Hva er GDPR?

- GDPR (General Data Protection Regulation) er EUs forordning for personvern (vedtatt i 2016), og blir gjeldende norsk lov i 2018
- Innebærer et nytt sett av regler for personvern i Norge
- Det nye regelverket gir virksomheter nye plikter og enkeltpersoner nye rettigheter
- Eneste kravet som forsvinner er ordningen med registrering/konsesjon for personregistre
- GDPR er langt mer omfattende enn tidligere lover og regelverk, med potensielt høye bøter for brudd

Få kontroll på personsensitive data

Viktige krav til offentlige og private virksomheter i GDPR

- Alle skal gi god informasjon om hvordan de behandler personopplysninger
- Alle skal vurdere risiko og personvernkonsekvenser
- Alle skal bygge personvern inn i nye løsninger
- Mange virksomheter må opprette personvernombud
- Reglene gjelder også virksomheter utenfor Europa
- Alle databehandlere får nye plikter
- Alle bør samarbeide i egne nettverk og følge bransjenormer
- Alle får nye krav til avvikshåndtering
- Alle må kunne oppfylle borgernes nye rettigheter

Viktige momenter vedr. ITSM og GDPR (1/2)

- **Gjelder ikke bare «personnummer»**: Alle former for identifikasjon av en person er relevant, f.eks. brukernavn, epostadresse, eventuelle biometriske data som benyttes for identifikasjon, etc.
- **Gjelder både databehandler og dataansvarlig**: Å hevde at det var den annen part (f.eks. i outsourcing eller SaaS) som er skyld ved en datalekkasje hjelper ikke – det er felles ansvar, også for å betale eventuell bot!
- **Hurtig rapportering av datalekkasjer**: Enhver datalekkasje skal rapporteres til alle som den omfatter, samt til offentlige myndigheter snarest og senest innen tre døgn.
- **Flere rettigheter til de registrerte**: Individet har rett til å få se alt som er registrert om vedkommende (inkl. «få se alle saker hvor jeg er med»), få data korrigert, få data slettet (med mindre det er lover som begrenser dette), etc.

Viktige momenter vedr. ITSM og GDPR (2/2)

- **Personvernombud påkrevet hos mange**: Denne personen kommer til å «blande seg inn» i hvordan servicedesk håndterer informasjon, og potensielt påvirke prosesser og rutiner
- **Aksept for å bli registrert**: Ved all registrering av personinformasjon, må den det gjelder akseptere dette, dvs. at man trenger rutiner (og systemer) som gjør det mulig å registrere at vedkommende har svart «ja»
- **Internasjonale begrensninger**: Krav som gjelder utveksling av data med virksomheter i andre land (spesielt utenfor EU/EØS) er strengere; kan ha stor innvirkning på SaaS og outsourcing
- **Dokumentasjon**: Krav til at man ikke bare følger reglene, men kan dokumentere at man gjør det, f.eks. ha verktøy som kan finne igjen alle dokumenter relatert til en gitt person

Hva bør en Service Management organisasjon gjøre?

- Minimere bruken av personsensitive data så langt det lar seg gjøre
- Dokumentere all dataflyt (ikke bare prosesser), inklusive rapportering, dataekstrakt etc.
- Lagre eventuelle rapporter, eksporter, etc. på dokumentert, sikkert sted
- Unngå mail med personsensitive data (spres ofte for lett!)
- Vurdere om enkelte data bør lagres kryptert

Spørsmål og (mulige) svar

www.managenordic.no manag e