GRANSKNINGSRAPPORT

Dataskyddsförordningen, GDPR

PERSONUPPGIFTSANSVARIG

Samordningsförbundet Södra Vätterbygden

GRANSKAT OMRÅDE

Information till registrerade enligt art. 12-14

DATUM

2023-08-14

Erik Österberg
Dataskyddsombud
dso.finsam-svatterbygden@insatt.com

Insatt AB
Kyrkogatan 4
553 16 Jönköping

www.insatt.com

Sammanfattning av granskningsresultatet

- Sammanfattningsvis är dataskyddsombudets slutsats att det är positivt att det finns en Integritetspolicy upprättad samt att förbundet strävar efter att informera de registrerade i skikt/lager. En stor del av informationen ges muntligen, vilket förbundet visserligen inte behöver upphöra med. Däremot behöver den muntliga informationen kompletteras med skriftligen sammanställd information, dels för att de registrerade ska kunna gå tillbaka och åter ta del av informationen, dels för att förbundet lättare ska kunna leva upp till ansvarsskyldigheten.

- Den skriftliga information som finns upprättad, Integritetspolicyn, finns tillgänglig både internt för anställda och styrelsemedlemmar och på hemsidan för vem som helst. Integritetspolicyn är daterad och behöver kompletteras så att den lever upp till samtliga krav i artikel 13-14. Jag ser fördelar med att se över befintlig Integritetspolicyn och anpassa den för dess interna personuppgiftsbehandlingar (gällande anställda och styrelsemedlemmar) samt upprätta en ny fullständig informationstext för hemsidan för externa behandlingar (gällande webbplats- och sociala mediebesökare, eventbesökare, kandidater med flera).

- Förbundet behöver även jobba vidare med att informera i lager och skikt genom att tydligare hänvisa och länka tydligare till var den registrerade kan hitta kompletterande information. Detta gäller såväl webbplatsen som i e-postsignaturer med mera.

- Sammanfattningsvis rekommenderas samordningsförbundet att:

  - säkerställa att den information som ges kandidater, anställda och styrelsemedlemmar omfattar samtliga personuppgiftsbehandlingar av de registrerades personuppgifter före, under och efter anställningen/styrelseuppdraget,
  - (om det inte redan finns) upprätta en rutin för hantering av spontanansökningar och information till spontanansökare. Sådana ansökningar kan ju alltid komma in mejl-ledes till förbundet och behöver då hanteras,
  - se över befintlig Integritetspolicyn och anpassa den för dess interna personuppgiftsbehandlingar (gällande anställda och styrelsemedlemmar),
    - åtgärda felaktigheterna (som nämns under avsnitt 3.2) i Integritetspolicyn.
    - stämma av Integritetspolicyn med artikel 13-14 samt addera relevanta delar som saknas,
  - ta fram en ny fullständig informationstext för hemsidan för era externa behandlingar (gällande webbplats- och sociala mediebesökare, eventbesökare, kandidater med flera),
  - gällande e-postsignaturen, att säkerställa att informationstexten

- beskriver att kontakt med samordningsförbundet innebär behandling av personuppgifter där förbundet är personuppgiftsansvarig,
- begränsar att förbundet får in känsliga personuppgifter via e-post, och
- innehåller en länk till kompletterande information och de registrerades rättigheter exempelvis till extern personuppgifts-/integritetspolicy på hemsidan, samt

 i samband med prenumeration på nyheter från hemsidan, att säkerställa att

- ”första lagersinformation” med hänvisning till kompletterande information och de registrerades rättigheter förslagsvis till extern personuppgifts-/integritetspolicy på hemsidan tillhandahålls de registrerade, se vidare avsnitt 3.2.

- Jag råder förbundet att upprätta en plan för när åtgärderna ska vara genomförda.

