EU:s allmänna dataskyddsförordning - hur förbereder man sig?

SNS 8 april 2016

Elisabeth Wallin, Jurist, Datainspektionen

Datainspektionen

Vad händer 2018?

- EU:s allmänna dataskyddsförordning ersätter dataskyddsdirektivet från 1995
- PUL ersätts troligen med en ”rest-PUL”
- All svensk lagstiftning inom förordningens tillämpningsområde måste ses över – bl.a. den s.k. ”Förordningsutredningen”, klar 12 maj 2017
- Europeiska dataskyddsstyrelsen ersätter den s.k. 29-gruppen
- Datainspektionen får nya arbetsuppgifter
- Personuppgiftsansvariga (PUA) och personuppgiftsbiträden (PUB) ska vara förberedda och följa GDPR

Datainspektionen

1. Hur ser medvetenheten om integritet och dataskydd ut i organisationen?

- Ta reda på vad de nya reglerna innebär – hur kommer er organisation att påverkas?
- Identifiera de områden som ni kan behöva arbeta särskilt med.
- Medvetenhet hos alla beslutsfattare och nyckelpersoner i organisationen …

Datainspektionen

2. Dokumentera den behandling av personuppgifter som sker

- Dokumentera vilka personuppgifter ni hanterar, för vilka syften det sker, varifrån och hur uppgifterna samlas in och till vem de lämnas ut.

- Kan underlätta att uppfylla förordningens krav på förteckningsskyldighet …

Datainspektionen

3. Har ni stöd i förordningen för personuppgifts-behandlingen?

- Nya krav ifråga om samtycke
- Myndigheter kommer inte att kunna behandla uppgifter med stöd av en intresseavvägning
- Missbruksregeln i 5 a § PuL försvinner – se över vilka förutsättningar som finns enligt förordningen att behandla uppgifter i t.ex. löpande text på internet.

Datainspektionen

4. Accountability – bevisa ”compliance”

- Med vilket rättsligt stöd utförs er personuppgiftsbehandling? Se till att ni tydligt har bestämt och dokumenterat vilket rättsligt stöd ni har.

- Ta fram policies, riktlinjer m.m. för hur personuppgiftsbehandlingen ska gå till.

- Finns det förutsättningar för branschöverenskommelser eller certifiering avseende er behandling som kan underlätta att visa *accountability*?

5. Gör en konsekvensbedömning

- Kan er personuppgiftsbehandling innebär särskilda risker för de enskilda?

- Behandlar ni en stor mängd känsliga uppgifter, behandlar ni uppgifter i syfte att profilera kunder, anställda etc eller utför ni kameraövervakning på allmän plats?

- Om denna bedömning visar på höga risker med behandlingen – måste ni samråda med DI

Datainspektionen

6. Kan de skyddsåtgärder som behövs byggas in?

- T.ex. gm pseudonymisering och data minimering
- Andra tekniska och organisatoriska åtgärder/säkerhetsåtgärder?
- Dataskyddsåtgärder per automatik, som grundinställningar
- Skyldighet att se till löpande, både vid beslut om ett system och därefter

7. Behöver ni utse ett dataskyddsombud?

- Gäller myndigheter, vid behandling av känsliga uppgifter eller brottsuppgifter i stor skala samt vid behandling av uppgifter som innebär systematisk övervakning om enskilda

- Ge ombudet möjlighet och resurser att utföra sina uppgifter, att upprätthålla nödvändig kompetens och att rapportera direkt till högsta ledningen

8. Informationen till enskilda – är den tillräcklig?

- Krav på mycket mer detaljerad information till enskilda,

(t.ex. information om rättslig grund, ev. tredjelandsöverföring, lagringstid, enskildas rättigheter rätt att ge in klagomål till DI m.m.)

- Uttryckligt krav på tydlig, begriplig, lätt tillgänglig och kortfattad information – särskilt om personuppgifterna avser barn

Datainspektionen

9. Kan ni uppfylla kraven ifråga om rättigheter för de som uppgifterna avser

- Nu gällande krav - rätt till åtkomst, rättelse, radering, att motsätta sig direkt marknadsföring - men mer specificerade. Kan ni uppfylla dessa?

- Nya rättigheter - rätt till begränsad behandling, rätt till data portabilitet, utökad rätt att motsätta sig behandling. Vad behöver ni göra för att möta förordningens mer detaljerade krav?

- Nya krav på elektroniskt utlämnande – klarar ni detta? (Rätt till åtkomst, rätt till dataportabilitet)

Datainspektionen

10. Inför rutiner för att anmäla datasäkerhetsincidenter till Datainspektionen

- Kräver rutiner både för att kunna upptäcka, rapportera och utreda incidenter.
- Vilka uppgifter behandlas? Vilka situationer skulle kunna bli anmälningspliktiga?
- Hur kan kravet på rapportering inom 72 timmar uppfyllas?
- Behöver de registrerade informeras?

Datainspektionen

11. Är er organisation verksam i flera olika EU-länder ?

- Var ligger huvudkontoret eller det bolag där besluten om behandling tas?
- Har ni rutiner för att samarbeta med detta bolag och inom koncernen i stort för att uppfylla gemensamma krav på personuppgiftsbehandling
- Andra dataskyddsmyndigheter än den svenska kan komma att fatta beslut som blir bindande

Datainspektionen

12. Hur ska ni hantera ev. sanktionsavgifter och skadeståndskrav?

- Sanktionsavgifter på upp till 20 miljoner € eller 4 % av den personuppgiftsansvariges globala omsättning …

- Skadeståndsansvar – kan behöva ersätta hela skadan även om man bara kan ses som ansvarig för en del