DATASKYDDSOMBUDETS ÅRSRAPPORT FÖR NEAB OCH NEFAB, VERKSAMHETSÅRET 2023

Jakob Söderbaum, DSO

2024-11-26

Om mig

Min bakgrund:

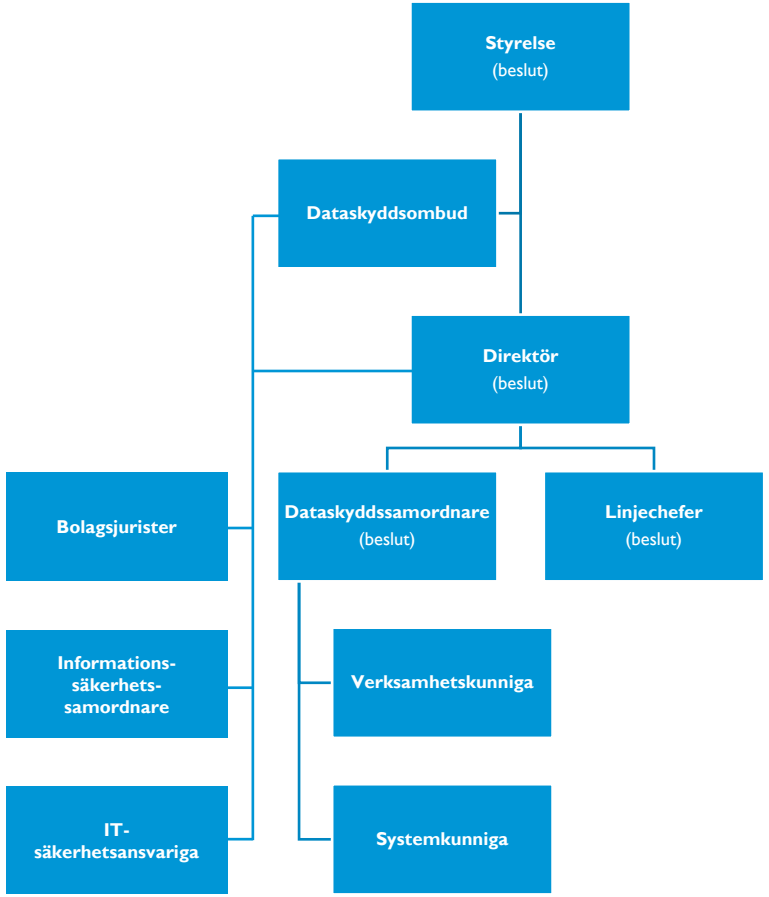
- Jur. kand. och fil. kand. i företagsekonomi
- 8 år som managementkonsult inom verksamhetsutveckling
- 6,5 år som GDPR-specialist, inkl. 4 år som DSO
- Arbetat för:
  - multinationella företag
  - mellanstora företag
  - startups
  - fackförbund
  - myndigheter
  - kommuner

LinkedIn: https://www.linkedin.com/in/jakobsoderbaum2/

E-post: jakob.soderbaum@nacka.se

NACKA KOMMUN

DSO och dataskyddsorganisationen i bolag



Dataskyddsorganisationen i en kommunal myndighet, givet att det finns en eller flera utsedda Dataskyddssamordnare under var och en direktör.

Dataskyddsombudet är tillförordnat av nämnden att bevaka dess intressen enligt dataskyddslagstiftningen, Direktören ansvarar inför nämnden för de prioriteringar som görs i verksamheten, Dataskyddssamordnaren driver och ansvarar för GDPR-utvecklingsarbetet, med stöd av Dataskyddsombudet, verksamhetskunniga och systemkunniga.

Dataskyddsombudet är inte beslutsmässigt, utan beslutsmässigheten följer nämndens delegationsordning.

Dataskyddsombudet rapporterar årligen till nämnden och delårsvis till direktören.

