Fördjupad kontroll

Kontrollpunkt 7: Integritetspolicy

Bakgrund

Dataskyddsförordningen innehåller ett antal rättigheter för den registrerade, alltså den vars personuppgifter behandlas. En av dessa rättigheter är rätten till information, vilket innebär att registrerade har rätt att få information från myndigheter och andra verksamheter om hur dessa behandlar personuppgifterna som samlas in. Denna information ska som regel ges både när uppgifterna samlas in och på begäran från den registrerade. Utifrån kraven i dataskyddsförordningen ska informationen vara lättillgänglig och tillhandahållas kostnadsfritt i skriftlig form, samt vara utformad med ett klart och tydligt språk. Ett sätt för en verksamhet att uppfylla kravet på information till registrerade är att tillhandahålla en integritetspolicy. Integritetspolicyns syfte blir då att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. För att integritetspolicyn ska kunna anses bidra till att en verksamhet uppfyller dess ansvarsskyldighet krävs det att policyn är utformad så att den motsvarar de krav som ställs i förordningen.

Av artikel 12 framkommer hur information som lämnas till den registrerade ska vara utformad, medan artikel 13 ställer krav på vilken information som ska lämnas. Ingen av artiklarna reglerar i detalj vilken form eller var informationen ska lämnas till den registrerade. I vägledningen om öppenhet och transparens anser arbetsgruppen att en bästa praxis innebär att en länk till dataskyddsinformationen ges eller att sådan information ges på samma sida som personuppgifterna hämtas från, när personuppgifterna samlas in online. En skiktad dataskyddsinformation bör användas om den personuppgiftsansvarige har en webbplats.

Syftet med kontrollen är att undersöka verksamhetens integritetspolicy samt rutiner för arbetet med policyn. Kontrollen har genomförts i två delar, där den första varit ett generellt frågeutskick där verksamheten ombads skicka in relevant dokumentation och den andra var ett kompletterande frågeutskick.

Iakttagelser från kontrollen

Intraservice har skickat in två versioner av sin integritetspolicy, en gammal och en ny reviderad version. Dataskyddsombudet kommer i granskningen enbart att titta på den reviderade versionen eftersom den gamla är inaktuell. Tillhörande till policyn finns också en ny framtagen rutin för att hålla policyn uppdaterad. Någon sådan fanns inte när kontrollen påbörjades.

Intern integritetspolicy

En intern integritetspolicy kan användas för de särskilda behandlingar som avser anställda i verksamheten, eftersom de ofta skiljer sig ifrån de behandlingar som sker av t.ex. kunder eller medborgares personuppgifter.

Intraservice uppger att det inte finns någon särskild integritetspolicy som riktar sig till anställda, men att alla får information vid anställningstillfället om hur deras

personuppgifter kommer att hanteras. En del av informationen är gemensam för hela staden och inte specifik för förvaltningen Intraservice. Intraservice uppger att informationen finns tillgänglig via inloggning i förvaltningens personaladministrativa system Personec. Dataskyddsombudet saknar information om vem som ansvarar för blanketten och säkerställer att den är uppdaterad. Därför är det oklart om Intraservice kan påverka denna information och på så sätt säkerställa att informationsplikten uppfylls.

Intraservice uppger att det finns planer på att ta fram verksamhetsspecifik information för anställda vilket beräknas beslutas om under hösten 2022. Dataskyddsombudet rekommenderar förvaltningen att göra detta, eftersom det sker ett flertal behandlingar som de anställda inte får information om. Intraservice har i dagsläget alltså inte något sätt att säkerställa att informationsplikten uppfylls gentemot de anställda.

Extern integritetspolicy

Av artikel 5.1 a dataskyddsförordningen framgår bland annat att uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet). Det följer vidare av artikel 5.2 att den personuppgiftsansvarige ska ansvara för och kunna visa att de principer som räknas upp i 5.1 efterlevs (ansvarsskyldighet).

