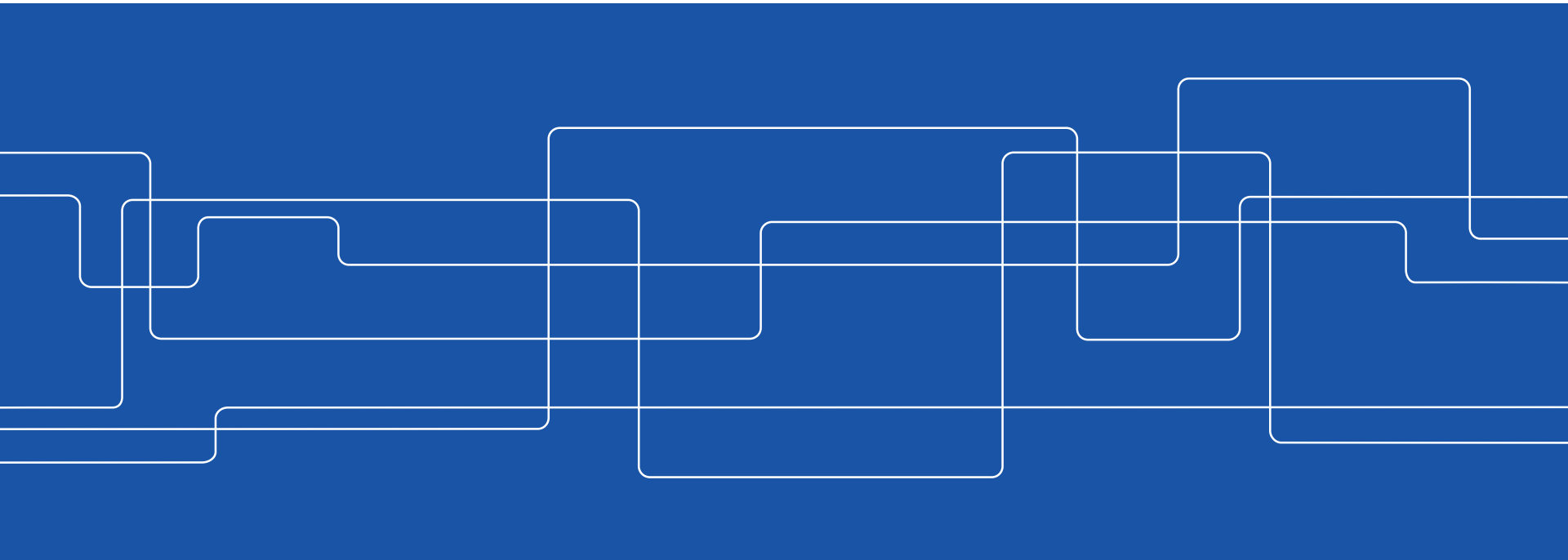
KTH ROYAL INSTITUTE
OF TECHNOLOGY

Dataskyddsförordningen (GDPR)

- En kort introduktion



Agenda

1. Allmänt om GDPR
2. Personuppgifter – vad är det?
3. KTH:s skyldigheter
4. Dataskyddsombudet
5. Den enskildes rättigheter
6. Personuppgiftsincidenter
7. Vad händer vid olydnad
8. Inskickade frågor
9. Avrundning

Allmänt om GDPR

EU:s allmänna dataskyddsförordning (GDPR)


ÖSTRA SMÅLAND

ÖSTRA SMÅLAND NYHETERNA

Lokal nyhetstidning på nätet

ostrasmaland.se/nyheterna.net

MISSA INTE!

Kalendern

Fem tips att läsa på webben:

DEL B

Grundligt Dumförklarade Personer i Riket - och dess konsekvenser

"Jag finns i okända japaners fotoalbum som illustration till hur stora människorna är i norra Europa. Det gör mig ingenting."