NACKA KOMMUN

DSO:s arbete i Nacka (ställning och uppdrag enligt GDPR artiklar 38 och 39)

Kontroll & granskning

- Proaktivt: Systematiskt (t.ex. område eller befintliga styrdokument)
- Proaktivt: Riktat (t.ex. område eller specifika rutiner)
- Reaktivt: Baserat på händelser eller önskemål (inkl. specifika rutiner)

Rådgivning

- Bereder nya förslag på styrdokument och stöddokument
- Besvarar specifika frågor från verksamheterna
- PM med behovsstyrda juridiska analyser

Informering & utbildning

- Kvalitetssäkrande av informationstexter
- Utbildning av DSS:er
- Verksamhetsspecifika utbildningar
- Juridiska perspektiv på svaren på alla frågor

Rapportering

- Nuläge till nämnder, styrelser och direktörer (regelbundet)
- Omvärldsbevakning till direktörer och DSS:er (spontant)

Övrigt (utöver DSO:s ordinarie arbetsuppgifter)

- Stöttar hantering av personuppgiftsincidenter
- Stöttar ifyllandet av personuppgiftsbiträdesavtal
- Stöttar kravställning i upphandlingar
- Hanterar frågor från allmänheten

NACKA KOMMUN

Personuppgifter är en mycket värdefull resurs

"THE WORLD'S MOST VALUABLE RESOURCE IS NO LONGER OIL, BUT DATA"

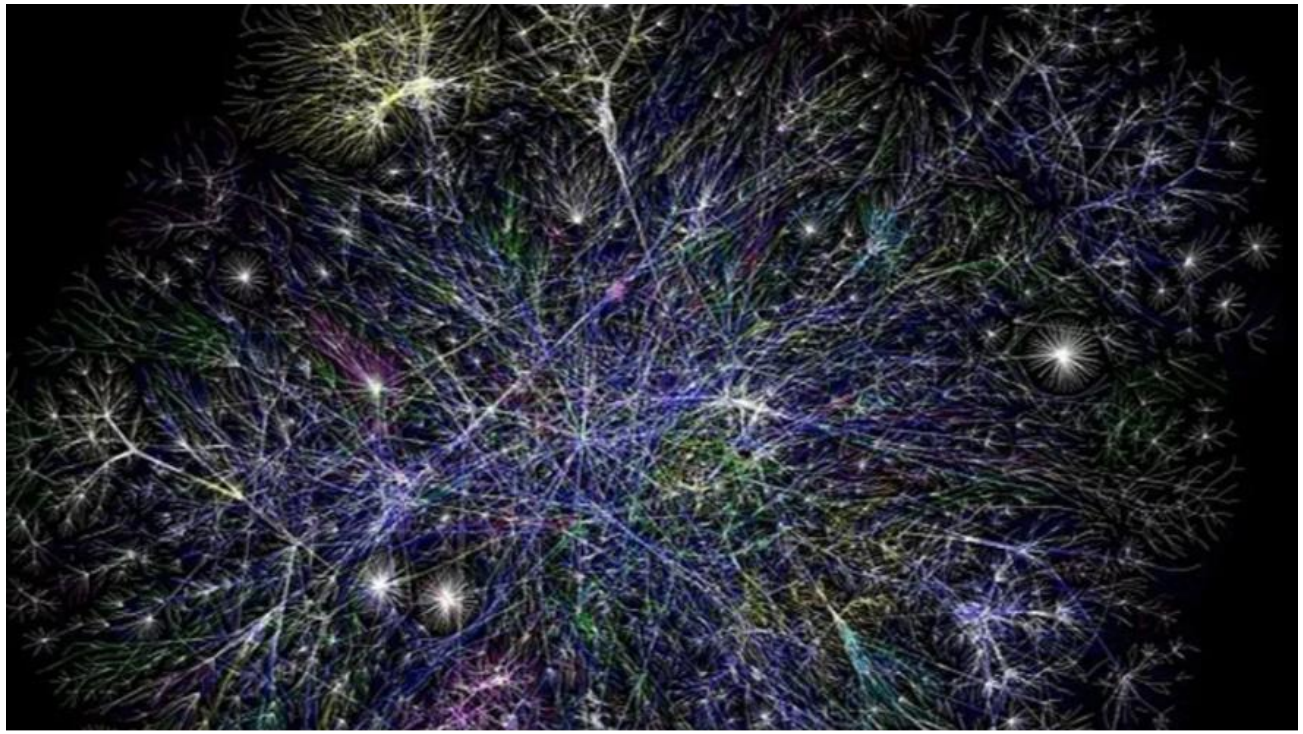
The Economist, 6 maj 2017. Illustration David Parkins.

