Personvernhåndteringen i ACOS WebSak

16.oktober 2018

Ivar Wessel Thomassen
Direktør fag og innovasjon


GDPR

Hovedformålet med GDPR

Hva er hovedformålet med GDPR?

Å sikre vern av personer i forbindelse med behandling av personopplysninger

Hva er en personopplysning?

Personopplysninger er alle opplysninger som kan knyttes til deg som enkeltperson

Acos

Hva er en personopplysning?

Personopplysning er en opplysning eller vurdering som kan knyttes til oss som enkeltpersoner.

For eksempel:

- Navn, adresse, telefonnummer og e-postadresse
- IP-adresse, bilnummer og bilder
- **Fingeravtrykk, irismønster, hodeform og fødselsnummer** (både fødselsdato og personnummer)
- Adferdsmønster etc.

Acos

Sensitive personopplysninger

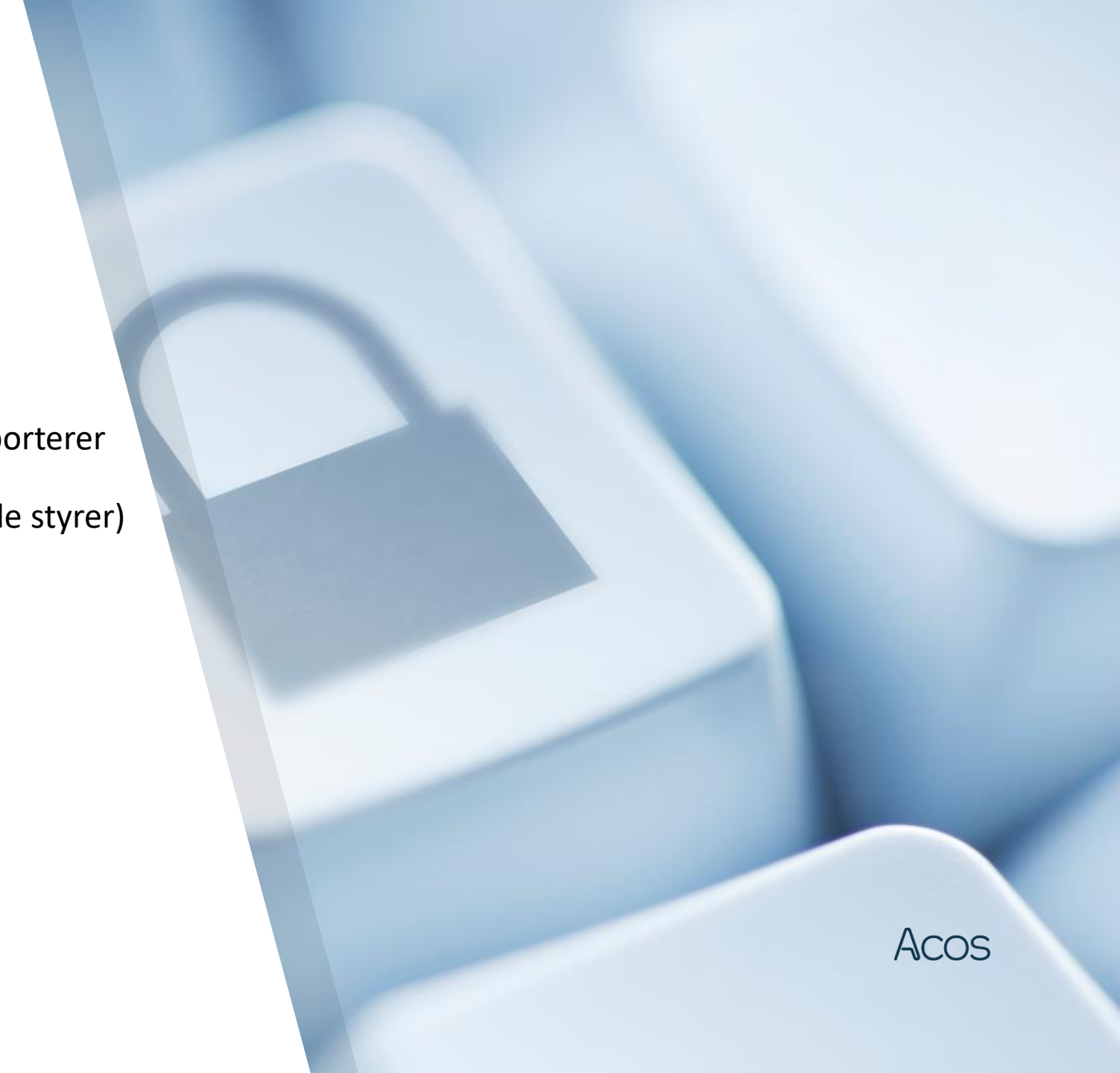
Opplysninger som krever spesiell varsomhet:

