Regeringskansliet,
Justitiedepartementet

Remiss av förslag till EU-direktiv om skydd för personer som rapporterar om överträdelser av unionsrätten

Inledning och sammanfattning

Datainspektionen har granskat förslaget till EU-direktiv utifrån myndighetens uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter.

Datainspektionen konstaterar att inrättande av rapporteringskanaler i enlighet med förslaget i de flesta fall kommer att innebära att personuppgifter behandlas på ett sådant sätt att EU:s dataskyddsförordning 2016/679 blir tillämplig. Datainspektionen konstaterar vidare att det är fråga om en integritetskänslig behandling av personuppgifter som i vissa fall kommer att innefatta känsliga personuppgifter samt uppgifter om lagöverträdelser som avses i artikel 10 EU:s dataskyddsförordning. Datainspektionen anser att behandlingen medför höga risker för enskildas personliga integritet. Detta kräver noggranna överväganden utifrån dataskyddsförordningens bestämmelser.

Datainspektionen anser att det krävs en närmare analys av hur förslaget till EU-direktiv förhåller sig till EU:s dataskyddförordning och andra relevanta dataskyddsregler, innan det nya regelverket kan träda i kraft.

Datainspektionen efterfrågar bland annat en närmare analys av behovet av att stärka kontrollen av efterlevnaden av ett flertal nya unionsrättsakter genom krav på att inrätta rapporteringskanaler för visselblåsare. Det gäller inte minst behovet av att stärka kontrollen av efterlevnaden av EU:s regelverk till skydd för den personliga integriteten genom krav på inrättande

av rapporteringskanaler som i sig medför integritetskänslig behandling av personuppgifter. Det behöver övervägas om krav på att inrätta rapporteringskanaler för visselblåsare är en sådan nödvändig åtgärd som, till exempel på området skydd av privatliv och personuppgifter, kan motivera integritetskänslig behandling av personuppgifter i enlighet med EU:s dataskyddsregler.

Datainspektionen anser att de krav som föreslås i kapitel 3 på att utse behöriga myndigheter för extern rapportering gällande överträdelser av EU:s regler om dataskydd i enlighet med bland annat förordning (EU) 2016/679, står i konflikt med förordningens bestämmelser i kapitel 4 om oberoende tillsynsmyndigheter och deras uppgifter. Det finns alltså redan tillsynsmyndigheter som i enlighet med förordning (EU) 2016/679 har att kontrollera efterlevnaden av dessa regler. Datainspektionen avstyrker därför förslaget i denna del.

Inte heller i övrigt kan Datainspektionen på föreliggande underlag tillstyrka förslaget till EU-direktiv.

Datainspektionen uppfattar att förslaget till EU-direktiv omfattar krav på att inrätta sådana interna system för uppgiftslämnande som Artikel 29-gruppen har yttrat sig om i Yttrande 1/2006 om tillämpningen av EU:s regler om uppgiftsskydd på interna system för uppgiftslämnande inom bokföring, intern bokföringskontroll, revision, bekämpande av mutor samt brottslighet inom bank- och finansväsen (WP 117), det vill säga så kallade system för visselblåsning.

Datainspektionen kan konstatera att förslaget till EU-direktiv i väsentliga avseenden skiljer sig från och går utöver vad Artikel 29-gruppen har uttalat om sådana system samt Datainspektionens praxis som rör behandling av personuppgifter i system för visselblåsning. Förslaget innebär exempelvis inga begränsningar vad gäller vilka kategorier av anställda som kan bli rapporterade genom kanalerna, eller överträdelsens allvarlighetsgrad. Det framstår vidare som oklart hur förslagets krav på att inrätta kanaler för rapportering förhåller sig till andra, alternativa metoder för att rapportera missförhållanden, till exempel när det gäller frivilligheten för anställda att använda de föreslagna kanalerna och möjligheten att rapportera anonymt.

Datainspektionen anser att det inte är tillräckligt att i förslaget till direktiv hänvisa till att behandling av personuppgifter enligt detta direktiv ska ske i enlighet med bland annat förordning (EG) 2016/679. Utan närmare analys av hur förslagen i sig förhåller sig till dataskyddsreglerna ser Datainspektionen

en stor risk för att kraven enligt det föreslagna direktivet kan komma att stå i konflikt med dessa regler. De som ska uppfylla kraven enligt regelverken riskerar annars att hamna i situationer där man genom att följa kraven enligt det föreslagna direktivet, kommer att bryta mot EU:s dataskyddsregler.

Datainspektionen ifrågasätter om de åtgärder för att skydda berörda personer som räknas upp i förslaget ger ett tillräckligt skydd och anser att det krävs en närmare analys av vilka integritetsrisker som förslaget ger upphov till, särskilt för den som blir rapporterad. Detta är nödvändigt för att kunna ta ställning till vilket skydd som behövs för att möta riskerna för den enskilde samt se till att behandlingen kan anses proportionerlig i enlighet med EU:s regler om dataskydd.