Innehållsförteckning

1. Inledning

I rollen som dataskyddsombud ingår att övervaka organisationens efterlevnad av dataskyddsförordningen genom att bland annat samla in information om hur organisationen bedriver sin personuppgiftsbehandling, granska att organisationen följer bestämmelser och interna styrdokument samt att informera och ge råd inom organisationen.

Som en del av ovanstående uppdrag har en sådan granskning genomförts och dess resultat presenteras i den här rapporten.

1.1 Granskningens innehåll och begärda underlag

Granskningen omfattar den information den personuppgiftsansvarige enligt GDPR är skyldig att tillhandahålla de registrerade vars personuppgifter organisationen behandlar.

Granskningen utgår från följande underlag:

- den personuppgiftsansvariges svar i utskickat frågebatteri över vilken information som lämnas till de registrerade vars uppgifter den personuppgiftsansvarige behandlar, samt
- en av den personuppgiftsansvariges framtagna informationstexter som dataskyddsombudet valt för en kvalitativ granskning.

1.2 Syfte

Syftet med granskningen är att undersöka om den personuppgiftsansvarige dels

- informerar om personuppgiftsbehandlingar som sker inom de för verksamheten relevanta områdena[1], dels
- informerar de registrerade på ett begripligt och lättillgängligt sätt enligt art. 12 GDPR, dels
- lämnar fullständig information i enlighet med kraven i art. 13 och art. 14 GDPR,

För det fall den personuppgiftsansvarige tagit fram informationstexter är syftet vidare att genomföra en kvalitativ analys av en av dessa. För det fall det finns brister i de granskade underlagen ges dataskyddsombudets rekommendationer med förslag på förbättringsåtgärder gällande informationen till registrerade.

[1] Specifik information i särskilda situationer exempelvis vid personuppgiftsincidenter ligger utanför denna granskning.

1.3 Metod

Granskningen har genomförts i två delar. I den första delen har den personuppgiftsansvariges svar på frågorna i utskickat frågebatteri analyserats. I den andra har en kvalitativ analys av en utvald informationstext företagits. I denna del har samordningsförbundets Integritetspolicy (2018-11-19) valts ut för detta syfte.

Dataskyddsombudets analys och rekommendationer har sammanställts i denna rapport, vilken tillställs organisationen och dess ledning via förbundschefen.

1.4 Rapportens disposition

Innehållet i granskningsrapporten har ställts upp enligt följande. Under kapitel 2 återges en sammanfattning av rättsläget som också är den juridiska utgångspunkten för granskningen. I kapitel 3 återfinns själva granskningen, dess resultat och dataskyddsombudets rekommendationer. Avsnitt 3.1 innehåller en sammanfattning och analys av samordningsförbundets svar på utskickat frågebatteri och avsnitt 3.2 den kvalitativa analysen av förbundets informationstext.

2. Juridisk utgångspunkt för granskningen

Granskningen har genomförts med beaktande av dataskyddsförordningen:

- artikel 4.1 och 4.2: definition av personuppgifter och behandling,
- artikel 5: grundläggande principer inklusive ansvarsskyldigheten,
- artikel 12: krav på klar och tydlig information och kommunikation,
- artikel 13: information som ska tillhandahållas om personuppgifterna samlas in från den registrerade,
- artikel 14: information som ska tillhandahållas om personuppgifterna inte har erhållits från den registrerade, och
- artikel 24.1: krav att kunna visa att organisationen lever upp till kraven i GDPR,

Samt:

- Riktlinjer om öppenhet enligt förordning (EU) 2016/679, och
- Vägledande beslut från tillsynsmyndigheter och EU-domstolen.

2.1 Varför de registrerade ska informeras

En av de grundläggande principerna i GDPR är öppenhets- eller transparensprincipen. Denna kräver att information ges de registrerade på ett begripligt och lättillgängligt sätt. Att vara transparent med hur de registrerades personuppgifter behandlas bidrar till att medborgarna får större förståelse för behandlingen och skapar tillit. Samtidigt möjliggör öppenheten för

medborgarna att bestrida och invända mot processer och personuppgiftsbehandlingar. Enligt den grundläggande principen om ansvarsskyldighet (artikel 5.2) måste den personuppgiftsansvarige alltid kunna visa att personuppgifterna behandlas på ett öppet sätt gentemot den registrerade.