- Rasemessig eller etnisk bakgrunn
- Politisk, religiøs eller filosofisk oppfatning
- Rulleblad (mistenkt, siktet, tiltalt eller dømt)
- Helsemessige forhold
- Seksuelle forhold
- Medlemsskap i fagforeninger
- **Genetiske og biometriske data (nytt i GDPR)**

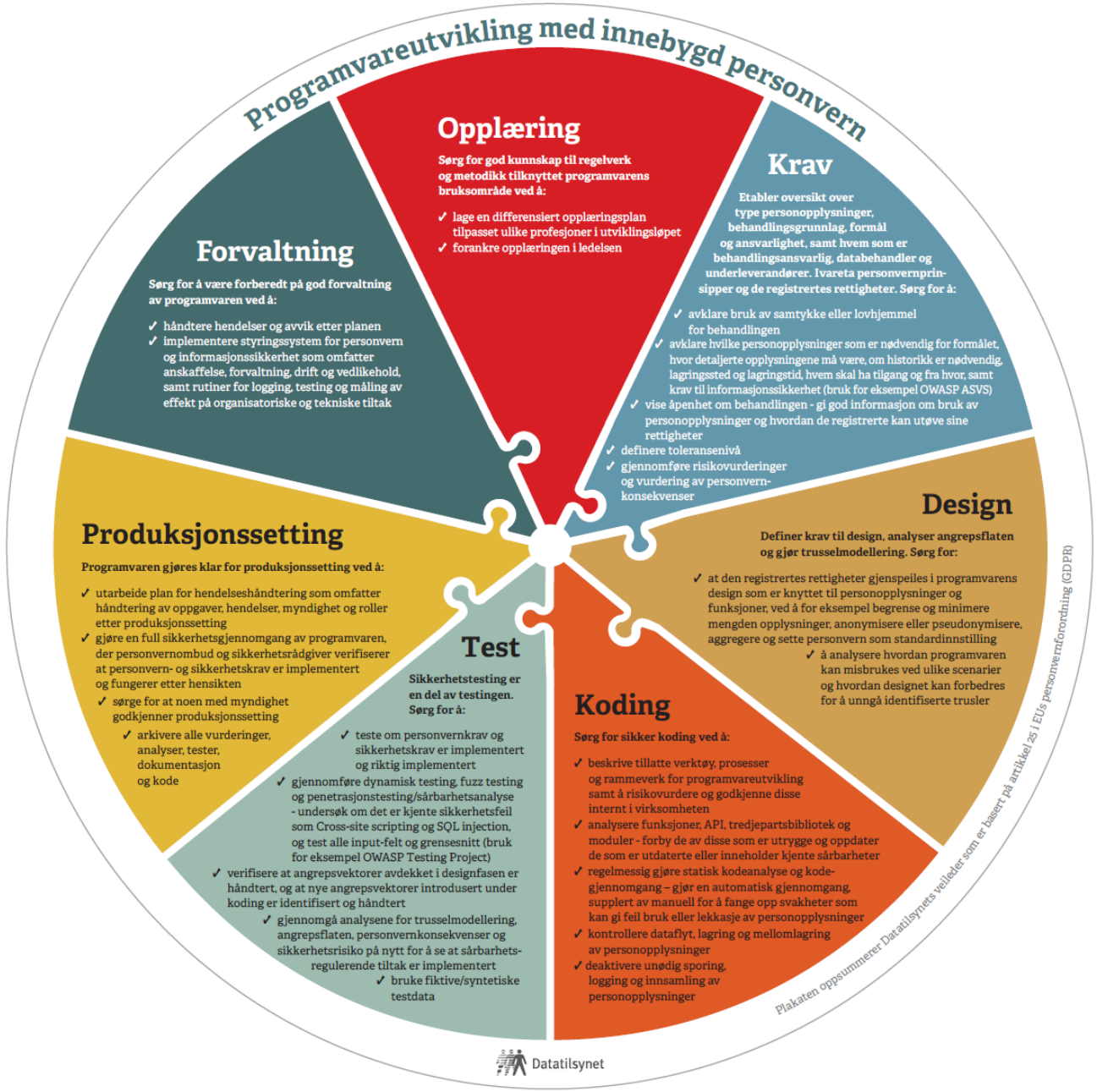
Acos

Databehandleravtale (DBA)
og statens standard 2018

- DBA med alle kunder vi drifter eller teknisk supporterer
- DBA pga support- og vedlikeholdsansvaret (kunde styrer)
- SSA-V (2018) har egne reguleringer om personopplysninger i kap 9.