Generella synpunkter

Förslaget till EU-direktiv medför bland annat krav på organisationer inom såväl privat som offentlig sektor att inrätta interna kanaler och förfaranden för rapportering av överträdelser av unionsrättsakter på vissa områden samt uppföljning av sådana rapporter. Dessutom föreslås att medlemsstaterna på motsvarande områden ska utse så kallade behöriga myndigheter som ska inrätta även externa rapporteringskanaler och följa upp sådana rapporter.

Datainspektionen konstaterar att inrättande av sådana rapporteringskanaler i de flesta fall kommer att innebära att personuppgifter behandlas på ett sådant sätt att EU:s dataskyddsförordning 2016/679 blir tillämplig. Datainspektionen konstaterar att det är fråga om en integritetskänslig behandling av personuppgifter som i vissa fall kommer att innefatta känsliga personuppgifter samt uppgifter om lagöverträdelser som avses i artikel 10 dataskyddsförordningen. Datainspektionen anser att behandlingen medför höga risker för enskildas personliga integritet. Detta kräver noggranna överväganden utifrån dataskyddsförordningens bestämmelser.

Datainspektionen uppfattar att förslaget till EU-direktiv omfattar krav på att inrätta sådana interna system för uppgiftslämnande som Artikel 29-gruppen har yttrat sig om i Yttrande 1/2006 om tillämpningen av EU:s regler om uppgiftsskydd på interna system för uppgiftslämnande inom bokföring, intern bokföringskontroll, revision, bekämpande av mutor samt brottslighet inom bank- och finansväsen (WP 117), det vill säga så kallade system för visselblåsning.

Datainspektionen har med utgångspunkt från dataskyddsreglerna och Artikel 29-gruppens yttrande ovan gjort följande bedömningar vad gäller bolags3 användning av system för visselblåsning.

Ändamålet med ett system för visselblåsning bör vara att fånga upp sådana särskilt allvarliga oegentligheter som annars riskerar att inte nå fram till rätt personer och som kan få allvarliga konsekvenser för organisationen. Det innebär att normala informations- och rapporteringskanaler ska användas i första hand. Systemet ska därför utgöra ett komplement till normal internförvaltning och måste vara frivilligt att använda. Systemet får bara användas när det är sakligt motiverat att behandla uppgifterna i en sådan särskilt inrättad rapporteringskanal. Ett exempel kan vara att den anmälde ingår i ledningen och de misstänkta oegentligheterna av det skälet riskerar att inte tas om hand på vederbörligt sätt. Därför får också endast personer i nyckelpositioner eller ledande ställning inom det egna bolaget eller koncernen anmälas och behandlas i systemet. System för visselblåsning ska generellt begränsas till allvarliga oegentligheter som rör bokföring, intern bokföringskontroll, revision, bekämpande av mutor, brottslighet inom bank- och finansväsen, eller andra allvarliga oegentligheter som rör organisationens vitala intressen eller enskildas liv och hälsa. Detta följer även av Datainspektionens föreskrifter om behandling av personuppgifter som rör lagöverträdelser, DIFS 2018:2 2 § punkten 4.

Datainspektionen kan konstatera att förslaget till EU-direktiv i väsentliga avseenden skiljer sig från och går utöver, vad Artikel 29-gruppen har uttalat om system för visselblåsning samt Datainspektionens praxis som rör sådana system. Förslaget innebär exempelvis inga begränsningar vad gäller vilka kategorier av anställda som kan bli rapporterade genom kanalerna, eller överträdelsens allvarlighetsgrad. Det framstår vidare som oklart hur förslagets krav på att inrätta kanaler för rapportering förhåller sig till andra, alternativa metoder för att rapportera missförhållanden, till exempel när det gäller frivilligheten för anställda att använda de föreslagna kanalerna och möjligheten att rapportera anonymt.

Datainspektionen har inte inom ramen för sin tillsynsverksamhet kontrollerat system för visselblåsning inom offentlig sektor, men har i andra sammanhang uttalat bland annat följande. De överväganden som Datainspektionen ansett att bolag måste göra vid inrättande av särskilda rapporteringskanaler bör, som utgångspunkt vara desamma för myndigheter vid inrättande av sådana kanaler för liknande ändamål. För myndigheternas del tillkommer dock problemställningar med anledning av bestämmelserna i offentlighets- och sekretesslagen och arkivlagen om skyldighet att diarieföra,