Det följer av artikel 12.1 dataskyddsförordningen att den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

Intraservice anger att integritetspolicyn inte ämnar vara heltäckande, utan att den bara övergripande är tänkt att beskriva några av de behandlingar som förvaltningen utför. Om alla behandlingar skulle behövas tas med skulle det inte vara enkelt för de registrerade att ta del av. Intraservice har utgått ifrån IMY och Regeringskansliet för att hitta en rimlig nivå som övergripande beskriver de olika behandlingarna.

Information som måste tillhandahållas den registrerade

Dataskyddsombudet har utgått ifrån Artikel 29-gruppens vägledning om öppenhet och information vid granskningen av integritetspolicyn. I bilagan till vägledningen finns en lista över information som måste tillhandahållas den registrerade enligt artiklarna 13 eller 14 som dataskyddsombudet haft som utgångspunkt.

Eftersom förvaltningen valt en övergripande beskrivning av personuppgiftsbehandlingarna finns endast ett fåtal behandlingar beskrivna mer utförligt. För de sex angivna behandlingarna finns ett ändamål och rättslig grund angiven. Dataskyddsombudet anser att Intraservice inte uppfyller sin informationsplikt eftersom samtliga behandlingar med ändamål och rättslig grund inte finns angivna. För att förvaltningen skulle kunna uppfylla informationsplikten krävs att korrekt information gällande en specifik behandling i sådana fall lämnas till den registrerade vid varje insamlingstillfälle inför en ny behandling. Något sådant sker inte vad dataskyddsombudet

vet, utan normen är snarare att hänvisning sker till integritetspolicyn utan någon vidare eftertanke. Det innebär att för många av Intraservice behandlingar så är informationen varken klar, tydlig eller lättillgänglig. Den registrerade kan inte på något sätt få reda på hur dennes personuppgifter behandlas och vilket rättsligt stöd förvaltningen har. Intraservice har inte angett hur de registrerade får information annat än via integritetspolicyn, utöver i anställningsförhållandet. Dataskyddsombudet har förståelse för att en heltäckande integritetspolicy för en förvaltning med många behandlingar kan innebära en informationsutmattning för den registrerade. Men utifrån just mängden behandlingar anser dataskyddsombudet att de registrerade inte erhåller den information från förvaltningen som de har rätt till. Intraservice bör utreda hur policyn bättre kan formuleras, t.ex. med hjälp av skiktad integritetspolicy, eller hur det annars kan säkerställas att information lämnas till de registrerade.

Angående överföring till tredjeland uppger Intraservice i vaga termer att sådan överföring kan förekomma. Vilka behandlingar som innebär en tredjelandsöverföring framkommer dock inte. Dataskyddsombudet anser att detta måste framgå, annars vet den registrerade inte när dennes personuppgifter riskerar att överföras till tredjeland. Dataskyddsombudet saknar också information om relevant artikel i dataskyddsförordningen som förvaltningen stödjer sin överföring på och tillhörande överföringsmekanism. Det framkommer inte heller hur och var den registrerade kan få tillgång till eller erhålla den handling där all information framkommer. I Artikel 29-gruppens vägledning står det att information om tredjelandsöverföring ska vara så meningsfull som möjligt för den registrerade, vilket generellt sett bland annat innebär att tredjeländernas namn ska anges. Intraservice har inte fullgjort detta. Dataskyddsombudet rekommenderar att förvaltningen ser över informationen om tredjelandsöverföringar och säkerställer att den uppfyller kraven enligt GDPR.

Intraservice anger att förvaltningen inte sparar personuppgifter längre än vad som är nödvändigt för syftet med behandling. Någon precis angiven lagringstid per behandling framkommer inte. Artikel 29-gruppen yttrar i sin vägledning att det inte räcker att den personuppgiftsansvarige generellt anger att personuppgifterna bevaras så länge som är nödvändigt för de berättigade ändamålen, utan att olika lagringstider bör anges för olika kategorier av personuppgifter och/eller olika behandlingsändamål. Intraservice rekommenderas att komplettera informationen med konkreta uppgifter om hur länge lagring sker för de olika behandlingarna.