Kraven som åligger den personuppgiftsansvarige för att löpande ge information framgår av artiklarna 12–14. Öppenhetskravet måste följas oavsett vilken rättslig grund som behandlingen grundas på samt under hela behandlingens löptid. Det följer av art. 12 att öppenhet ska iakttas vid följande skeden i behandlingen:

- Innan eller när behandlingen av personuppgifter inleds, det vill säga när personuppgifterna inhämtas antingen från den registrerade eller från annat håll.
- Under hela behandlingen, det vill säga vid kommunikation med registrerade om deras rättigheter.
- Vid särskilda tillfällen under pågående behandling, till exempel vid personuppgiftsincidenter eller vid väsentliga förändringar i behandlingen.

2.2 Vad de registrerade ska informeras om

De registrerade ska få information om vem som behandlar deras personuppgifter, det vill säga identiteten och kontaktuppgifterna till den personuppgiftsansvarige samt kontaktuppgifter till dataskyddsombudet om en sådan har utsetts. Informationen ska även innehålla uppgifter om ändamålet med behandlingen, den rättsliga grunden för behandlingen, om behandlingen baserats på en intresseavvägning (art. 6.1 (f)), vilka som kommer ta del av personuppgifterna samt om den personuppgiftsansvarige avser överföra personuppgifterna till tredjeland (i det senare fallet ska även de registrerade få information om använd överföringsmekanism och vidtagna skyddsåtgärder).

Ytterligare information som ska förmedlas till de registrerade är bland annat hur länge personuppgifterna kommer lagras alternativt vilka kriterier som används för att avgöra detta, information om de registrerades rättigheter enligt GDPR, att inhämtat samtycke kan återkallas samt rätten att inge klagomål om behandlingen till tillsynsmyndigheten (Integritetsskyddsmyndigheten).[2]

2.3 När de registrerade ska informeras

Information om behandlingen ska tillhandahållas de registrerade när behandlingen påbörjas. Då personuppgifter inhämtas direkt från den registrerade, exempelvis om en registrerad medvetet lämnar information till personuppgiftsansvarig genom att fylla i ett formulär på internet, ska informationen ges när personuppgifterna erhålls. Om personuppgifter inhämtas från andra källor än den registrerade själv, exempelvis allmänt tillgängliga källor, andra registrerade eller personuppgiftsansvariga i egenskap av tredje part, måste

[2] Se vidare artikel 13-14.

informationen lämnas inom en månad. Denna tidsfrist kan dock vara kortare beroende på hur personuppgifterna behandlas. I det fall personuppgifterna används för att kunna kommunicera med den registrerade måste information om behandlingen lämnas senast i samband med den första kommunikationen med den registrerade. Ofta sker den första kontakten via e-post, varför förstalagersinformation[3] med fördel ges i medarbetarnas e-postsignatur med kortfattad information om behandlingen av personuppgifter samt en hänvisning till fullständig information innehållandes rättigheter med mera.

2.4 Hur de registrerade ska informeras

Enligt artikel 12.1 ska informationen tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Vidare framgår även att informationen eller kommunikationen måste vara i en koncis, klar, tydlig, begriplig och lättillgänglig form. Informationen bör presenteras på ett effektivt och kortfattat sätt i syfte att inte överväldiga och utmatta den registrerade med för mycket information på en och samma gång. Att informera den registrerade i olika lager samt att dela upp (det externa) integritetsmeddelandet i skikt förespråkas för att undvika denna problematik. I regel finns stora fördelar med att dela upp informationen som ges internt respektive externt. Detta görs ibland i en intern integritetspolicy och ett externt integritetsmeddelande online (extern integritetspolicy).