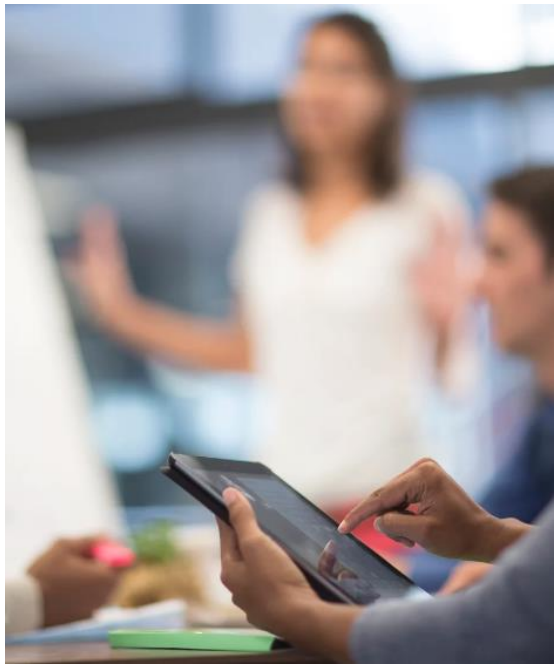
Acos


Programvareutvikling med innebygd personvern
Opplæring
Sørg for god kunnskap til regelverk og metodikk tilknyttet programvarens bruksområde ved å:
✓ lage en differensiert opplæringsplan tilpasset ulike profesjoner i utviklingsløpet
✓ forankre opplæringen i ledelsen
Krav
Etabler oversikt over type personopplysninger, behandlingsgrunnlag, formål og ansvarlighet, samt hvem som er behandlingsansvarlig, databehandler og underleverandører. Ivareta personvernprinsipper og de registrertes rettigheter. Sørg for å:
✓ avklare bruk av samtykke eller lovhjemmel for behandlingen
✓ avklare hvilke personopplysninger som er nødvendig for formålet, hvor detaljerte opplysningene må være, om historikk er nødvendig, lagringssted og lagringstid, hvem skal ha tilgang og fra hvor, samt krav til informasjonssikkerhet (bruk for eksempel OWASP ASVS)
✓ vise åpenhet om behandlingen - gi god informasjon om bruk av personopplysninger og hvordan de registrerte kan utøve sine rettigheter
✓ definere toleransenivå
✓ gjennomføre risikovurderinger og vurdering av personvernkonsekvenser
Design
Definer krav til design, analyser angrepsflaten og gjør trusselmodellering. Sørg for:
✓ at den registrertes rettigheter gjenspeiles i programvarens design som er knyttet til personopplysninger og funksjoner, ved å for eksempel begrense og minimere mengden opplysninger, anonymisere eller pseudonymisere, aggregere og sette personvern som standardinnstilling
✓ å analysere hvordan programvaren kan misbrukes ved ulike scenarier og hvordan designet kan forbedres for å unngå identifiserte trusler
Koding
Sørg for sikker koding ved å:
✓ beskrive tillatte verktøy, prosesser og rammeverk for programvareutvikling samt å risikovurdere og godkjenne disse internt i virksomheten
✓ analysere funksjoner, API, tredjepartsbibliotek og moduler - forby de av disse som er utrygge og oppdater de som er utdaterte eller inneholder kjente sårbarheter
✓ regelmessig gjøre statisk kodeanalyse og kodegjennomgang – gjør en automatisk gjennomgang, supplert av manuell for å fange opp svakheter som kan gi feil bruk eller lekkasje av personopplysninger
✓ kontrollere dataflyt, lagring og mellomlagring av personopplysninger
✓ deaktivere unødig sporing, logging og innsamling av personopplysninger
Test
Sikkerhetstesting er en del av testingen. Sørg for å:
✓ teste om personvernkrav og sikkerhetskrav er implementert og riktig implementert