Dataskyddsombudet saknar information om huruvida Intraservice baserar någon behandling på samtycke. Om så är fallet rekommenderas förvaltningen att uppdatera integritetspolicyn med uppgifter om hur samtycket kan återkallas.

Lättillgänglig

Kravet på att informationen ska vara lättillgänglig innebär att de registrerade inte ska behöva leta reda på informationen. Det ska vara direkt uppenbart för dem var och hur de kan få åtkomst till informationen.

Intraservice integritetspolicy finns tillgänglig via Göteborg Stads hemsida. För att komma till policyn behövs ett klick från Intraservice egna sida, men flera klick om man kommer

via stadens hemsida. Det är i enlighet med vägledningen som säger att information aldrig ska vara mer än "två klick bort". Intraservice har även som regel i sitt digitala arbetssätt att varje medarbetare ska länka till integritetspolicyn i sin e-postsignatur. Dataskyddsombudet anser att det är positivt att den registrerade får information om personuppgiftsbehandlingen vid första kontakt med förvaltningen.

Språket

Kravet om ett klart och tydligt språk innebär att informationen bör ges på ett så enkelt sätt som möjligt och att komplicerade meningar och språkstrukturer bör undvikas. Informationen bör vara konkret och exakt, och den bör inte vara abstrakt eller tvetydig eller kunna tolkas på olika sätt. Framför allt bör syftena med och de rättsliga grunderna för behandlingen av personuppgifterna vara tydliga. Bestämningsord som "får", "kan", "viss", "ofta" och "eventuellt" bör undvikas, om man inte kan visa varför sådant språk är nödvändigt. Språket bör inte vara överdrivet formalistiskt, tekniskt eller specialiserat.

Dataskyddsombudet rekommenderar förvaltningen att se över språket då flera bestämningsord förekommer i policyn. Texten innehåller också några långa och komplicerade meningar som kan försvåra de registrerades förståelse av informationen.

Övrigt

I integritetspolicyn finns hänvisning till att mer information om specifika tjänster finns att läsa på intranätet men informationen där är ej åtkomlig för utomstående. Dataskyddsombudet rekommenderar att förvaltningen säkerställer så att informationen går att nå på annat sätt om det hänvisas som komplement till integritetspolicyn.

Översyn av integritetspolicy

Intraservice har tagit fram en ny rutin som säkerställer att integritetspolicyn ses över två gånger per år och att informationen i den hålls aktuell i takt med ändring av lagstiftning och riktlinjer, Intraservice uppdrag eller ändring i personuppgiftsbehandlingar. Dataskyddsombudet ser positivt på framtagande av rutinen eftersom den gamla integritetspolicyn inte setts över på flera år.

Sammanfattade rekommendationer

- Ta fram verksamhetsspecifik information (intern integritetspolicy) som fokuserar på de behandlingar som omfattar anställda.
- Utreda hur policyn bättre kan formuleras, t.ex. med hjälp av skiktad integritetspolicy, eller hur det annars kan säkerställas att information lämnas till de registrerade.
- Se över informationen om tredjelandsöverföring.
- Ange precis lagringstid för uppgifterna (inte ange "så länge det är nödvändigt för de berättigade ändamålen")
- Om samtycke används som rättslig grund rekommenderas det att informationen kompletteras med uppgifter om hur ett samtycke kan återkallas.
- Se över språket för att uppfylla kravet på ett klart och tydligt språk.
- Ta bort hänvisning till intranätet eftersom informationen där är ej åtkomlig för utomstående och inte fungerar som ett komplement till integritetspolicyn.

Bilagor

- Information om fördjupad kontroll 2022.
- Frågeunderlag fördjupad kontroll 2022, del 1 och del 2.