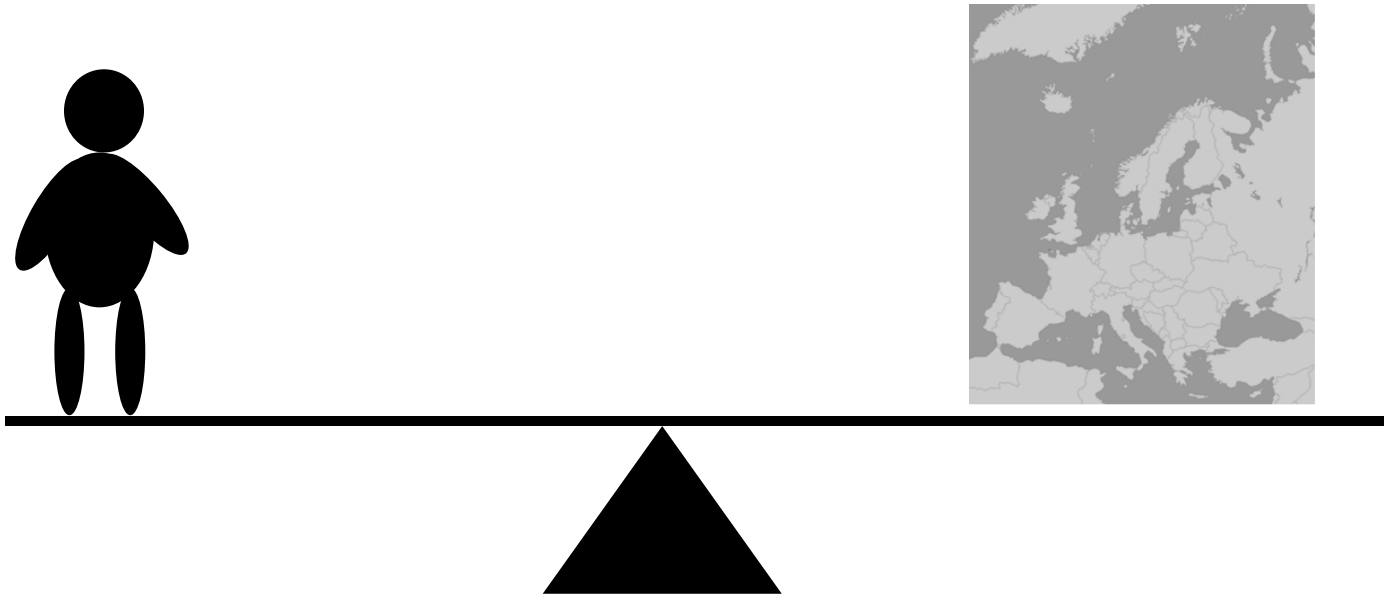
Källa: Östra Småland, 2 april 2019

- Evolution, inte revolution: Modernisering av direktiv från 1995, bl.a. p.g.a. tekniska utvecklingen
- Harmonisering inom EU
- Kompromissprodukt
- Direkt tillämpar i svensk rätt, nationella undantag medges
- Kompletteringslagar (dataskyddslagen, forskningsdatalagen)

