



KLAGANDE

Philip Naskret

ÖVERKLAGAT AVGÖRANDE

Datainspektionens beslut den 28 januari 2019 i ärende med diarienummer DI-2019-1083, se bilaga A

SAKEN

Rätt att ta del av allmän handling

KAMMARRÄTTENS AVGÖRANDE

Kammarrätten undanröjer Datainspektionens beslut och visar målet åter till Datainspektionen för ny prövning i enlighet med vad som framgår av skälen för detta avgörande.

YRKANDEN M.M.

Philip Naskret vidhåller sin begäran att få ta del av uppgift om hur många anmälningar om personuppgiftsincidenter enligt artikel 33 i EU:s allmänna dataskyddsförordning (EU/2016/679), dataskyddsförordningen, som Datainspektionen har tagit emot från Region Jönköpings län från och med den 25 maj 2018 till och med den 31 december 2018. Han för fram bl.a. följande. Uppgift om antal personuppgiftsincidenter kan inte anses utgöra känslig information på sätt som lagstiftaren avsett. Tvärtom är uppgifterna harmlösa och kan lämnas ut utan risk för skada. Aktuell begäran om att få ut allmänna handlingar omfattar inte innehållet i incidentrapporterna utan endast antalet anmälda incidenter. Detta kan inte äventyra IT-säkerheten för Region Jönköpings län.

SKÄLEN FÖR KAMMARRÄTTENS AVGÖRANDE

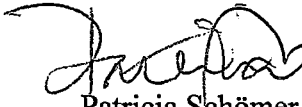
Enligt 2 kap. 15 § första stycket tryckfrihetsförordningen, TF, ska en begärd handling, om den inte kan tillhandahållas utan att en sådan del av handlingen som inte får lämnas ut röjs, i övriga delar göras tillgänglig för sökanden. Av detta följer att en begäran att få ta del av en allmän handling ska leda till att den beslutande myndigheten noggrant prövar vilka uppgifter i handlingen som kan lämnas ut. Övrig relevant rättslig reglering framgår av det överklagade beslutet.

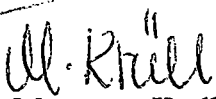
För att ta ställning till Philip Naskrets begäran om att få del av antalet anmälningar om personuppgiftsincidenter som har gjorts av Region Jönköpings län under den aktuella perioden krävs det enligt kammarrätten en bedömning av uppgifterna i respektive anmälan. Kammarrätten har tagit del av de aktuella anmälningarna i dess helhet och konstaterar att de till stora delar inte omfattar känsliga uppgifter. Om anmälan inte innehåller känsliga uppgifter, t.ex. uppgifter om intrång eller brister i den personuppgiftsansvariges IT-system eller uppgifter som kan bidra till att

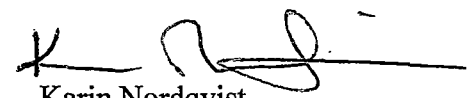
avslöja att IT- eller säkerhetssystemet är sårbart för attacker, borde anmälan och därigenom uppgift om anmälnans förekomst som utgångspunkt kunna lämnas ut. Anmälningar som inte innehåller känsliga uppgifter lämnar inte upplysning om att ingivarens säkerhetsåtgärder har brister. Den personuppgiftsansvariges säkerhetsåtgärder kan därmed inte heller antas motverkas om uppgift om anmälnans förekomst röjs.


Mot denna bakgrund är det inte tillräckligt att endast göra en generell bedömning som får till följd att samtliga anmälningar ska anses omfattas av sekretess enligt 18 kap. 8 § 3 offentlighets- och sekretesslagen (2009:400). Det framgår inte av det överklagade beslutet att Datainspektionen har gjort en prövning av uppgifterna i respektive anmälan och utifrån denna prövning beslutat att inte lämna ut uppgift om antalet anmälda personuppgiftsincidenter. Enligt kammarrätten kan Datainspektionen därför inte anses ha gjort en sådan noggrann sekretessprövning som krävs enligt 2 kap. 15 § första stycket TF. Det är inte kammarrättens uppgift att som första insats göra en sådan prövning. Datainspektionens beslut ska därför undanröjas och målet visas åter till inspektionen för ny prövning av Philip Naskrets begäran.

HUR MAN ÖVERKLAGAR, se bilaga B (formulär 2).


Patricia Schömer
kammarrättsråd
ordförande


Margareta Krüll
kammarrättsråd


Karin Nordqvist
tf. assessor
referent


Camilla Stark
föredragande jurist

Begäran om utlämnande av allmän handling

Beslut

Datainspektionen avslår begäran.

Bakgrund

Philip Naskret har den 25 januari 2019 inkommit med en begäran om att få ta del av uppgift om hur många anmälningar om personuppgiftsincidenter enligt artikel 33 i EU:s allmänna dataskyddsförordning (EU/2016/679) (dataskyddsförordningen) som Datainspektionen har tagit emot från en viss utpekad aktör.

Skäl för beslutet

Enligt 18 kap. 8 § 3 offentlighets- och sekretesslagen (2009:400) (OSL) gäller sekretess för uppgifter som lämnar eller kan bidra till upplysning om säkerhets- och bevakningsåtgärd om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser bland annat system för automatiserad behandling av information.