NACKA KOMMUN

Personuppgifter är idag global de facto-valuta

Men det är inte bara risken för intrång och behovet av IT-säkerhet som är stort idag.

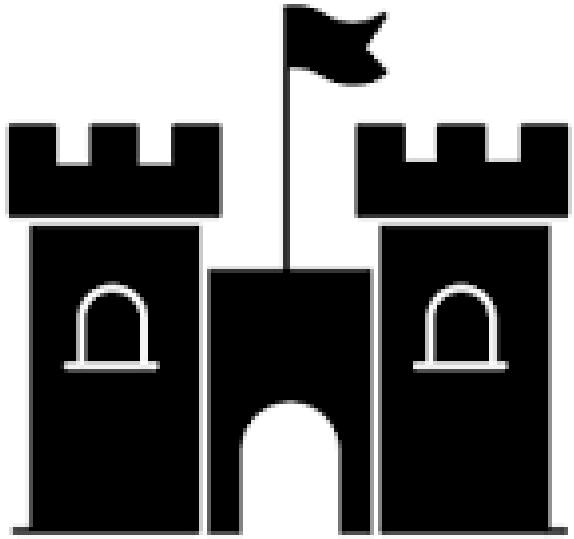
De flesta företag som säljer IT-system som inte är dyra per användare har affärsmodeller där de tankar ner mängder av Dina personuppgifter och säljer vidare till alltifrån andra företag till organiserade kriminella och stater som letar efter politiska dissidenter som flytt.

