KTH ROYAL INSTITUTE
OF TECHNOLOGY

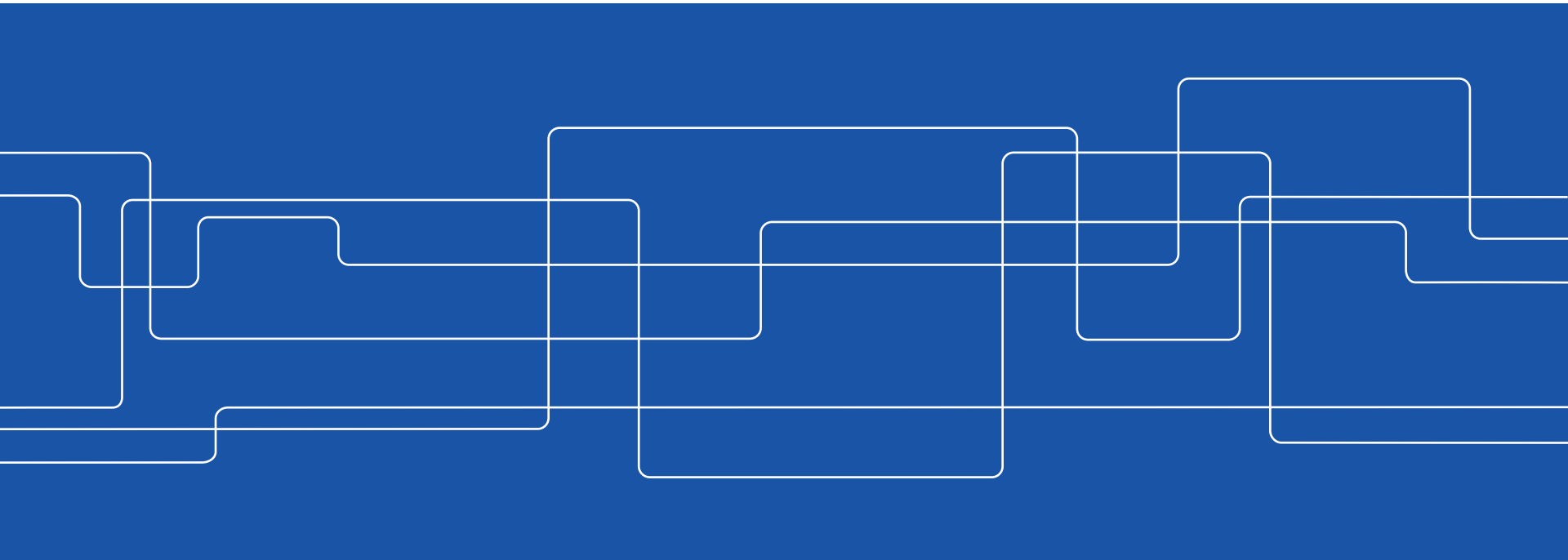
Dataskyddsförordningen (GDPR)

Robin Roy

Arkivarie/ utredare, personuppgiftsombud (fr.o.m. 25 maj: dataskyddsombud)

✉ rroy@kth.se

☎ 08-790 87 52



Upplägg

1) Den enskildes rättigheter
2) Principer för behandling av personuppgifter
3) Personuppgifter
4) Anonymisering och pseudonymisering
5) Uppförandekoder och certifiering
6) Frågestund

Enskildes rättigheter (inkl. barn)

- Personuppgifterna ska behandlats lagligt, korrekt och öppet sätt – beta var, vad och varför
- Rättelse och radering
- Dataportabilitet
- Begränsning av behandling
- Invändning mot behandling
- Motsätta sig automatiserad behandling

Kapitel III (Artikel 12-23)

Principer för behandling av personuppgifter

- 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
- Anmälan av personuppgiftsincidenter
- För ett register över personuppgiftsbehandlingar
- Säkert sätt – både system och organisation. Proaktivt arbete (konsekvensbedömningar, inbyggd dataskydd.

(Artikel 6)

Personuppgifter

Definition

- ”**Varje upplysning** som **avser** en **identifierad** eller **identifierbar fysisk person**”
- ”…**särskilt med hänvisning till en identifierare**…
- ”…**en eller flera faktorer** som är **specifika** för den **fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet**”

Identifiering

- **”**… **beakta alla hjälpmedel** som, **antingen av den personuppgiftsansvarige eller av en annan person**, **rimligen kan komma att användas** för att direkt eller indirekt identifiera den fysiska personen.”

- ”…**bör man beakta samtliga objektiva faktorer**, såsom kostnader och tidsåtgång för identifiering, med beaktande av såväl **tillgänglig teknik vid tidpunkten för behandlingen som den tekniska utvecklingen”**.

Om den registrerade inte eller inte längre är identifierbar: GDPR gäller inte.

(Artikel 4.1, skäl 26)

Exempel personuppgifter

Kungliga Tekniska Högskolan (SE) | https://www.kth.se/profile/gk

Go | Ixquick Search Engine | W3D3 | Tips | Förströelser | Fo-data | e-arkiv | Mögel | skadedjur | Språk | Ordböcker | General Data Protectio...