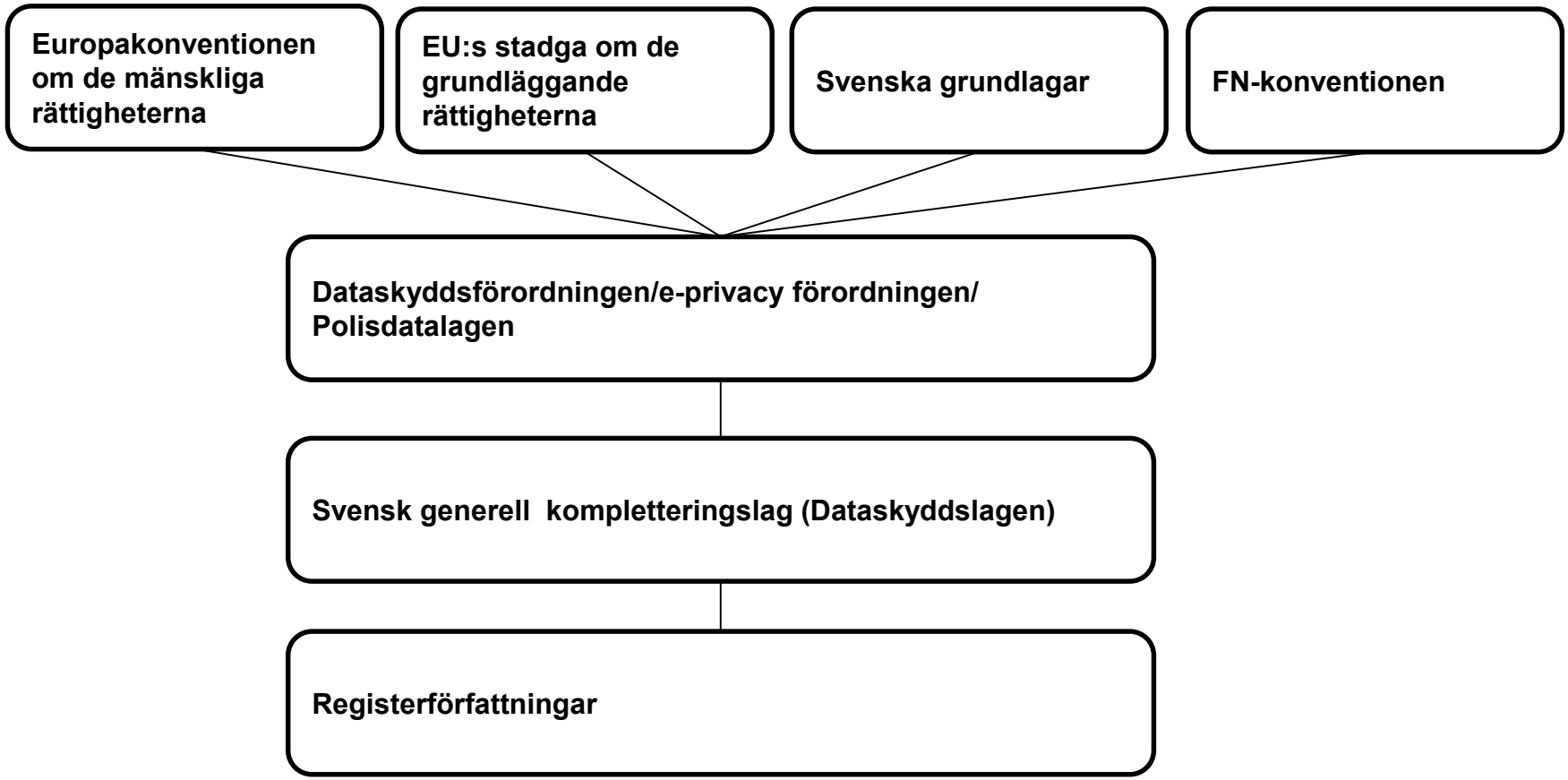
GDPR:s syfte

- Stärka individens rättigheter
- Skydda individens integritet

Öka rörligheten av tjänster och varor inom EU



Rätten till privatliv



Personuppgifter

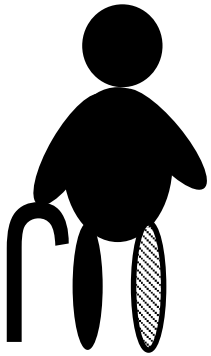
Personuppgifter - Definition

”**Varje upplysning** som **avser** en **identifierad** eller **identifierbar fysisk person**”

”…**särskilt med hänvisning till en identifierare** som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer”

”…**en eller flera faktorer** som är **specifika** för den **fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet**,”