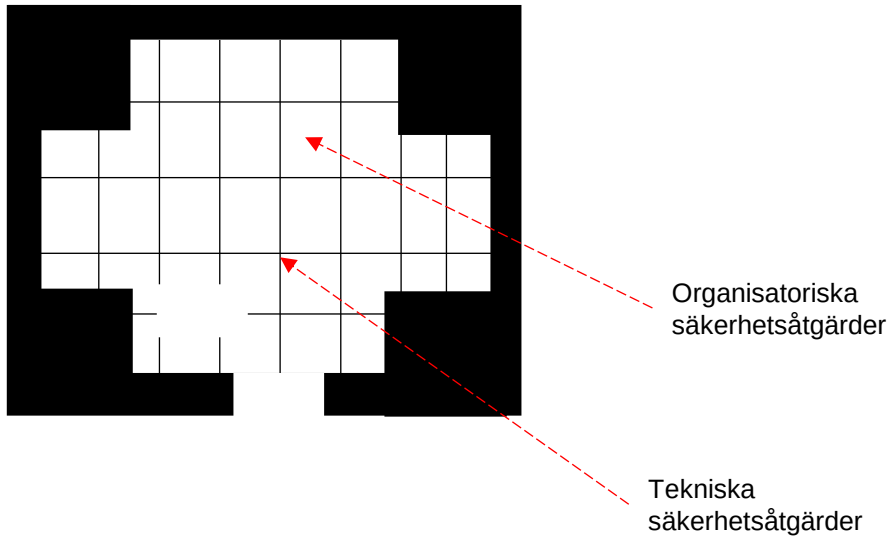


Internet övervakar oss alla/ Foto: WikiCommons Public Domain

NACKA KOMMUN

GDPR, Informationssäkerhet, IT-säkerhet





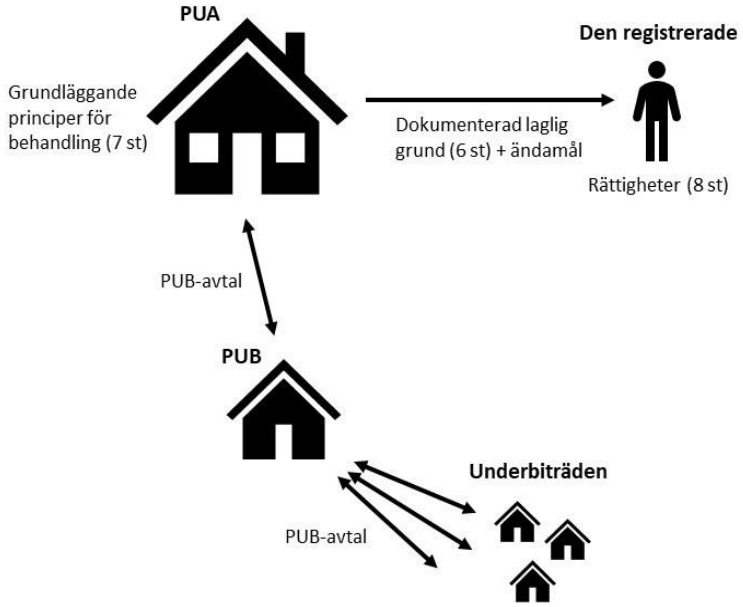
IT-säkerheten är som muren runt IT-miljön. Informationssäkerhet och dataskydd är väggarna mellan rummen. IT-miljön består av system (rum) och integrationer (dörrar). Kommer en inkräktare förbi muren så ska det inte vara lätt att bränna ner hela IT-miljön inifrån, och det ska helst vara svårt att ta sig från ett rum till ett annat – detta är vad GDPR handlar om. Dataskyddet består av tekniska säkerhetsåtgärder (väggar) och organisatoriska (väktarna i dörröppningarna) mellan rummen – specifikt för personuppgifter, medan Informationssäkerhet och IT-säkerhet även rör alla andra datamängder.

NACKA KOMMUN

”GDPR-rustningens” beståndsdelar

Grundstruktur för ansvarstagande enligt GDPR (”rustningen”):

1. Behandlingsregister **– artikel 30**
2. Processbeskrivningar och relevant organisation för tillgodoseendet av de registrerades rättigheter (främst Registerutdrag, Radering, Rättelse) **– artiklar 15, 16, 17**
3. PUB-avtalsmall inklusive instruktionsbilaga **– kapitel IV**
4. Interna riktlinjer för hur alla delar av verksamheten ska efterleva de grundläggande principerna och GDPR i det huvudsakliga **– artikel 5**
5. Etablera grundläggande tekniska förutsättningar (främst behörighetsstyrning, nätverksskydd, och möjlighet att kunna upptäcka dataintrång) **– skäl 39, 49, 83, artiklar 4.12, 5.1 f, 24, 25, 32**
6. Relevant ärendehantering av personuppgiftsincidenter **– artiklar 4.12, 33, 34**



