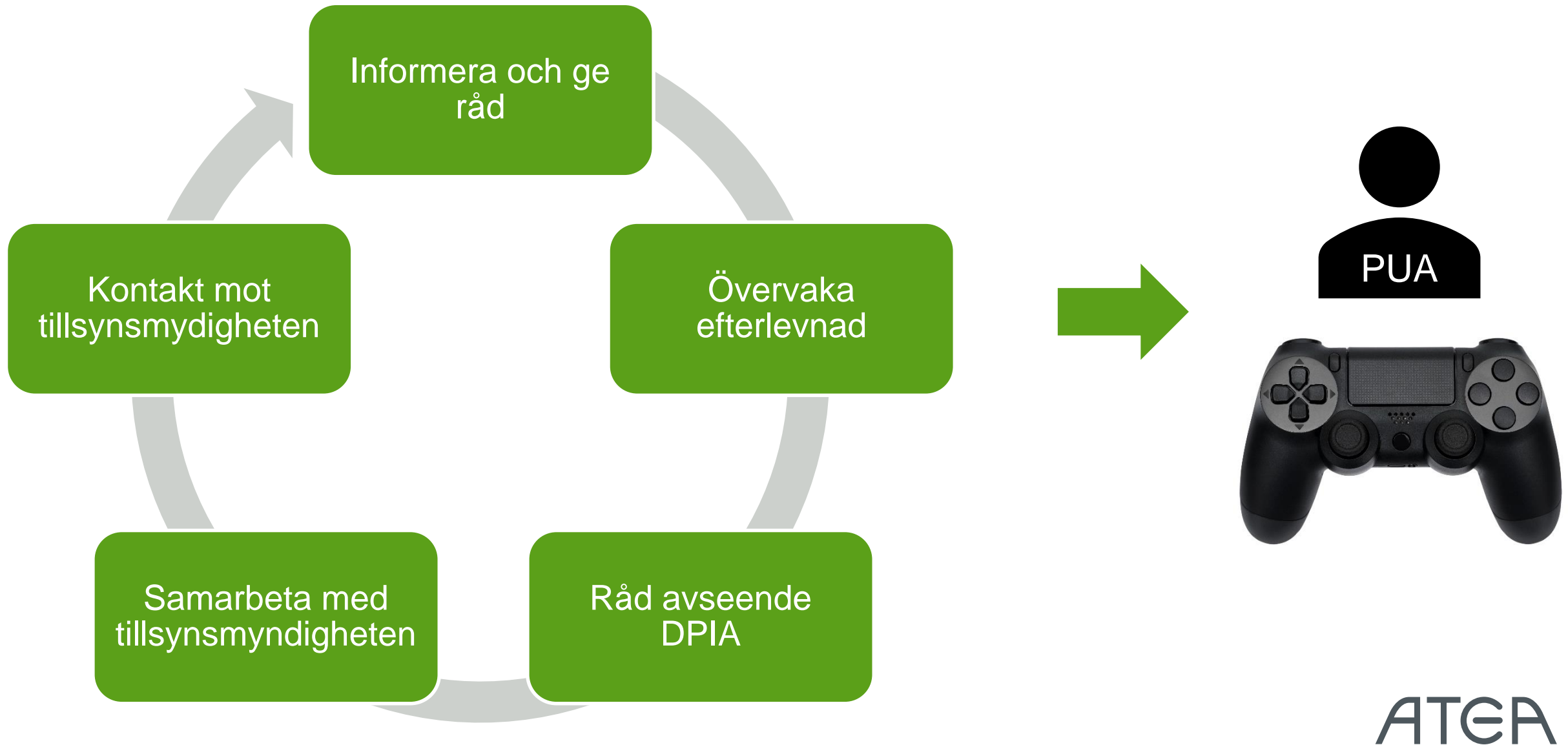
Utmaningen, “still doing business”



Systematiskt informationssäkerhetsarbete



DPO - möjligheter, uppgifter och ansvar



Transparens och tillgänglighet

Din trygghet är viktig för oss

Oavsett om du är elev, förälder, medarbetare eller deltagare i någon av våra vuxenutbildningar, vill vi på AcadeMedia att du ska känna dig trygg med att vi hanterar dina personuppgifter på ett säkert sätt. På de här sidorna berättar vi om vilka personuppgifter vi behandlar, varför vi gör det och vad vi gör för att skydda dem.