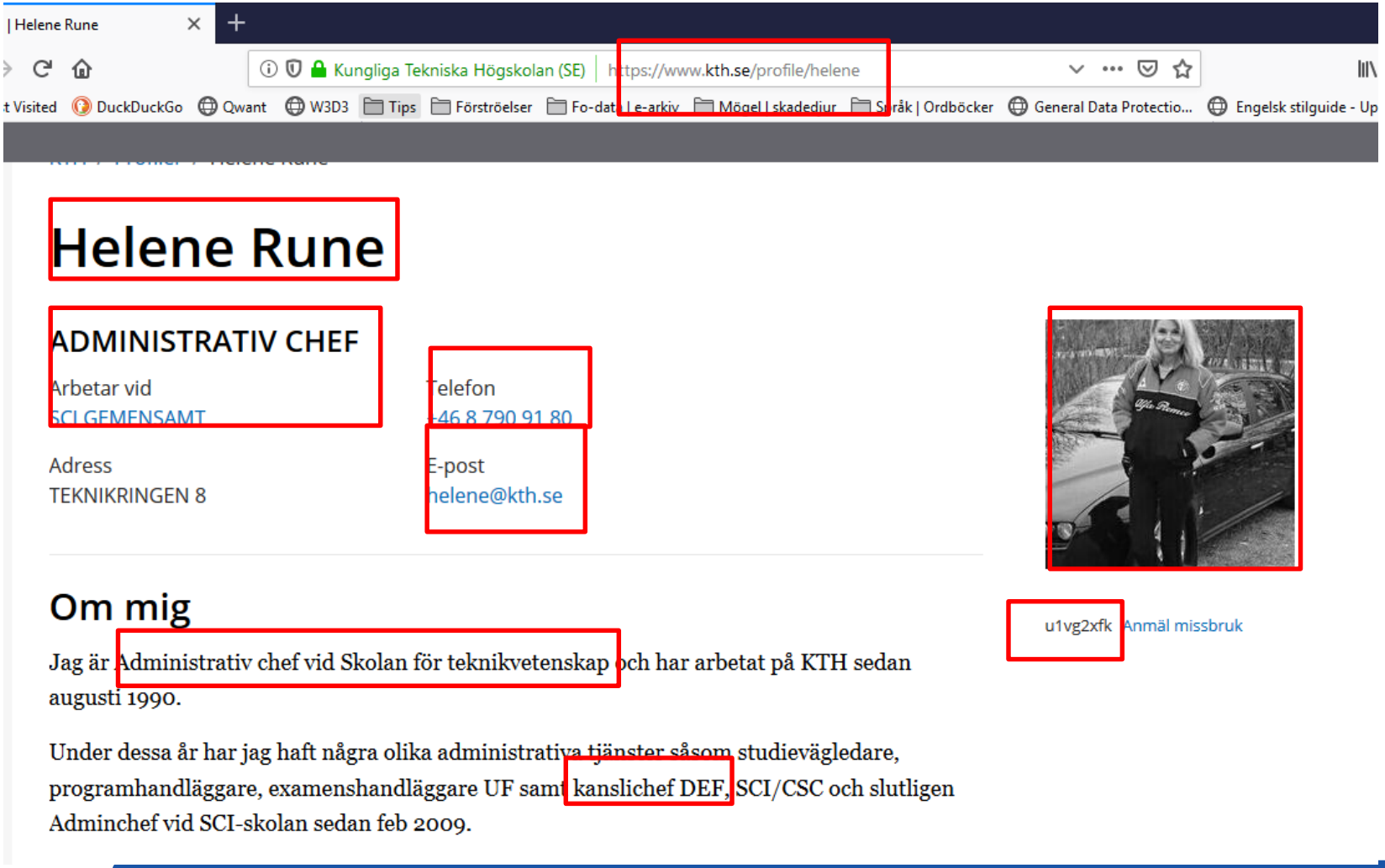
Känsliga personuppgifter



Personuppgifter om

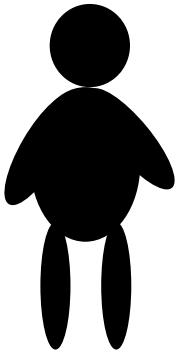
- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- hälsa
- sexualliv eller sexuell läggning
- **genetiska uppgifter**
- **biometriska uppgifter för att entydigt identifiera en fysisk person**

