

2016-10-11

Justitiedepartementet  
103 33 StockholmVårt diarienummer: KS/2016:254  
Ert diarienummer: Ju2016/04398/L6**Yttrande angående Delbetänkande – Hur står det till med den personliga integriteten?  
(SOU 2016:41), Ju2016/04398/L6**

Given möjlighet att avge yttrande i rubricerat ärende vill Nykvarns kommun inge följande synpunkter.

**Frågor som uppkommer med anledning av remissen om Datainspektionens roll**

Nykvarns kommun bedömer att det finns ett behov av ett nytt integritetsskyddsorgan som skulle ha till huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen. Datainspektionen sköter ej sitt uppdrag till fullo, ser ej till alla parter intresse och skulle i och med detta inte kunna verka för en säkrare avvägning.

Därför bedömer vi att ett integritetsskyddsorgan skulle kunna komplettera och framförallt säkerställa att alla parter intressen tas i beaktande, något som Datainspektionen i sitt nuvarande uppdrag inte lyckas med. Nykvarns kommun avstyrker därför kommitténs förslag att utvidga Datainspektionens uppdrag att följa och beskriva utvecklingen på IT-området när det gäller frågor som rör personlig integritet och ny teknik samt de legala förutsättningarna för integritetsskyddet.

Nykvarns kommun ser också att lagstiftningen kopplat till de risker som identifierats bör gås igenom, bearbetas och ändras, många gånger är lagen ej anpassad till den utveckling som skett de senaste åren och kan därför inte appliceras på de ärenden som hamnar inom området ”integritet”. Det är framförallt de lagar som finns i brottsbalken som bör ses över för att vara relevanta till den form av brott som begås idag. Lagstiftningen bör också beakta den situation som brottsoffer och drabbade idag befinner sig i, många gånger är deras möjligheter till att få upprättelse minimala och deras integritet skyddas inte eller tas inte i beaktande.

**Risker för medborgaren med bristande informationssäkerhet**

Integritetskommitténs uppdrag är att utifrån ett individperspektiv kartlägga och analysera risker för intrång i den personliga integriteten som kan uppkomma i samband med användningen av informationsteknik. Kommittén konstaterar att enskilda personer har bristande möjligheter att påverka hur uppgifter om dem hanteras och att det finns starka indikationer på allvarliga brister i informationssäkerheten i offentliga verksamheter som gör omfattande personuppgiftsbehandlingar. Betänkandet betonar att huvudmän som hanterar personuppgifter måste ta sitt ansvar för säkerheten. Det är viktigt att integritets- och sekretessaspekten beaktas vid all dokumentation och hantering.

Att flera olika offentliga och privata aktörer kan vara inblandade i hanteringen av de enskildas uppgifter medför en ökad risk av bristande informationssäkerhet och ansvarstagande för hanteringen. Detta ställer särskilda krav på säkerhet där personuppgifterna ska hanteras på ett tekniskt och juridiskt säkert sätt. Om uppgifterna samordnas mellan flera huvudmän får detta inte leda till risk för läckage. För många kommuners del behövs åtgärder som förbereder för den nya dataskyddsförordningen, informationsklassning av system och översyn av behörighetshantering.



Några företeelser som förekommer i kommuner förknippade med **viss** risk för den personliga integriteten:

- Hantering av personuppgifter inom elevhälsan (skolan)
- Arbetsgivares granskningar av vad arbetstagare skriver på sociala medier (arbetsliv)
- Kompetensdatabaser och bakgrundskontroller inom arbetslivet
- När vårdgivare tillhandahåller både hälso- och sjukvård och personaladministrativa tjänster
- Myndigheters användning av sociala medier (e-förvaltning)

Företeelser förknippade med **påtaglig** risk för den personliga integriteten:

- Kameraövervakning (i allmänhet och särskilt beträffande övervakning inomhus i skolan)
- Informationsdelning inom och mellan myndigheter (e-förvaltning)
- Oskyddad e-post