bevara och lämna ut personuppgifter i allmänna handlingar. Dessa bestämmelser kan behöva vägas in vid bedömningen av huruvida det finns rättsligt stöd för behandlingen, eftersom de kan inverka på den enskildes personliga integritet. Datainspektionen anser att det finns skäl att överväga behovet av särskild reglering av funktioner för visselblåsning hos myndigheter inbegripet personuppgiftsbehandling. Vid övervägandena behöver även bestämmelsen i 2 kap. 6 § regeringsformen beaktas. Genom kompletterande författning till dataskyddsförordningen är det möjligt att klargöra vad som är nödvändig behandling av personuppgifter inom ramen myndigheters system för visselblåsning. I samband därmed kan även nödvändiga överväganden göras utifrån bestämmelserna i offentlighet- och sekretesslagen samt arkivlagen om skyldighet att diarieföra, bevara och lämna ut uppgifter i allmänna handlingar. Vidare har lagstiftaren enligt dataskyddsförordningen artikel 35.10 möjlighet att inom ramen för ett lagstiftningsarbete befria de personuppgiftsansvariga myndigheterna från sin skyldighet att i vissa fall göra en konsekvensbedömning i enlighet med artikel 35.1-7. Detta kan väsentligt underlätta för myndigheterna, som annars själva behöver göra dessa bedömningar. Kompletterande nationella regler som tas fram måste givetvis vara förenliga med dataskyddsförordningen. Fråga om gränsdragning mellan dataskyddsförordningen och brottsdatalagen kan också behöva utredas såvitt avser behöriga myndigheter enligt brottsdatalagen.

Synpunkter på de specifika förslagen till bestämmelser

Artikel 1och bilaga till förslaget samt artikel 4 och 6

Datainspektionen efterfrågar en närmare analys av behovet av att stärka kontrollen av efterlevnaden av ett flertal nya unionsrättsakter genom krav på att inrätta rapporteringskanaler för visselblåsare. Det gäller inte minst behovet av att, i syfte att stärka kontrollen av efterlevnaden av EU:s regelverk till skydd för den personliga integriteten, kräva inrättande av rapporteringskanaler som i sig medför integritetskänslig behandling av personuppgifter. Det behöver övervägas om ett krav på att inrätta rapporteringskanaler för visselblåsare är en sådan nödvändig åtgärd som, till exempel på området skydd av privatliv och personuppgifter, kan motivera integritetskänslig behandling av personuppgifter i enlighet med EU:s dataskyddsregler.

Artikel 2

Datainspektionen konstaterar att förslaget innebär en utvidgning av den krets som kan använda kanalerna för rapportering jämfört med vad som framgår av artikel 29-gruppens yttrande om interna system för

uppgiftslämnande inom vissa områden och Datainspektionens föreskrift om behandling av personuppgifter som rör lagöverträdelser som rör system för visselblåsning.

Artikel 3.4 och 3.5
Datainspektionen efterfrågar ett förtydligande av huruvida även misstankar om inträffade överträdelser ska kunna få rapporteras i interna och externa kanaler enligt förslaget.

Datainspektionen anser vidare att det behövs en definition av begreppet interna kanaler för rapportering som klargör hur förslaget förhåller sig till sådana interna system för uppgiftslämnande (system för visselblåsning) som Artikel 29-gruppen har yttrat sig om enligt ovan vad gäller hur sådana kan inrättas i överensstämmelse med EU:s regler för uppgiftsskydd. I yttrandet har sådana system för uppgiftslämnande beskrivits som en extra möjlighet för de anställda att rapportera via en särskild kanal som kompletterar företagens normala informations- och rapporteringskanaler t.ex. personalrepresentanter och överordnade. I yttrandet framhålls vidare att sådana system ska ses som ett komplement till och inte som en ersättning för internförvaltning. I yttrandet utesluts inte möjligheten att i vissa fall rapportera anonymt.

Datainspektionen efterfrågar även ett förtydligande när det gäller hur de föreslagna kanalerna för rapportering förhåller sig till vad som ovan beskrivs som normala informations- och rapporteringskanaler och internförvaltning, samt hur förslagets krav på att inrätta kanaler för rapportering förhåller sig till andra, alternativa metoder för att rapportera missförhållanden, till exempel när det gäller frivilligheten för anställda att använda de föreslagna kanalerna och möjligheten att rapportera anonymt. Se även synpunkter till artikel 4.2. nedan.

Artikel 4.2
Se även synpunkterna ovan till artikel 3.4 och 3.5. Datainspektionen anser att det behöver tydliggöras huruvida bestämmelsen att det inte ska vara obligatoriskt för andra än anställda att använda interna rapporteringskanaler ska tolkas motsatsvis när det gäller anställda, med andra ord huruvida avsikten är att det ska vara obligatoriskt för anställda att använda sådana interna rapporteringskanaler som avses i förslaget och vad som i så fall innefattas i det begreppet.