Läs mer om vad som gäller för just dig genom att välja roll i listan nedan.

Jag är vårdnadshavare ▾

Vi har anpassat innehållet så det är aktuellt för dig som vårdnadshavare

Personuppgiftsbehandling

Barn i förskolan ▾

Visa rapport ↓



Powered by [DPOrganizer](#) - Data Protection Management Software

Barn i förskolan ▾

För Barn i förskolan behandlar vi 22 olika typer av personuppgifter: Namn, Personnummer, E-post adress, Grupp (avdelning)/förskola, Vistelseid Förskolan, Ersättning (förskolepeng), Kommunens utbetalningsunderlag, Beskrivningar av barnets förändrade kunskande, Adress, Egenvård - medicinska behandlingsscheman, Orosanmälningar till socialtjänst, Diskriminering/kränkande behandling, Specialkost, Incidenter/tillbudsrapport, Klagomålsärenden, Foton/film, Medicinsk anamnes, Psykologisk anamnes, Specialpedagogiska behov, Psykosocial status, Extra anpassningar, Foto/bild.

Personuppgiftsansvarig som är juridiskt ansvarig är Pyssling Förskolor och Skolor AB, Vittraskoloma AB.

Källan fick vi dina personuppgifter från ^

Ändamål och rättslig grund för behandling av dina personuppgifter ^

Personuppgiftsbiträden som vi använder för att behandla dina personuppgifter ^

Andra parter som vi delar dina personuppgifter med ^



Powered by [DPOrganizer](#) - Data Protection Management Software

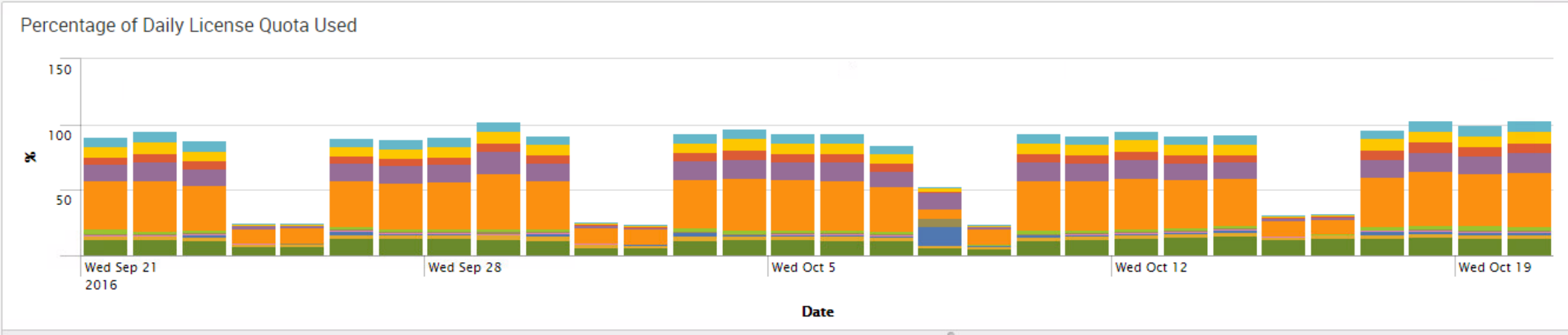
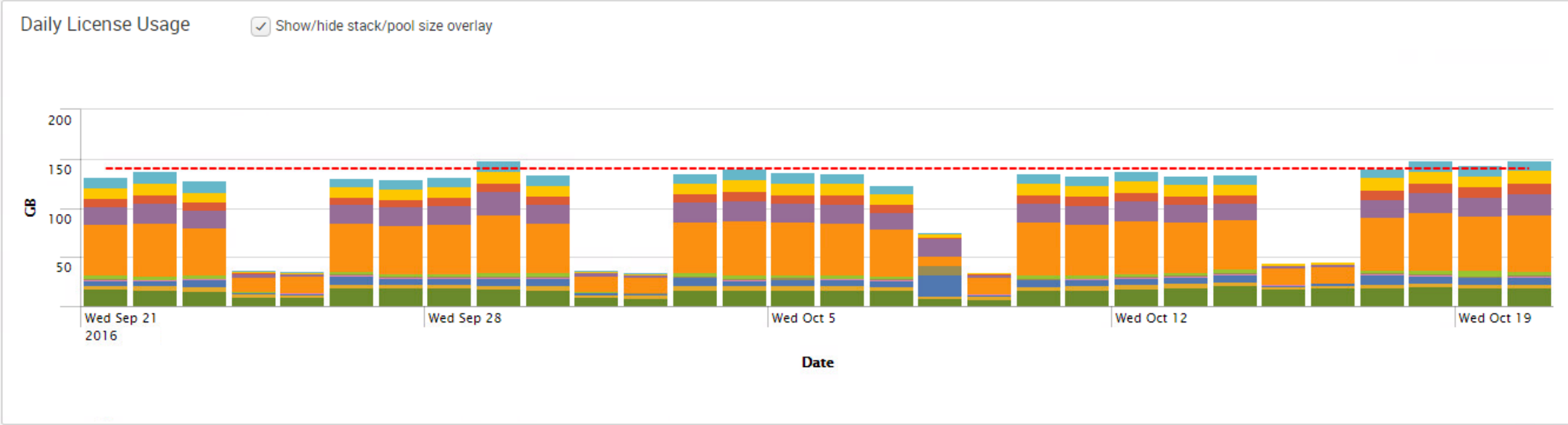
ATEA