NACKA KOMMUN

Nuläge: NEAB

a. Del i grundl. strukturen	b. Hexagon i *Bild 2*		c. Aktivitet
	Alla system är kartlagda		Inventering av alla leverantörer av system och tjänster inom enheten, vilka det har gjorts risk- och sårbarhetsanalyser på, och om enheten har alla PUB-avtal man behöver
	Personuppgiftsflödet är kartlagt		Huvudsaklig kartläggning av hur personuppgifter kommer in och behandlas inom enheten har gjorts
1	Grunddokument är kvalitetssäkrade		Kvalitetssäkrat behandlingsregister för nämnden
	Dataskyddsansvarig(a) finns		Formellt utsedd(a) dataskyddssamordnare inom enheten
	Utbildning specifika roller		Dataskyddssamordnare har relevant GDPR-kunskap och verktyg
6	Dataskyddsansvarig(a) finns		Incidenthanteringsorganisation etablerad i den egna enheten
6	GDPR-processer implementerade		Incidenthanteringsprocess etablerad i enhetens incidenthanteringsorganisation
2	GDPR-processer implementerade		Registerutdragsprocess etablerad i enheten
2	GDPR-processer implementerade		Processer för radering och rättelse etablerade i enheten
1	Grunddokument finns		Val av leverantör för systemstöd till behandlingsregister
6	GDPR-processer implementerade		Val av leverantör för systemstöd till incidenthantering
	Generell utbildning		Val av leverantör för GDPR-utbildning
	Generell utbildning		Huvudsaklig GDPR-utbildning för kommuner genomförd för alla enhetens medarbetare
4	Grunddokument finns		Gap-analys ifråga om vad som finns och vad som ska finnas med i enhetens GDPR-rutiner, -regler och -anvisningar
4	Grunddokument finns		Dokumenterade rutiner, regler och anvisningar rörande det huvudsakliga ifråga om hur enhetens olika verksamheter får/bör behandla personuppgifter har upprättats.
	Utbildning specifika roller		Verksamhetsspecifik GDPR-utbildning genomförd för flertalet av enhetens medarbetare
	Systematisk gallring		En huvudsaklig, systematisk GDPR-inriktad gallring har ägt rum i enheten inför eller efter 25 maj 2018
	Grunddokument finns		Alla personuppgiftsbiträdesavtal som enheten behöver ha är på plats.
4	Grunddokument är kvalitetssäkrade		Alla mallar och instruktioner för Samtycke som enheten använder är kvalitetssäkrade.
5	Relevant behörighetsstyrning		Inventering av alla behörigheter och licenser i alla system samt specificerande av vad som behöver förbättras
	Relevant behörighetsstyrning		Felaktiga behörigheter har gallrats och GDPR-säkrade rutiner för behörighetsstyrning är dokumenterade och etablerade
	Grunddokument är kvalitetssäkrade		Alla personuppgiftsbiträdesavtal som enheten behöver ha är kvalitetssäkrade
4	Systematisk gallring		Relevanta rutiner för gallring finns beskrivna i enhetens informationshanteringsplan och efterlevs
4	Grunddokument är kvalitetssäkrade		GDPR-relaterade rutiner, regler och anvisningar har kvalitetssäkrats
	All PU-behandling är dokumenterad		Alla processer och rutiner där personuppgifter behandlas inom enheten har GDPR-anpassats
	Medarbetarna har huvudsaklig förståelse		Enkät för uppföljning av medarbetarnas befintliga GDPR-kunskaper har genomförts, och visar på tillräckligt god förståelse.