Artikel 4 och 4.6

Datainspektionen anser att begreppet rättsliga enheter behöver förtydligas, särskilt i förhållande till begreppet personuppgiftsansvarig enligt EU:s dataskyddsförordning. Datainspektionen anser exempelvis att respektive nämnd i en kommun normalt är personuppgiftsansvarig för sin verksamhet och att en avdelning normalt sett inte är personuppgiftsansvarig.

Artikel 5.2
Vad gäller rapporteringskanaler som tillhandahålls externt av en tredje part vill Datainspektionen påminna att det finns krav på bland annat avtal med personuppgiftbiträden i EU:s dataskyddsförordning. Vid anlitande av en annan organisation behövs vidare tas ställning till om den organisationen utför uppdraget som personuppgiftsansvarig, eller har en osjälvständig roll som personuppgiftsbiträde. Bestämmelser om sekretess- och tystnadsplikt behöver också beaktas i detta sammanhang.

Artikel 6
Datainspektionen anser att de krav som föreslås i kapitel 3 på att utse behöriga myndigheter för extern rapportering gällande överträdelser av EU:s regler om dataskydd i enlighet med bland annat förordning (EU) 2016/679, står i konflikt med förordningens bestämmelser i kapitel 4 om oberoende tillsynsmyndigheter och deras uppgifter. Det finns alltså redan tillsynsmyndigheter som i enlighet med förordning (EU) 2016/679 har att kontrollera efterlevnaden av dessa regler. Datainspektionen avstyrker därför förslaget i denna del.

Artikel 7.4
Datainspektionen anser att frågor om tystnadsplikt- och sekretess behöver övervägas när det gäller samtliga som kommer i kontakt med informationen, det vill säga även när det gäller till exempel ansvarig handläggare.

Artikel 9.1.a
Datainspektionen anser att det behöver förtydligas om avsikten är att införa en informations- och/eller editionsplikt för den som rapporterar om en överträdelse.

Artikel 11
Bestämmelsen behöver förtydligas vad gäller hur samtyckena enligt punkterna 3 och 5 förhåller sig till samtycke som rättslig grund till behandling av personuppgifter enligt förordning (EU) 2016/679. Ett sådant samtycke måste uppfylla kraven i artikel 4.11 och 7, med beaktande av skäl 43. Det innebär bland annat att myndigheter normalt sett inte kan stödja sin behandling av personuppgifter på samtycke. Detsamma gäller arbetsgivares

behandlingar av personuppgifter om anställda. Om avsikten inte är att behandlingen av personuppgifter ska vila på den rättsliga grunden samtycke, bör ett annat ord användas, exempelvis medgivande. Av formuleringarna framgår inte heller klart vad som får göras med respektive utan den rapporterande personens ”samtycke”, varför ett förtydligande är nödvändigt även i den delen. Datainspektionen anser vidare att ett eventuellt samtycke som rättslig grund som regel ska lämnas innan samtalet spelas in.

Artikel 15.4 och 15.7
Datainspektionen anser att förslaget i dessa delar behöver analyseras närmare utifrån svensk rättstradition.

Artikel 16
Datainspektionen ifrågasätter om de åtgärder för att skydda berörda personer som räknas upp i förslaget ger ett tillräckligt skydd och anser att det krävs en närmare analys av vilka integritetsrisker som förslaget ger upphov till, särskilt för den som blir rapporterad. Detta är nödvändigt för att kunna ta ställning till vilket skydd som behövs för att möta riskerna för den enskilde samt se till att behandlingen kan anses proportionerlig i enlighet med EU:s regler om dataskydd.

Datainspektionen anser vidare vad gäller punkten 2 om att de behöriga myndigheterna ska säkerställa att identiteter skyddas är svårt att förena med hur sekretess- och tystnadsplikt regleras.

Artikel 17
Datainspektionen anser att uttrycket illvilliga eller ogrundade rapporter behöver förtydligas, eventuellt i artikel 3.

Artikel 18.
Datainspektionen anser inte att det är tillräckligt att i förslaget till direktiv hänvisa till att behandling av personuppgifter enligt detta direktiv ska ske i enlighet med bland annat förordning (EG) 2016/679. Utan närmare analys av hur förslagen i sig förhåller sig till dataskyddsreglerna ser Datainspektionen en stor risk för att kraven enligt det föreslagna direktivet kan komma att stå i konflikt med dessa regler. De som ska uppfylla kraven enligt regelverken riskerar att hamna i situationer där man genom att följa kraven enligt det föreslagna direktivet, kommer att bryta mot EU:s dataskyddsregler.

Detta yttrande har beslutats av enhetschefen Catharina Fernquist efter föredragning av juristen Katarina Högquist. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom deltagit.

Catharina Fernquist, 2018-09-12 (Det här är en elektronisk signatur)