”safety into design”



ATEA

DPbDbD = god affär



Rollbaserad behörighetskontroll

Role Based Access Control (RBAC)

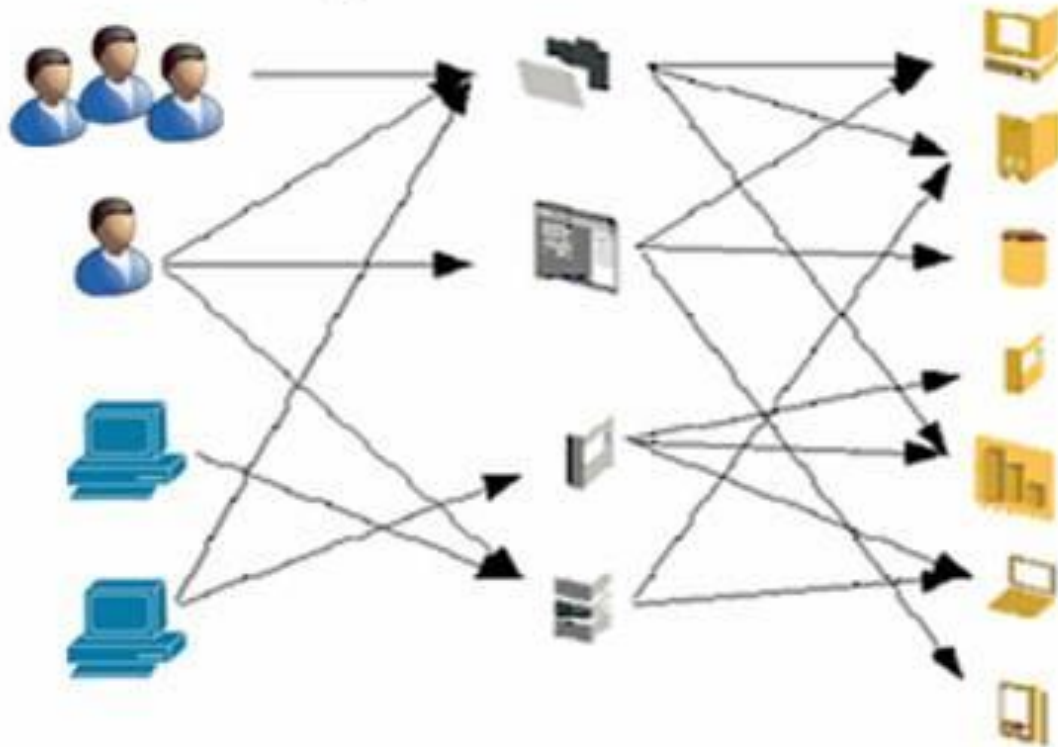