2.4.1 Att informera i lager

Vid den första behandlingen av den registrerades personuppgifter behöver den personuppgiftsansvarige säkerställa att registrerade får ett första lager av information om vilka personuppgifter som behandlas och för vilket ändamål, den personuppgiftsansvariges identitet samt hur man får tillgång till den fullständiga informationen (det andra eller tredje lagret). I det andra lagret bör nödvändig informationen ges om den registrerades rättigheter samt information om den behandling som mest påverkar den registrerade och sådan behandling som skulle kunna komma som en överraskning för den registrerade. Det andra lagret kan vara det sista lagret och ska då inkludera komplett information såsom laglig grund för behandlingen, hur länge personuppgifterna sparas och övrig information som krävs enligt art. 13 och 14 GDPR. Alternativet är att samla den kompletta informationen för sina samtliga behandlingar i ett tredje informationslager. I så fall ska det andra lagret innehålla en hänvisning så att den registrerade enkelt kan ta del av den ytterligare informationen om personuppgiftsbehandlingen i det tredje lagret. Det sista lagret utgörs ofta av ett integritetsmeddelande online (extern integritetspolicy). Rekommendationen är att skikta integritetspolicyn.

[3] Se vidare avsnitt 2.4.

2.4.2 Skiktad integritetspolicy

Oavsett om den fullständiga informationen ges i ett andra eller tredje lager rekommenderar Europeiska dataskyddsstyrelsen (EDPB)[4] att dela upp informationen i skikt. För att undvika att utsätta de registrerade för informationsutmattning är rekommendationen framför allt att skiktade integritetspolicyer/integritetsmeddelanden bör användas för att länka till de olika kategorier av information som måste ges till de registrerade, i stället för att ge all sådan information i ett och samma meddelande. Integritetspolicyns första skikt bör vara utformat så att de registrerade får en tydlig översikt över den information som finns om behandlingen av deras personuppgifter och var/hur de kan finna denna utförliga information bland policyns olika skikt. Ett sätt att undvika informationsöverflöd, skapa översikt och göra det enkelt för den registrerade att direkt kunna gå till det avsnitt i policyn som denne vill läsa är att dela upp integritetspolicyn i ”klickbara” rubriker. Vad gäller innehållet rekommenderar EDPB att det första skiktet inkluderar uppgifter om behandlingens ändamål, den personuppgiftsansvariges identitet, en beskrivning av den registrerades rättigheter samt information om den behandling som mest påverkar den registrerade och sådan behandling som skulle kunna komma som en överraskning för denne.

2.4.3 Språk och målgrupp

För att uppfylla kravet på ett klart och tydligt språk ska informationen ges på ett så enkelt sätt som möjligt. Undvik komplicerade meningar och språkstrukturer. Det är också viktigt att informationen är så konkret och exakt som möjligt samt att informationen inte är motstridig. Bland annat rekommenderas det att inte använda benämningsord som ”eventuellt”, ”kan” och ”ofta”. Detta syftar till att undvika tolkningsmöjligheter för den registrerade som, enligt art. 13–14, ska få ta del av information om hur deras personuppgifter faktiskt behandlas.

Informationen måste anpassas till den målgrupp som den riktar sig till. Det gäller också i förhållande till barn och andra utsatta personer. Dessa kategorier av registrerade anses vara extra skyddsvärda enligt dataskyddsförordningen då de kan ha svårare att förstå innebörden av informationen, förutse riskerna med att lämna ifrån sig uppgifter och förstå vilken rätt till skydd för sina uppgifter de har. Nivån på informationen bör anpassas utifrån exempelvis ett barns ålder men om det anses motiverat kan informationen lämnas till en vårdnadshavare, god man eller förvaltare som å sina barns eller å annans vägnar har en skyldighet att tillvarata den skyddsvärde individens rättigheter.

3. Granskningen

Resultatet av granskningen av den personuppgiftsansvariges information till registrerade utifrån kraven i GDPR visar följande.