NACKA KOMMUN

Nuläge: NEFAB

a. Del i grundl. strukturen	b. Hexagon i *Bild 2*		c. Aktivitet
	Alla system är kartlagda		Inventering av alla leverantörer av system och tjänster inom enheten, vilka det har gjorts risk- och sårbarhetsanalyser på, och om enheten har alla PUB-avtal man behöver
	Personuppgiftsflödet är kartlagt		Huvudsaklig kartläggning av hur personuppgifter kommer in och behandlas inom enheten har gjorts
1	Grunddokument är kvalitetssäkrade		Kvalitetssäkrat behandlingsregister för nämnden
	Dataskyddsansvarig(a) finns		Formellt utsedd(a) dataskyddssamordnare inom enheten
	Utbildning specifika roller		Dataskyddssamordnare har relevant GDPR-kunskap och verktyg
6	Dataskyddsansvarig(a) finns		Incidenthanteringsorganisation etablerad i den egna enheten
6	GDPR-processer implementerade		Incidenthanteringsprocess etablerad i enhetens incidenthanteringsorganisation
2	GDPR-processer implementerade		Registerutdragsprocess etablerad i enheten
2	GDPR-processer implementerade		Processer för radering och rättelse etablerade i enheten
1	Grunddokument finns		Val av leverantör för systemstöd till behandlingsregister
6	GDPR-processer implementerade		Val av leverantör för systemstöd till incidenthantering
	Generell utbildning		Val av leverantör för GDPR-utbildning
	Generell utbildning		Huvudsaklig GDPR-utbildning för kommuner genomförd för alla enhetens medarbetare
4	Grunddokument finns		Gap-analys ifråga om vad som finns och vad som ska finnas med i enhetens GDPR-rutiner, -regler och -anvisningar
4	Grunddokument finns		Dokumenterade rutiner, regler och anvisningar rörande det huvudsakliga ifråga om hur enhetens olika verksamheter får/bör behandla personuppgifter har upprättats.
	Utbildning specifika roller		Verksamhetsspecifik GDPR-utbildning genomförd för flertalet av enhetens medarbetare
	Systematisk gallring		En huvudsaklig, systematisk GDPR-inriktad gallring har ägt rum i enheten inför eller efter 25 maj 2018
	Grunddokument finns		Alla personuppgiftsbiträdesavtal som enheten behöver ha är på plats.
4	Grunddokument är kvalitetssäkrade		Alla mallar och instruktioner för Samtycke som enheten använder är kvalitetssäkrade.
5	Relevant behörighetsstyrning		Inventering av alla behörigheter och licenser i alla system samt specificerande av vad som behöver förbättras
	Relevant behörighetsstyrning		Felaktiga behörigheter har gallrats och GDPR-säkrade rutiner för behörighetsstyrning är dokumenterade och etablerade
	Grunddokument är kvalitetssäkrade		Alla personuppgiftsbiträdesavtal som enheten behöver ha är kvalitetssäkrade
4	Systematisk gallring		Relevanta rutiner för gallring finns beskrivna i enhetens informationshanteringsplan och efterlevs
4	Grunddokument är kvalitetssäkrade		GDPR-relaterade rutiner, regler och anvisningar har kvalitetssäkrats
	All PU-behandling är dokumenterad		Alla processer och rutiner där personuppgifter behandlas inom enheten har GDPR-anpassats
	Medarbetarna har huvudsaklig förståelse		Enkät för uppföljning av medarbetarnas befintliga GDPR-kunskaper har genomförts, och visar på tillräckligt god förståelse.

NACKA KOMMUN

Huvudsaklig statistik

Personuppgiftsincidenter

Ansvarig nämnd	Upp-täckta 2023	IMY-anmälda 2023
NEAB	10	0
NEFAB	0	0
Totalt i kommunen:	82	5

Registrerades utövande av sina rättigheter

Nämnd	Begäran om Register-utdrag	Begäran om Radering	Begäran om Rättelse
NEAB	0	0	0
NEFAB	0	0	0
Totalt i kommunen:	35	7	4

NACKA KOMMUN

Rekommenderade och pågående aktiviteter

DSO samarbetar under 2024 med alla nämnders DSS:er och andra sakkunniga i kommunen om att kvalitetssäkra de grundläggande förutsättningarna för GDPR-efterlevnad:

- ✓ Behandlingsregister
- ✓ Process för personuppgiftsincidenthantering
- ✓ Process för registerutdrag
- ✓ Riktlinjer och mallar för personuppgiftsbiträdesavtal
- ✓ Arbetsplaner för alla dataskyddssamordnare
- ✓ GDPR-handbok för alla medarbetare
- ✓ Delegationsordningarna

Jfr ”rustningen”

Tidpunkt för årsrapporterna till nämnderna 2024 föreslås tidigareläggas till februari-mars?

NACKA KOMMUN

NACKA
KOMMUN