Några exempel



KTH:s skyldigheter

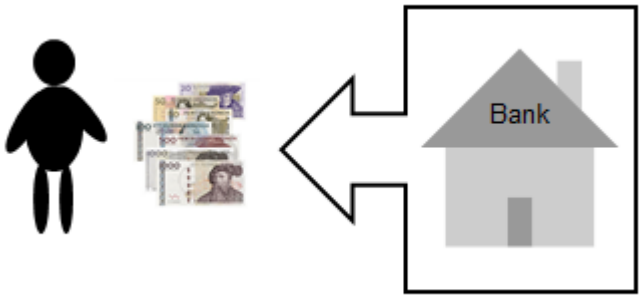
Kund – Bank



- Kontroll och ägarskap
- Veta vad banken gör med mina pengar
- Trygg förvaring
- Kunna flytta pengarna

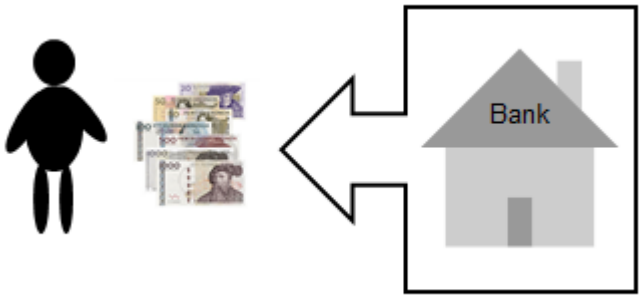
- Redovisa vad pengarna används till
- Skydda pengarna

Ansvarskyldighet (artikel 5)



- Enskildes rättigheter upprätthålls
- Både följa och att visa att vi följer GDPR (dokumentation, revisioner)
- Vi på ett tydligt och lättbegripligt sätt kan redogöra för hur KTH behandlar personuppgifter.
- Personuppgifterna ska alltid behandlas på laglig grund.
- Vi kan motivera varför KTH samlar in, bearbetar och förvarar personuppgifterna samt varifrån vi har fått uppgifterna. Det ska finnas ett tydligt ändamål med hanteringen.

Ansvarskyldighet (artikel 5)

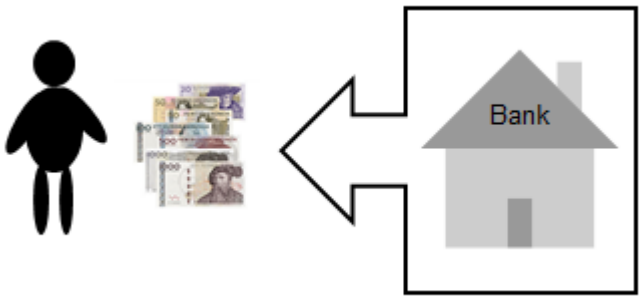


- Proportionalitet -- Vi ser till att personuppgifterna är relevanta och inte för omfattande i relation till syftet med insamlingen, bearbetningen eller förvarandet.
- Vi håller personuppgifterna korrekta och uppdaterade.
- Vi inte förvarar personuppgifter längre än nödvändigt med hänsyn till syftet. Vad som ska gallras och bevaras framgår av KTH:s dokumenthanteringsplan