Företeelser som är förknippade med **allvarlig** risk för den personliga integriteten:

- Digitala lärplattformar och digitala läromedel (skolan)
- Vissa sociala medier (i allmänhet och särskilt beträffande användningen av sociala medier i skolans undervisning)
- Arbetsgivares positionering och annan övervakning och kontroll av arbetstagarnas aktiviteter och beteenden på arbetet
- Kameraövervakning på arbetsplatser
- Hälso- och sjukvård och välfärdstjänster inom socialtjänsten
- Myndigheter med kunddata i molnet (e-förvaltning)
- Lagring och vidarebearbetning av uppgifter som har samlats in med hjälp av kameraövervakning
- Publika molntjänster

**Säker digital identifiering ett krav vid e-tjänster och e-förvaltning**

För att digitaliseringens potential inom såväl privat som offentlig sektor ska utnyttjas fullt ut krävs att den personliga integriteten hanteras på ett sådant sätt att den enskilde känner tillit till och kan använda de tjänster som erbjuds. Valfungerande och säkra lösningar för e-identifiering och digitala underskrifter höjer säkerhetsnivån vid identifierings- och autentiseringsförfaranden och bidrar till utvecklingen av e-förvaltning och e-tjänster.

System för säker identifiering och autentisering har också en integritetsfrämjande potential eftersom de på ett effektivt sätt motverkar att personuppgifter tillgängliggörs eller sprids på ett otillbörligt sätt. De



utgör också en viktig beståndsdel för att skydda enskildas personliga integritet när tekniska system och lösningar tas fram genom ”privacy by design”.

Utredningen lämnar ett exempel på detta där myndigheters e-tjänster förses med programmatiska gränssnitt, där det är möjligt för medborgaren att med hjälp av sin e-legitimation begära ut nödvändiga uppgifter från olika myndigheter för att sedan låta sammanställa dessa uppgifter i den egna omgivningen, till exempel i webbläsaren eller i en applikation, innan de överförs till en specifik myndighet. Därmed undviks det mer integritetsingripande alternativet som bygger på att myndigheter ges direktåtkomst till andra myndigheters register. Genomtänkta system för e-identifiering som tar hänsyn till enskildas personliga integritet är ett krav vid framtagandet av e-tjänster inom offentlig sektor och i utbyggnaden av e-förvaltningen. Det ställer i sin tur stora krav på myndigheterna att sätta sig in i de tekniska och legala förutsättningarna. Eftersom det rör sig om ett komplext område under utveckling är det viktigt med samordning och samsyn på detta område.

### **Nykvarns kommuns sammanfattande synpunkter**

Nykvarns kommun anser att det är viktigt att medborgarnas rätt till integritet skyddas och stärks vid användning av informationsteknik. Vi anser vidare att kommitténs riskbedömning av de områden och företeelser som redovisas i delbetänkandet är välgrundad samt att de redovisade åtgärdsförslagen är väl avvägda.

Nykvarns kommun bedömer att det finns ett behov av ett nytt integritetsskyddsorgan som skulle ha till huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen. Datainspektionen sköter ej sitt uppdrag till fullo, ser ej till alla parter intresse och skulle i och med detta inte kunna verka för en säkrare avvägning.

Nykvarns kommun tillstyrker förslaget att regeringen i en årlig skrivelse till riksdagen ska informera om utvecklingen och det aktuella tillståndet när det gäller frågor som rör personlig integritet, informationsteknik och de legala förutsättningarna för integritetsskyddet.

Nykvarns kommun ser fram emot slutredovisningen av uppdraget 2017 och de förslag till åtgärder som då ska presenteras. En förhoppning är att slutbetänkandet på ett konkret sätt kan underlätta och stödja i den komplexa frågan om digital utveckling, nyttoeffektivisering och hur riskerna för intrång i den personliga integriteten kan minskas. Vi anser att det är mycket viktigt att medborgarnas rätt till integritet skyddas och stärks vid användning av informationsteknik.