På ett minutt
– dette er hva den nye EU GDPR betyr for deg

EUs generelle forordning om databeskyttelse vil øke enkeltpersoners personvern og gi lovgivende myndigheter større myndighet til å aksjonere mot selskaper som bryter de nye lovene. Det betyr følgende for din bedrift:

Høyt straffenivå:
bøter på opptil

4 % av total årlig omsetning eller

20 millioner Euro

er satt som den største boten du kan få.

Forordningen gjelder også selskaper **utenfor EU**, og som håndterer persondata for individer innen EU.

Internasjonal overføring av data vil fortsatt bli regulert under EUs GDPR regelverk.

Definisjonen av persondata er utvidet og omfatter identifiserende data som:

genetisk

mental

kulturell

økonomisk

sosial identitet

Det må være klare regler for **innhenting av samtykke** for å behandle personlige data, og det skal være bekreftende svar.

Det kreves samtykke fra foreldre for **å prosessere personlige data til barn** under 16 år.

Individer har **rett til å bli glemt** og slettet fra registre.

Brukere kan be om å få tilsendt en **kopi av personlige data**.

Data-ansvarlige må **rapportere databrudd** ikke senere enn

72 timer

etter at de har fått kjennskap til bruddet, med mindre bruddet har lav risiko for individets rettigheter.

Utnevnelse av en **databeskyttelsessjef** (Data Protection Officer – DPO) vil være obligatorisk for selskaper som behandler store volum av personlige data, og det vil også være fornuftig for andre selskaper.

Det vil kreves at det foretas en **risikovurdering for personvern** i prosjekter hvor risikoen er høy.

Produkter, systemer og prosesser må ta hensyn til at det skal **designes inn personvern** under utviklingen.

Data-ansvarlige må sørge for at det er passende avtaler for å **styre data-prosessen**.

Databehandlere kan bli holdt **direkte ansvarlige** for sikkerheten til persondata.

Ansvarlige må ha en **juridisk grunn for å prosessere** og samle inn persondata.

ISO 27001 og andre sertifiseringer kan hjelpe til med å vise **"nødvendige tekniske og organisasjonsmessige forholdsregler"** for å beskytte persondata og systemer.

One-stop shop (Supermarked for databehandling): internasjonale selskaper behøver bare å forholde seg til en overordnet databeskyttelsesinstans (Datatilsyn).

EU GDPR må oppfylles innen mai 2018

Kilde: itgovernance.co.uk

Bisnode
Make a smart decision