Teoretiskt exempel

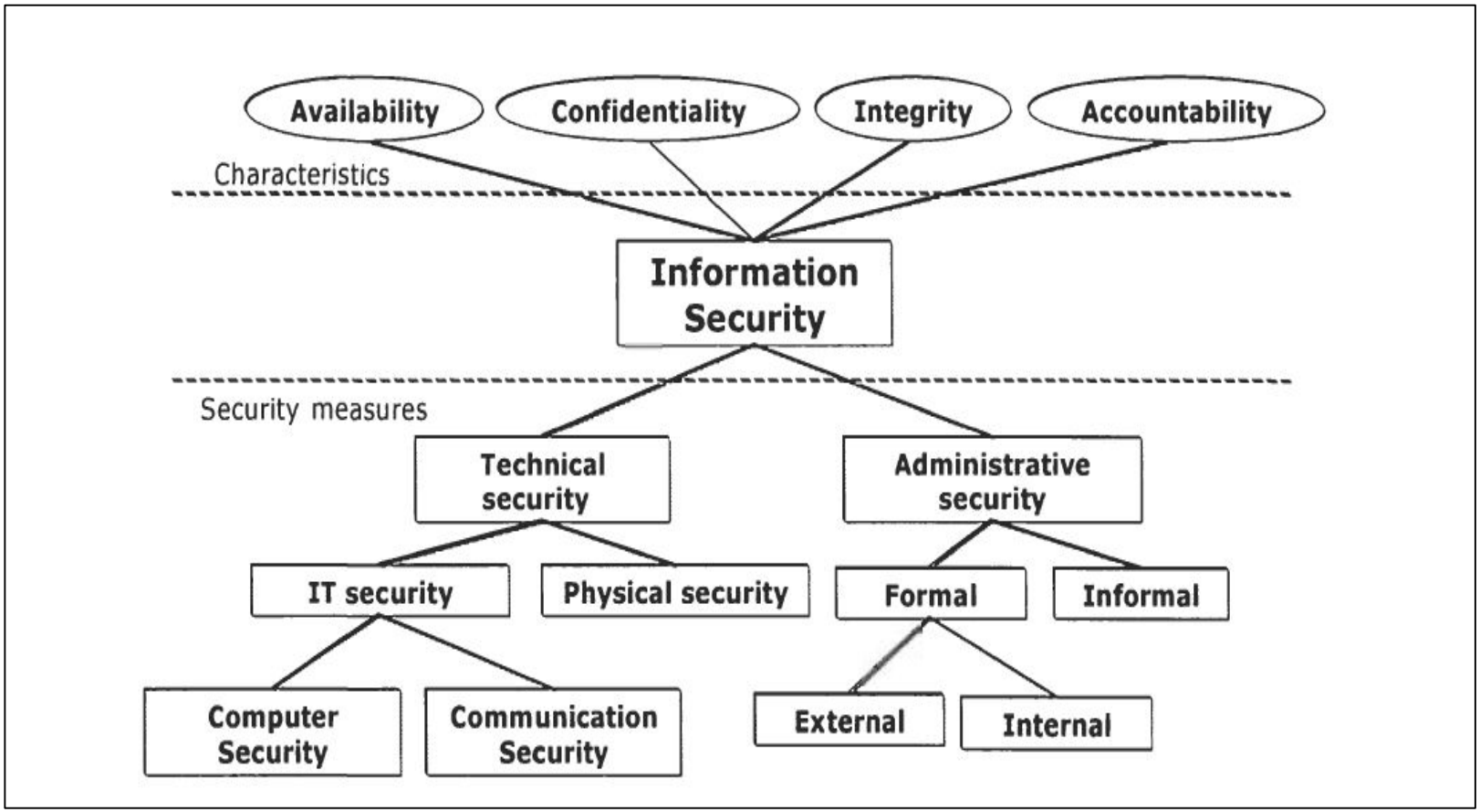
- Enskildes rättigheter upprätthålls
- Både följa och att visa att vi följer GDPR (dokumentation, revisioner)
- Rättslig grund
- Hanteringen av uppgifterna proportionerliga och i förväg bestämda ändamål
- Sparas inte längre än vad som är nödvändigt m.a.p. ändamål

Ansvarskyldighet (artikel 5)



