

2019-02-15

Frågeunderlag inför granskning

Frågeunderlag inför granskning av dataskyddsorganisation

Inledning

Dataskyddsombuden genomför en granskning av personuppgiftsansvarigas dataskyddsorganisationer, som en del av dataskyddsenhetens övervakande arbete 2019. Denna granskning genomförs hos alla personuppgiftsansvariga organisationer inom dataskyddsenhetens arbetsområde. Granskningens syfte är att kontrollera hur personuppgiftsansvariga arbetar strategiskt med dataskyddsfrågor samt hur det systematiska arbetet med dataskydd är organiserat hos personuppgiftsansvariga.

Om dataskyddsförordningens krav på dataskyddsorganisation

Av artikel 24 i dataskyddsförordningen följer att den personuppgiftsansvarige ska genomföra lämpliga tekniska och *organisatoriska åtgärder för att säkerställa* och kunna visa att organisationens personuppgiftsbehandlingar följer dataskyddsförordningen. Detta innebär även att den personuppgiftsansvarige vidtar lämpliga strategier för dataskydd. Dessa skyldigheter tydliggörs och förstärks ytterligare av artikel 5.2 enligt vilken den personuppgiftsansvarige ska kunna visa att all personuppgiftsbehandling följer de viktiga grundprinciperna för personuppgiftsbehandling.

Dessa och andra bestämmelser i dataskyddsförordningen medför att det är centralt för personuppgiftsansvariga att organisera sig för att säkerställa att förordningen följs. Detta är en del av det strategiska dataskyddsarbetet. Mer konkret handlar det om att sätta upp en dataskyddsorganisation anpassad för verksamheten och initiera styrande dokument och processer för strategiskt viktiga dataskyddsfrågor.

Dataskyddsorganisationen kan utformas på många olika sätt. Det är viktigt att arbetet rent praktiskt fungerar och att strategierna får det tydliga genomslag i arbetet som avsetts. Det är den högsta ledningen som ytterst ansvarar för hur organisationen uppfyller kraven i artikel 24 dataskyddsförordningen. Ledningen ansvarar generellt för att verksamhetens organisation och förvaltning har ordnats på ett tillfredställande sätt för verksamheten.

Granskningsmetod och tidpunkt för granskning

Varje personuppgiftsansvarig organisation inom dataskyddsenhetens arbetsområde kommer att svara på de frågor avseende dataskyddsorganisation som följer nedan. Organisationerna har delats upp utifrån hur återkopplingen på frågorna ska levereras (genom möte med dataskyddsombuden eller genom skriftligt svar).

Ni som mottar denna skrivelse kommer att få lämna ett skriftligt svar på frågorna.

Ert svar ska ha inkommit till er organisations dataskyddsombud senast den 10 april 2019.

Granskningens syfte är att kontrollera hur personuppgiftsansvariga arbetar strategiskt med dataskyddsfrågor samt hur det systematiska arbetet med dataskydd är organiserat hos personuppgiftsansvariga.

Frågor om dataskyddsorganisation

1. Har ni en fastställd dataskyddsorganisation och hur har den förankrats i verksamheterna?
2. Om ja, vilka roller ingår i den och vilket ansvar/uppgifter har de olika rollerna? Om nej, hur säkerställer er organisation efterlevnaden av dataskyddsförordning och annan dataskyddslagstiftning?
3. Finns utöver dataskyddsombud och dataskyddssamordnare andra formella ansvarsområden med koppling till dataskydd och informationssäkerhet inom er organisation (t.ex.

systemägarskap, informationsägare, systemförvaltare)? Om ja, lämna in sådan dokumentation.

4. Dataskyddsarbetet behöver vara tydligt förankrat i organisationen och en central uppgift för ledning är att etablera en god dataskyddskultur i organisationen:

Hur förmedlar högsta ledningen betydelsen av dataskyddsarbetet och dess prioritering i verksamheten? Ge konkreta exempel.

5. Er organisation har utsett ett dataskyddsbud. Enligt dataskyddsförordningen ska den personuppgiftsansvarige säkerställa att dataskyddsbudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter. Beskriv hur er organisation säkerställer detta?
6. Er organisation har utsett dataskyddssamordnare. Beskriv hur dataskyddssamordnare ges förutsättningar att genomföra sitt arbete utifrån parametrarna mandat, tid och tillgång till ledningen.
7. Vilka åtgärder vidtar er organisation för att se till att dataskyddsfrågorna blir en del av hela organisationens kvalitetsarbete?
8. Beskriv hur er organisation arbetar strategiskt med dataskyddsfrågor? Har er verksamhet styrande dokument för dataskyddsfrågor? Hur har denna dokumentation förankrats i verksamheten?

I tjänsten,

Anu Sundin
Parisa Maleki Nordin

Dataskyddsbud
Gävle kommun