✓ gjennomføre dynamisk testing, fuzz testing og penetrasjonstesting/sårbarhetsanalyse - undersøk om det er kjente sikkerhetsfeil som Cross-site scripting og SQL injection, og test alle input-felt og grensesnitt (bruk for eksempel OWASP Testing Project)
✓ verifisere at angrepsvektorer avdekket i designfasen er håndtert, og at nye angrepsvektorer introdusert under koding er identifisert og håndtert
✓ gjennomgå analysene for trusselmodellering, angrepsflaten, personvernkonsekvenser og sikkerhetsrisiko på nytt for å se at sårbarhetsregulerende tiltak er implementert
✓ bruke fiktive/syntetiske testdata
Produksjonssetting
Programvaren gjøres klar for produksjonssetting ved å:
✓ utarbeide plan for hendelseshåndtering som omfatter håndtering av oppgaver, hendelser, myndighet og roller etter produksjonssetting
✓ gjøre en full sikkerhetsgjennomgang av programvaren, der personvernombud og sikkerhetsrådgiver verifiserer at personvern- og sikkerhetskrav er implementert og fungerer etter hensikten
✓ sørge for at noen med myndighet godkjenner produksjonssetting
✓ arkivere alle vurderinger, analyser, tester, dokumentasjon og kode
Forvaltning
Sørg for å være forberedt på god forvaltning av programvaren ved å:
✓ håndtere hendelser og avvik etter planen
✓ implementere styringssystem for personvern og informasjonssikkerhet som omfatter anskaffelse, forvaltning, drift og vedlikehold, samt rutiner for logging, testing og måling av effekt på organisatoriske og tekniske tiltak
Plakaten oppsummerer Datatilsynets veileder som er basert på artikkel 25 i EUs personvernforordning (GDPR)
Datatilsynet

Acos

Plikt til å varsle ved personvernbrudd (i ACOS)

- **Personvernbrudd** skal varsles umiddelbart.
- Fyll ut **avviksskjema**:
  - ✓ Beskrivelse av avviket og hovedårsak
  - ✓ Tidsrom avviket ble oppdaget
  - ✓ Antall berørte personer etc.
- Behandles av **leder**
- Datatilsynet skal ha varsel innen 72 timer etter at avvik er oppdaget



ACOS KVALITET GJENNOM ENGASJEMENT

Du er innlogget som **Ivar Thomassen**
Mine Skjema

Logg ut

GENERELT

BESKRIVELSE AV AVVIKET

PERSONOPPLYSNINGER OG RELASJON

KONSEKVENSER FOR DE BERØRTE

KONSEKVENSER FOR ACOS

TILTAK

OPPSUMMERING

Avvik ved uautorisert utlevering av personopplysninger

HJELP

Hovedårsak

Gjelder dette ACOS sine data eller kundens data? *

- (•) ACOS
- ( ) Kunde

Hvem forårsaket dette? *

- ( ) Brudd utført av ACOS
- ( ) Brudd utført av kunde (beskriv hvilken kunde og kontaktperson)
- (•) Brudd utført av annen ekstern (beskriv hvilket firma og kontaktperson)

Organisasjon * Konsulenter & Fjas AS

Person * Guri Malla

Hvilket brudd skjedde?