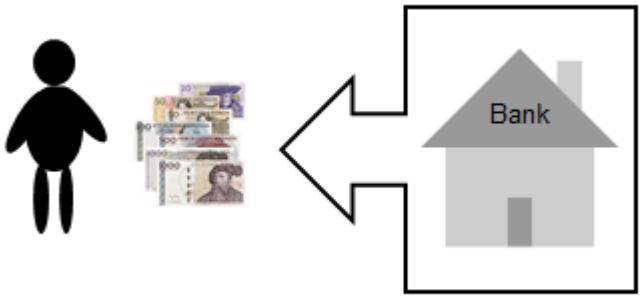
- Proportionalitet -- Vi ser till att personuppgifterna är relevanta och inte för omfattande i relation till syftet med insamlingen, bearbetningen eller förvarandet.
- Vi håller personuppgifterna korrekta och uppdaterade.
- Vi inte förvarar personuppgifter längre än nödvändigt med hänsyn till syftet. Vad som ska gallras och bevaras framgår av KTH:s dokumenthanteringsplan
- Vi vidtar tekniska/system och organisatoriska åtgärder för att säkerställa tillräckligt skydd så att personuppgifterna inte riskerar att komma i orätta händer eller bli manipulerade.
- Vi jobbar proaktivt med dataskydd.

Generell informationssäkerhetsmodell



Åhlfeldt RM., Spagnoletti P. & Sindre G. 2007. Improving the Information Security Model by using TFI. In: Venter H., Eloff M., Labuschagne L., Eloff J., von Solms R. (eds) New Approaches for Security, Privacy and Trust in Complex Environments. SEC 2007. IFIP International Federation for Information Processing, vol 232. Springer, Boston, MA)

Ansvarskyldighet



- Anmälan av personuppgiftsincidenter
- Föra ett register över personuppgiftsbehandling
- Dataskyddsombud.

Dataskyddsombudet (DSO)

Arbetsuppgifter (ett axplock)

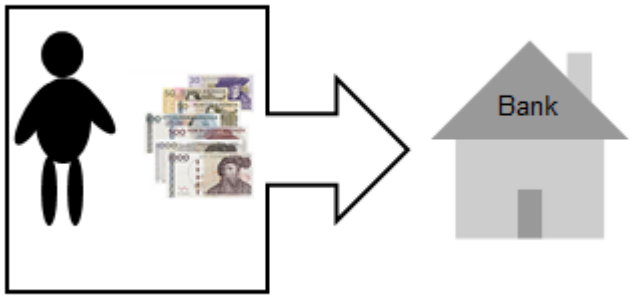
- **Självständigt agerande**
- **Tystnadsplikt**
- **Övervaka** den **interna efterlevnaden** av GDPR
- Den enskildes kontaktperson
- **Samrådande/ guidning inom KTH, beslut dock av verksamheten**
- **Samarbeta** med **Datainspektionen**.

KTH:s skyldighet (ett axplock)

- DSO på ett **korrekt sätt och i god tid deltar i alla frågor** som rör skyddet av personuppgifter.
- **Tillhandahålla resurser**
- Låta DSO få **tillgång till personuppgifter** och behandlingsförfaranden.
- **Upprätthålla DSO sakkunskap**.
- DSO **rapporterar direkt till det högsta förvaltningsnivå**.

Den enskildes rättigheter

Den enskildes rättigheter



- Veta var, vad och varför: information och tillgång till uppgifterna
- Rättelse och radering
- Dataportabilitet – överföring av personuppgifter till en annan organisation
- Begränsning av insamling och hantering
- Invändning mot insamling och hantering
- Motsätta sig automatiserad hantering

Vad ska man göra vid begäran (radering, registerutdrag etc.) och klagomål

När?
Begäran hanteras skyndsamt.

Hur?

- Inkommer via e-post: vidarebefordra skyndsamt till dataskydd@kth.se
- Telefon: hänvisa till dataskydd@kth.se
- Muntlig: hänvisa till KTH Entré i första hand.