Identities

Roles

Resources

Role assignments

Permissions



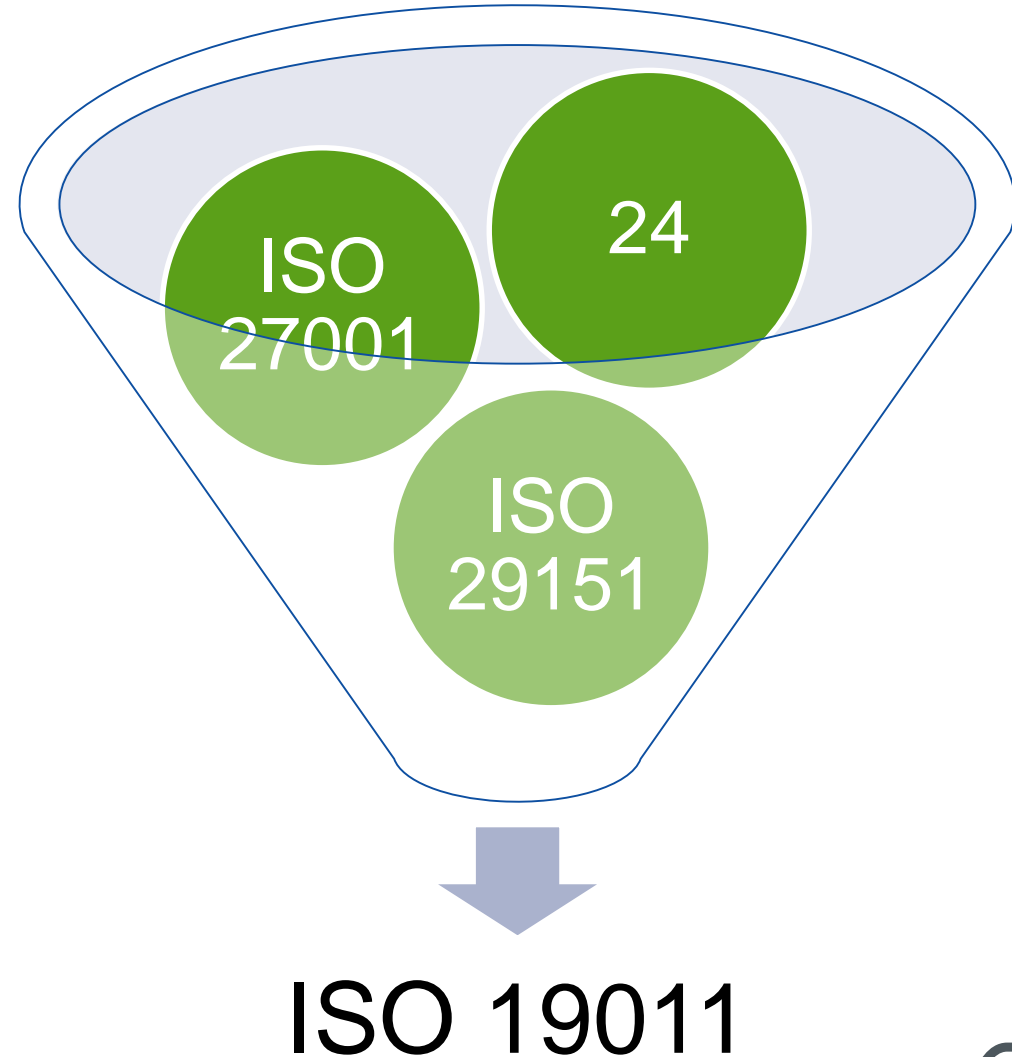
”Data protection by design and by default”