- (•) Brudd på generell taushetsplikt
- ( ) Brudd på gjeldende rutiner eller sikkerhetsbestemmelser
- ( ) Elektroniske angrep
- ( ) Annet, beskriv

Dokumenter ca. tidsrom avviket har oppstått i

Fra: dato * og klokkeslett * 13.10.2018 01:30

Til: dato og klokkeslett 13.10.2018 02:15

Når ble avviket oppdaget?

Dato * og klokkeslett * 14.10.2018 11:30

Antall berørte personer * 11

Beskriv hva som har skjedd *

På etterfesten gikk det galt når Guri logget seg på ePost serveren vår og kompromitterte ulest ePost.

Beskriv hvordan avviket oppstod *

Via egen iPad.

Utfylling og bruk

Klikk på hjelpesymbolene for informasjon om utfylling.

* Betyr obligatorisk for utfylling

Etter 20 minutt uten aktivitet kan utfylling av skjema gå tapt.

Klikk på **Hjelp** øverst til høyre for generell hjelp om skjema.

FORRIGE ← LAGRE ✓ AVBRYT ✕ NESTE →

Personvernerklæring | Informasjonskapsler

ACOS KVALITET GJENNOM ENGASJEMENT

Du er innlogget som **Ivar Thomassen**
Mine Skjema

Logg ut

GENERELT

BESKRIVELSE AV AVVIKET

PERSONOPPLYSNINGER OG RELASJON

KONSEKVENSER FOR DE BERØRTE

KONSEKVENSER FOR ACOS

TILTAK

OPPSUMMERING

Avvik ved uautorisert utlevering av personopplysninger

HJELP

Skjemaet er klart for innsending.
Se gjennom og fullfør skjema nederst på siden

Generelt

Fornavn: Ivar Wessel
Etternavn: Thomassen
Dato: 15.10.2018

Beskrivelse av avviket

Hovedårsak

Gjelder dette ACOS sine data eller kundens data?
☒ ACOS
☐ Kunde

Hvem forårsaket dette?
☐ Brudd utført av ACOS
☐ Brudd utført av kunde (beskriv hvilken kunde og kontaktperson)
☒ Brudd utført av annen ekstern (beskriv hvilket firma og kontaktperson)

Organisasjon: Konsulenter & Fjas AS

Person: Guri Malla

Hvilket brudd skjedde?
☒ Brudd på generell taushetsplikt
☐ Brudd på gjeldende rutiner eller sikkerhetsbestemmelser
☐ Elektroniske angrep
☐ Annet, beskriv

Fra: dato	klokkeslett
13.10.2018	01:30
Til: dato	klokkeslett
13.10.2018	02:15
Dato	klokkeslett
14.10.2018	11:30

Antall berørte personer: 11

Beskriv hva som har skjedd: På etterfesten gikk det galt når Guri logget seg på ePost serveren vår og kompromitterte ulest ePost.

Beskriv hvordan avviket oppstod: Via egen iPad.

Personopplysninger og relasjon

Gruppe

Beskriv hva slags type personopplysninger som ble berørt: ePost med bank kvitteringer, eFaktura opplysninger og mapper med øvrig lagret ePost.

Hvilken relasjon har virksomheten til de berørte personene?
☒ Ansatte i ACOS
☐ Søkere på stilling
☐ Kundens ansatte
☐ Kundens innbyggere
☒ Annet

Konkrete endringer i ACOS WebSak?

«Standard» krav i 2018:

«Tilbyder skal redegjøre for hvordan kravene i den nye personvernforordningen (GDPR 2018) oppfylles»

Slapp av, Oslo veit skikkelig lite om deg

Jeg prøvde å finne ut hva Oslo kommune veit om meg. Jeg ble litt skremt. Men av feil grunn.

OSLO

Før sommeren sendte jeg en liten epost til byen min.

«Hei Oslo kommune», skreiv jeg. «Jeg ønsker herved å be om alle personopplysninger kommunen har registrert om meg. Håper det lar seg gjøre.»