Ett rakt skaderekvisit innebär normalt att det är uppgifternas karaktär som får avgöra om sekretess gäller eller inte. Om uppgiften är sådan att den genomsnittligt sett måste betraktas som harmlös ska den alltså normalt anses vara offentlig. Om uppgiften i stället typiskt sett måste betraktas som känslig omfattas den normalt av sekretess. Skaderekvisitet kan alltså uppfattas som en metod att precisera föremål för sekretessen eller dess räckvidd (prop. 1979/80:2 Del A s. 77-78).

Bestämmelsen i 18 kap. 8 § 3 OSL har i ett tidigare lagstiftningsärende ansetts innebära att uppgifter om ingivare av incidentrapportering avseende säkerhetsbrister i IT-system till Post- och telestyrelsen, liksom uppgifter om innehållet i rapporterna, omfattas av sekretess (prop. 2003/04:93 s. 82). Utredningen om genomförande av NIS-direktivet har dessutom nyligen utrett om bestämmelsen behöver ändras för att känslig information i incidentrapporter som lämnas till Myndigheten för samhällsskydd och beredskap ska kunna skyddas. Den utredningen konstaterar i sitt betänkande att 18 kap. 8 § OSL ger ett tillräckligt skydd för uppgifter som kan komma att rapporteras vid en incident (SOU 2017:36 s. 247-257). Incidentrapporter hos Datainspektionen innehåller sådan skyddsvärd information rörande säkerhetsåtgärder som avses i 18 kap. 8 § 3 OSL. Det gäller oavsett om ingivaren är en myndighet eller ett privaträttsligt organ.

Den incidentrapportering som sker till Datainspektionen i enlighet med artikel 33 i förordningen kan i praktiken innebära en upplysning om att ingivarens IT-system är sårbart för attacker. Uppgiften om vem som har lämnat in en sådan rapport utgör i sig en uppgift som kan omfattas av sekretessens föremål enligt 18 kap. 8 § 3 OSL, eftersom den lämnar upplysning om att ingivarens säkerhetsåtgärder har brister. Det kan därför antas att den personuppgiftsansvariges säkerhetsåtgärder motverkas om det framkommer att dessa har brister. Bestämmelsens skaderekvisit är därmed uppfyllt, varvid sekretess gäller. Uppgiften om ingivarens identitet är typiskt sett känslig (prop. 2017/18:105 s. 129).

Datainspektionen beaktar vidare att en enskild personuppgiftsansvarig som anmäler en personuppgiftsincident kan komma att anmäla en eller flera nya personuppgiftsincidenter i framtiden. Det finns därmed risk för att uppgifter om de enskilda personuppgiftsincidenterna kan vara pusselbitar som tillsammans bildar en helhet som kan avslöja att ingivarens IT-system har brister.

Datainspektionen kan därför inte bekräfta att en viss aktör har inkommit med en anmälan när det inte står klart att sådan information är allmänt känd. Inte heller kan ett nekande svar lämnas på individuella förfrågningar, eftersom det i förlängningen skulle möjliggöra att genom systematiska förfrågningar kartlägga vilka aktörer som inkommit med anmälningar. Datainspektionen anser att ett sådant förfarande kan antas motverka syftet med åtgärden i den mening som avses i 18 kap. 8 § OSL.

Kammarrätten har i ett mål som gällde en prövning avseende en specifik anmälan ansett att personuppgiftsincidenter som inte avser intrång eller brister i den personuppgiftsansvariges IT-system och inte heller innehåller uppgifter som kan bidra till att avslöja att IT- eller säkerhetssystemet är

sårbart för attacker utgör harmlösa uppgifter. Kammarrätten anser att sådana personuppgiftsincidenter kan lämnas ut utan att det kan antas att syftet med vidtagna säkerhetsåtgärder motverkas om uppgifterna röjs (Kammarrätten i Stockholms dom den 2 augusti 2018 i mål nr 5200-18).

För att möjliggöra en handlägningsrutin som *dels* tillser att en individuell prövning görs av om en viss aktör inkommit med en anmälan som enbart innehåller sådana harmlösa uppgifter som kan lämnas ut, *dels* inte röjer uppgift om att en specifik aktör faktiskt har inkommit med en anmälan som innehåller uppgifter som inte kan lämnas ut, kontrollerar Datainspektionen alltid om den specifika aktören förekommer i Datainspektionens register över inkomna anmälningar. Om så görs en individuell bedömning av varje eventuell anmälan och i vilken mån det finns uppgifter som kan lämnas ut.

Mot bakgrund av det ovan anförda och kammarrättens vägledning i tidigare nämnda mål bedömer Datainspektionen att den begärda uppgiften inte kan lämnas ut i detta fall. Begäran ska därför avslås.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag ni fick del av beslutet. Datainspektionen sänder överklagandet vidare till Kammarrätten i Stockholm för prövning.

Beslutet har fattats av avdelningsdirektör Hans Kärnlöf efter föredragning av juristen Gustav Linder.



Hans Kärnlöf



Gustav Linder