Logg

Gunnar Karlsson

PROFESSOR

Works for
DEPARTMENT OF NETWORK AND SYSTEMS ENGINEERING

Address
Osquldas väg 10, 5tr

E-mail
gk@ee.kth.se

Telephone
+46 8 790 42 57

DEPUTY HEAD OF DEPARTMENT

Researcher ID
ORCID ID

About me

I am professor of teletraffic systems since March 1998 and was head of the Department of Network and Systems Engineering at KTH until the end of 2017. I have previously worked for IBM Zurich Research Laboratory, and for the Swedish Institute of Computer Science (SICS).

Publications

Publication list

Portfolio

Literature for engineers and computer scientists

Public presentations

Debate

Ph.D. Thesis: Subband Coding for Packet Video

Pseudonymisering

… behandling av personuppgifter på ett sätt som innebär att personuppgifterna **inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används**, under förutsättning att dessa **kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person**…

Metoder (urval):

- Substitutionsmetod
- Scrambling
- Maskering

(Artikel 4.9)

Rättsfall på KTH

Bakgrund

NN har inkommit med en begäran om att erhålla en lista över samtliga registrerade studenter på kursen "Fasta tillståndets fysik(kurskod: IM2601) för perioden 2007 -2012. Listan ska innehålla resultat på delmomenten, samtliga tentaregistreringar för samtliga registrerade och resultaten på dessa. Vidare ska listan innehålla unika identifikatorer för varje student som klart identifierar studenten med tentamensregistreringar och antagningsår. Slagningar i datan ska kunna göras per (anonymiserad) individ. Begäran avser ett s.k. massuttag av uppgifter. NN vill i första hand få listan i digitalt format.

Kammarrättens dom: ansluter sig till KTH:s bedömning och avslår yrkandet

Beslut UF-2012/0588

Anonymisering

… information **som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar**.

(Skäl 26)

Exempel

Personuppgift

Pseudonymi-serad

Anonymiserad

Uppförandekoder och certifiering

- Tillsynsmyndighet/ kommissionen uppmuntra utarbetandet. Branschorganisationer/ föreningar – har en bättre kunskap om specifika behandlingar.
- Datainspektionen: bl.a. periodisk översyn (certifiering), offentliggörande kriterier för en ackreditering
- Visa att man följer GDPR, men man måste ändå följa GDPR
- Effektiverar regelefterlevnad, öppnare (lättare för den enskilde att bedöma skyddsnivån)

(Artikel 40-42, skäl 98-100)

Uppförandekoder

1. Visa personuppgiftsansvar
2. Ger tillräckliga garantier för dataskydd
3. Adekvat dataskydd
4. Konsekvensbedömning (risk- och sårbarhetsanalys)
5. Överföring till tredje land (personuppgiftsbiträdesavtal måste ingås)
6. Administrativa straffsanktioner – bedömningsgrund

Riksidrottsförbundets uppförandekod:
http://www.rf.se/globalassets/riksidrottsforbundet/dokument/personuppgifter-och-gdpr/uppforandekod_personuppgifter-och-gdpr.pdf?w=900&h=900

Certifiering – dataskydd

1. Visa personuppgiftsansvar
2. Ger tillräckliga garantier för dataskydd
3. Adekvat dataskydd
4. Konsekvensbedömning (risk- och sårbarhetsanalys)
5. Överföring till tredje land (personuppgiftsbiträdesavtal måste ingås)
6. Administrativa straffsanktioner – bedömningsgrund
7. Inbyggt dataskydd och dataskydd som standard

Datatilsynet. Vejledning om adfaedskodekser og certificeringsordninger. Januar 2018.

Uppförandekod – process

- Branschorganisation/förening tar fram (helst även dialog med de registrerande) utkast, förslag till ändring eller utökning

- Skickas till Datainspektionen. Datainspektionen bedömning om den uppfyller GDPR, yttra sig och ev. godkänna:

  - Nationell nivå: Datainspektionen registrerar och offentliggöra uppförandekoden

  - Gemensamt flera medlemsländer: Datainspektionen lämnar till Europeiska dataskyddsstyrelsen(alla EU:s tillsynsmyndigheter avseende GDPR), EU kommissionen godkänner. Styrelsen ska offentliggöra koderna på ett offentlig sätt.

(Artikel 40)

Certifiering

- Certifieringsmekanismer för dataskydd och sigill och märkningar för dataskydd
- Innehåll och räckvidd trolig skillnad mellan GDPR och ISO (Datatilsynet).
- Utförs av certifieringsorgan. Datainspektionens remissvar: nationella bestämmelser som förtydligar och specificerar förfarandet kring ackreditering

https://www.datainspektionen.se/Documents/remissvar/2017-09-08-kompletterande%20dataskyddslag.pdf

(Artikel 42-43)

Läget idag

- Enligt uppgift från Datainspektionen: Artikel 29-gruppen ska komma med vägledning för uppförandekoder/certifiering. Skulle ha blivit klar i februari 2018 (enlig uppgift från Datainspektionens hemsida)

- Artikel 29- gruppen skrivelse till ISO om att låta ISO 17065 (Bedömning av överensstämmelse - Krav på organ som certifierar produkter, processer och tjänster) bli allmänt tillgänglig

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=625011

Frågor ?