Klagomål

Hänvisa till dataskyddsombudet

Personuppgiftsincident

Personuppgiftsincident

Säkerhetsincident som leder till:

1. Oavsiktlig eller olaglig förstöring
2. Förlust
3. Ändring till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats

Exempel

- Någon har kommit över ett lösenord som gör att den skulle kunna logga in i system som behandlar personuppgifter.
- E-post med känsligt eller extra skyddsvärda personuppgifter skickas till fel mottagare.
- En dator har fått skadlig kod som gör att obehörig skulle kunna komma åt personuppgifter.

Vad ska man göra vid personuppgiftsincident

När?

När ni vet/ misstänker/ ser en risk att det inträffat en incident. Hantera incident och ev. rapport till Datainspektionen inom 72 timmar.

Vad

Skicka e-post till abuse@kth.se**.** Ansvarig för incidenter på KTH: IT-säkerhetschef Patrik Lidehäll.

Frågor: kontakta dataskyddsombudet.

Vad händer vid olydnad?

Konsekvenser

Ersättning till den enskilde

- Den enskilde har rätt att begära få ersättning av KTH eller den som KTH har anlitat för att utföra en tjänst (sk. personuppgiftsbiträde).
- Skadan kan vara både konkret (t.ex. kostnader för ändring av information efter en personuppgiftsincident) eller abstrakt (t.ex. exempelvis intrång i upphovsrätten).
- 4% av årsomsättningen.
- Skada för KTH: minskad tillit, t.ex. studenter inte söker sig hit eller medel till forskningsprojekt.

Inskickade frågor

Många av våra partneruniversitet vill att vi skickar studenters betyg direkt till dem. Får vi göra det eller måste vi ha studentens godkännande?

Svar: Om detta är till för att uppfylla en förpliktelse i avtalet kan KTH skicka uppgifterna. Sättet för överföring dock måste övervägas (med avseende på bl.a. frekvens, uppgiftsmängden)

Vi har forskningsfinansiärer som ibland begär att få anställningsavtal på de som vi anställer på tjänster i deras projekt. Hur ska vi förhålla oss till detta? Ska vi skicka avtalen och i så fall på vilket sätt, är det till exempel bättre att skicka vanligt brev än att skicka med e-post? Frågan kan säkert användas för flera olika typer av situationer. Vad gäller med offentlighetsprincipen och GDPR kort och gott.

Svar: Offentlighetsprincipen går före GDPR. KTH måste göra dels en sekretessbedömning, dels lämplighetsbedömning avseende metod för utskick.

När vi skriver nya DPA:er, vilken instans ska göra detta (oftast är KTH part, inte skolan)? Finns det stöd för avvägningar gällande hantering av uppgifter eller utformning av dokument?

Svar: KTH får endast anlita ett biträde som ger tillräckliga garantier till att genomföra lämpliga tekniska och organisatoriska åtgärder. Syftet är att säkerställa kraven i GDPR uppfylls och den enskildes rättigheter. Detta kan regleras genom ett avtal, sk. personuppgiftsbiträdesavtal (*eng.* Data Protection Agreement (DPA).

Stöd för personuppgiftsbiträdesavtal ges av dataskyddsombudet. Numera även också GVS/IT involverad.

Avrundning

Veta mer?

KTH:s intranät:

https://intra.kth.se/anstallning/anstallningsvillkor/att-vara-statligt-an/behandling-av-person/dataskyddsforordningen-gdpr-1.800623

Hur länge sparas KTH:s handlingar ?

Detta framgår av KTH:s dokumenthanteringsplan:

https://intra.kth.se/administration/dokument/dhpl-1.353536

Kontaktuppgifter

Robin Roy
Dataskyddsombud

E-post: dataskyddsombud@kth.se Telefon: 08- 790 87 52

Övriga kontaktuppgifter: https://www.kth.se/profile/rroy