GDPR Audit – Redovisar efterlevnad enligt art 24

ATEA GDPR Audit

#	Mandatory Control/Security Mechanism	Status	Audit Comment
1	Records of Processing		
	Defined purpose		
	Legal basis for processing (consent management; LIA)		
	Media (Hw, Sw, communication channels, paper-based)		
	Data minimization		
	Completeness (departments and systems)		
	Retention times defined and implemented		
	Controls identified		
2	Data Protection Impact Assessment		
	Potential effects on rights and freedoms of individuals from CIA perspective		
	Sources of risks (who/what caused event; internal/external human and non-human sources;		
	High risk processing (Art. 9) applicable		
	Identification of possible threats		
	Existing or planned measures		
	Impact and likelihood assessment		
	Project management process (new DPIA)		
3	User Awareness/Security Policies		
	Educate and raise awareness among individuals handling personal data		
	Minimum annual security awareness training		
	Enforce Information Security Policy and/or Data Protection and Privacy Policy (PII protection)		
4	Authentication/Access Management/Provisioning		
	Define a unique identifier (login) for each user (no group accounts)		
	Adopt an enforced user password policy		
	Require each user to change his or her password whenever it has been resetted		
	Limit the number of access attempts to an account		
	Define authorisation profiles/roles (privileged access)		
	Remove obsolete access permissions (process)		
	Perform annual review of authorisations		
5	Event Logging and Monitoring		
	Implement a logging system		
	Inform users of the implementation of the logging system		
	Protect logging equipment and the information logged		
6	End User Protection		
	Securing workstations		
	Organise an automatic session locking procedure		
	Use regularly updated antivirus software		
	Install fire all software		
	Collect the user's consent before any intervention on his or her workstation (reserve right in User Policy)		
	Define acceptable use (User Policy)		
	Clean desk policy		
7	Mobile Devices		
	Securing mobile data processing		
	Securing mobile data storage		



ISO 19011

ATEA

Incidenthantering

Varför

GDPR

DpbDbD

0-72h

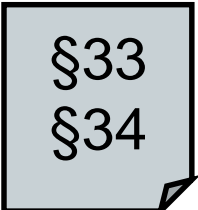
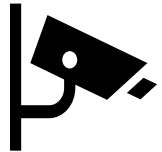
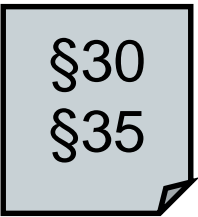
Hög risk