Det var bare et innfall. Rett etter lønsj, på en onsdag hvor jeg uansett ikke hadde noe spesielt å gjøre.

Vi har nemlig fått en ny lov, GDPR. Den sier at vi alle har rett på å vite hva forskjellige selskaper veit om oss.

Egentlig tenkte de nok mest på Facebook og Google og Twitter og sånt, da de lagde den loven. IT-selskapene som har så mye info om oss alle at vi egentlig burde ligge våkne hver natt og være skremt.

Men det er jo ikke bare bedrifter som har informasjon om oss. Hva har egentlig kommunen? Byen jeg er født i, har vokst opp i, gått på skole i, blitt forelska i og arrestert i? Byen jeg har sparka fotball i og jobba i, sånn omtrent alltid?

Hva veit de om meg? Det ville jeg finne ut. Og det var veldig lett. For meg, i hvert fall.

Les også: *Navn og logo-tabbe til 15 millioner*

«Heisann, er det Borgersrud?»

«Ja, hvem er det som ringer?»

«Det er arkivavdelingen i bydelen her, er du den Borgersrud som har bedt om innsyn i hele kommunen?»

I ukene etter at jeg hadde sendt eposten til kommunen, fikk jeg stadig nye telefoner, fra folk ansatt stadig dypere i byråkratiet og i bydelene i Oslo kommune. Selveste Byrådslederens Kontor hadde nemlig videresendt mailen min til alle etater, med streng beskjed om å besvare den så godt som mulig.

«Den enkelte virksomhet bes om å besvare henvendelsen direkte, uten kopi til overordnet byrådsavdeling», skrev Raymond Johansens kontor. Til alle bydeler, etater og kommunale foretak. Underforstått: Ikke bland Raymond oppi dette, bare fiks det!

Og dermed var stormen i gang.

Innsyn

- Innsyn = «hva vet dere om meg»-forespørsel
  - Rapport i ACOS Rapportmodul
  - Sakstittel og sakID der person er part eller i klassifikasjon
  - JP tittel og JPID der person er avsender eller mottaker

→Ikke nødvendig med systemendring, men en ny rapport


Acos

Råd ved behov for Sletting

- Vurdere om det er lovverk som krever oppbevaring
- «Faglover» går foran GDPR i mange tilfeller
  - Utilgjengeliggjøring (Begrense tilgang)
- Endelig sletting :
  - Utviklet egen kassasjonsmodul i samarbeid med kunder
  - Oppbevaringstider kan ha ulike vedtak og rutiner 1, 3, 5 og 10 år
  - Kan sletter data automatisk, men kvalitets- og sikkerhetsrutiner må etableres
- Tilleggsdata
  - Sletting av delmengder og delstrukturer av tilleggsdata erkjennes som en fremtidig utfordring

Acos

Logging

- ACOS har oversikt alle steder hvor personinformasjon logges
- Det er utviklet egen kassasjonsmodul for fysisk sletting av metadata og dokumenter som ivaretar krav til logging
- Script vil kunne effektivt benyttes i spesielle tilfeller når komplekse behov i arkivstruktur skal ivaretas

Acos

Testdata

- GDPR medfører at man ikke kan benytte kopi av driftsdata til testing direkte.
- ACOS har anonymiseringsscript som
  - Endrer navn på parter og korrespondanseparter
  - Genererer nye titler på sak, journalpost og dokumenter
  - Endrer navn og kode på brukere av systemet
  - Sletter logger
  - Sletter dokumentfiler
  - Sletter sendte oppgaver
  - Sletter merknader

Acos


HJEM
OM GDPR
GDPR OG ACOS PRODUKTER
VERKTØY
FAQ
NYTTIGE LENKER
HVA KAN VI HJELPE MED?
Viktig informasjon om
NY PERSONVERNFORORDNING (GDPR)
LES MER
Les mer på: https://www.gdpr.acos.no/
Acos

Takk for meg - men først kort demo ☺

Ivar Wessel Thomassen
Direktør fag og innovasjon

Acos