Information om fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy

Dataskyddsförordningen innehåller ett antal rättigheter för den registrerade, alltså den vars personuppgifter behandlas. En av dessa rättigheter är rätten till information, vilket innebär att registrerade har rätt att få information från myndigheter och andra verksamheter om hur dessa behandlar personuppgifterna som samlas in. Denna information ska som regel ges både när uppgifterna samlas in och på begäran från den registrerade. Utifrån kraven i dataskyddsförordningen ska informationen vara lättillgänglig och tillhandahållas kostnadsfritt i skriftlig form, samt vara utformad med ett klart och tydligt språk.

Ett sätt för en verksamhet att uppfylla kravet på information till registrerade är att tillhandahålla en integritetspolicy. Integritetspolicyns syfte blir då att informera registrerade om verksamhetens behandling av personuppgifter i enlighet med de krav som ställs i dataskyddsförordningen. För att integritetspolicyn ska kunna anses bidra till att en verksamhet uppfyller dess ansvarsskyldighet krävs det att policyn är utformad så att den motsvarar de krav som ställs i förordningen.

Granskningen avser kontrollera verksamhetens integritetspolicy, med fokus på utformning och tillhandahållande till registrerade (både internt och externt). Även verksamhetens rutiner för att arbeta med integritetspolicyn och säkerställa att den hålls uppdaterad ingår i kontrollen.

Tillvägagångssätt

Den fördjupade kontrollen kommer att genomföras i två delar. I del ett ombeds ni att skicka in dokumenterade integritetspolicys, rutiner samt besvara ett antal frågor. I del två kommer uppföljande frågor att ställas.

Dataskyddsombudet kommer sedan att sammanställa underlaget i en delårsrapport som lämnas till er i juni.

Fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy (del 1)

Dokumentation för er att skicka in till dataskyddsombudet:

1. Extern integritetspolicy (den policy som används för att informera medborgarna – kunder, besökare etc. – om de personuppgiftsbehandlingar som ni utför. Om ni har flera olika policys ombeds ni skicka in samtliga.)
    a. Skicka även med länkar till var informationen går att hitta så att dataskyddsombudet kan kontrollera tillgängligheten.
2. Intern integritetspolicy (den policy som används för att informera anställda/konsulter etc. om de personuppgiftsbehandlingar som ni utför. Om ni har flera olika policys ombeds ni skicka in samtliga.)
    a. Beskriv hur och när anställda/konsulter etc. får ta del av informationen.

Övrigt:

1. Har ni rutiner för att säkerställa att informationen i era integritetspolicys hålls uppdaterad?
    a. Om ja, beskriv rutinerna eller bifoga underlag där dessa framgår.
    b. Vem/vilken roll ansvarar för uppdateringen?

Underlaget ska ha inkommit till dataskyddsombudet **senast den 8 mars 2021.**

Har du frågor, kontakta ditt huvudansvariga dataskyddsombud.

Fördjupad kontroll 2022

Kontrollpunkt 7: Integritetspolicy (del 2)

Uppföljande frågor att besvara:

1. Omfattar den/de integritetspolicys som har skickats in/hänvisats till samtliga personuppgiftsbehandlingar som personuppgiftsansvarig utför och är skyldiga att informera om?
2. Om integritetspolicyn/de integritetspolicys som skickats in/hänvisats till inte är heltäckande, får de registrerade information om behandlingen/behandlingarna på annat sätt?
    a. Om ja, beskriv hur och ange den information som ges.
    b. Om nej, ange förklaring till varför information inte ges.
3. När man anställs hos Intraservice får man en bilaga med information om hur Intraservice hanterar anställdas personuppgifter. Ansvarar ni för den informationen och hur ofta uppdateras/ses den över?

Svar ska ha inkommit till dataskyddsombudet **senast den 8 juni 2022.**

Har ni frågor, kontakta ert huvudansvariga dataskyddsombud.