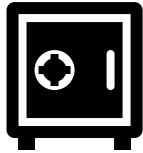
Vad

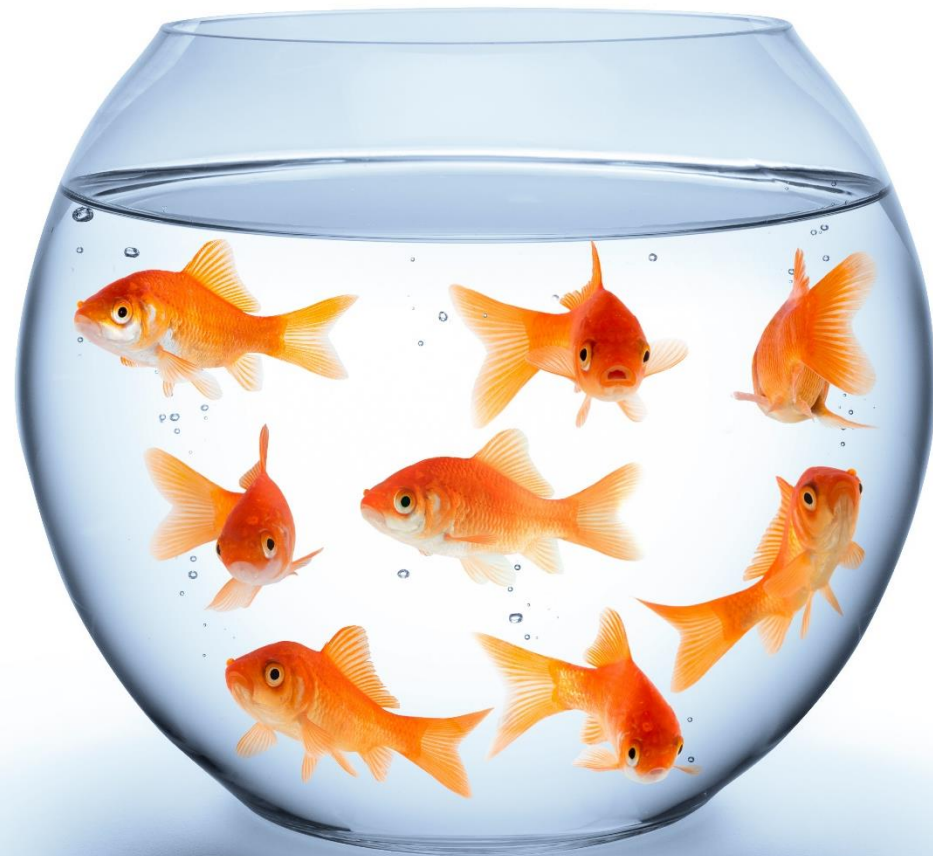
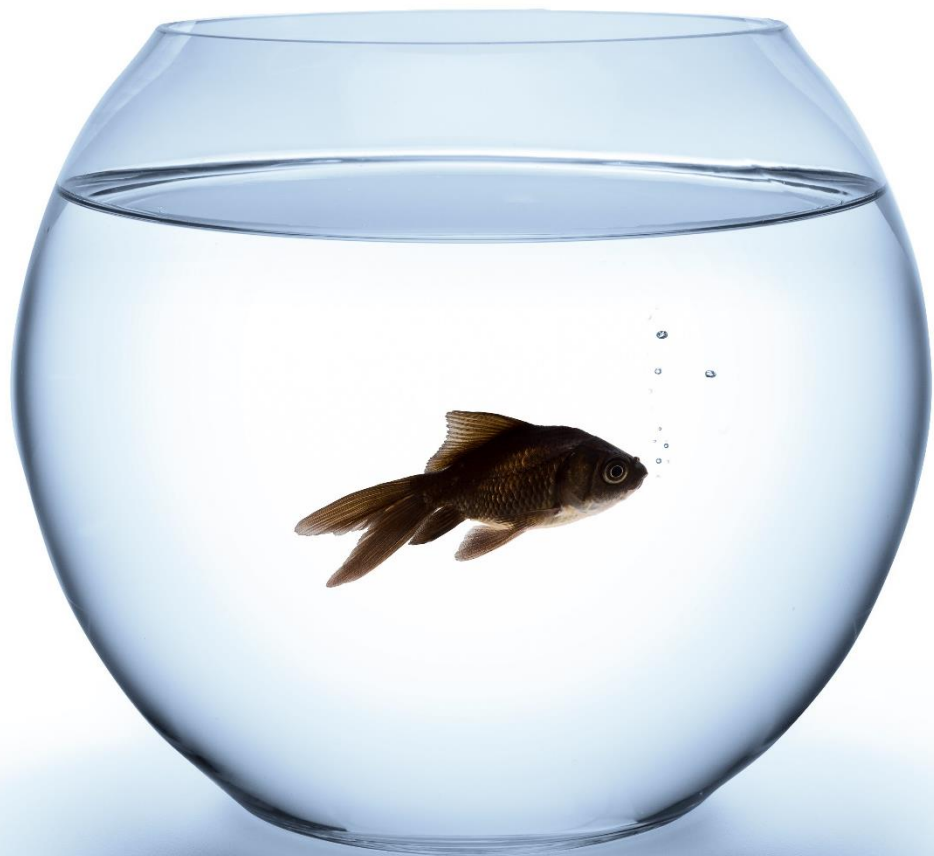


Hur



DPO





ATEA

2018 ATEA
**BOOT
CAMP**

Tack för mig

Företag

Vill du veta mer, registrera dig vid utgången.

Betygsätt gärna passet i appen.

REJTA
MITT PASS
I APPEN