[4] Tidigare Artikel 29-gruppen.

3.1 Resultat från granskning av den personuppgiftsansvariges svar i frågebatteriet

Frågeformuläret som skickades till den personuppgiftsansvarige bestod av ett antal informationskategorier. Dessa var:

- anställning,
- rekrytering,
- spontanansökningar,
- särskilt riktad information utifrån kärnverksamheten,
- webbplatsen,
- sociala medier,
- event/mässor,
- kamerabevakning, och
- övrigt (exempelvis e-postsignatur, nyhetsbrev, marknadsföring med mera).

Dessa kategorier har nedan delats upp i olika avsnitt för närbesläktade kategorier av registrerade. Exempelvis har information vid anställning och rekrytering lagts ihop under avsnitt 3.1.1.

3.1.1 Information till anställda, potentiella arbetstagare och spontanansökare

Samordningsförbundet har i huvudsak uppgett följande. Information om förbundets personuppgiftsbehandling ges dels till anställda, dels kandidater vid rekrytering och informationen lämnas främst muntligen. Skriftlig information lämnas främst genom hänvisning till lättillgängliga styrdokument och rutiner, men viss skriftlig GDPR-information återfinns även i rekryteringsannonser för tjänster. Möjligheten till spontanansökningar finns inte och är därför inte aktuellt. Av svaren framgår vidare att förbundet till viss del informerar i skikt/lager och att samtycken som inhämtas främst är muntliga.

Slutsats

Att viss information om personuppgiftsbehandling lämnas till grupper av registrerade såsom anställda och kandidater samt att förbundet strävar efter att informera i skikt/lager är positivt. Att merparten av informationen ges muntligen är jag däremot kritisk till. Även om informationen kan ges muntligen så länge den är koncis, klar, tydlig, begriplig och lättillgänglig är huvudregeln enligt artikel 12.1 att den (även) ska ges skriftligen. Dessutom ser jag fördelar utifrån ansvarsskyldigheten att informationen även finns tillgänglig för de registrerade i skriftlig form. Genom att tillhandahålla kandidater och anställda skriftlig information om personuppgiftsbehandlingen i samband med rekryteringsförfarandet och anställningen (be)visar förbundet på ett mycket tydligare sätt att det informerar de registrerade samt att informationen uppfyller kraven i art. 12-14 GDPR. Fördelarna med skriftlig form gäller även vid eventuellt inhämtande av samtycke från anställda/kandidater. Tänk även på att det ofta är

problematiskt för arbetsgivare att använda samtycke som laglig grund för behandling av arbetstagarnas personuppgifter med tanke på det beroendeförhållande som i regel finns mellan dessa och välj om möjligt annan laglig grund eller avstå från behandlingen.

Av de styrdokument jag tagit del av (Integritetspolicy och Informationssäkerhetspolicyn) inom ramen för granskningen framgår inte tillräckligt tydliga beskrivningar av vilka personuppgiftsbehandlingar som görs, för vilka ändamål, med vilka lagliga grunder, de registrerades rättigheter med mera. Sådan information kanske återfinns i andra informationstexter eller ges muntligen till de registrerade, men jag har utgått från att den saknas så att detta inte förbises. Som framgår under avsnitt 3.2 rekommenderar jag förbundet att behålla ”Integritetspolicy”, se över den och anpassa den så att den uppfyller kraven på information till de registrerade som finns internt (anställda och styrelsemedlemmar). Denna informationstext behöver nödvändigtvis inte ligga tillgänglig för alla på hemsidan.

Det noteras också att ”Informationssäkerhetspolicyn” inte finns tillgänglig på hemsidan med hänvisning till att sådan ska komma att beslutas av styrelsen inom kort. Informationstexten är däremot redan fastställd av styrelsen. Denna informationstext behöver nödvändigtvis inte ligga tillgänglig för alla på hemsidan, då informationen främst riktar sig internt.

Dataskyddsombudet rekommenderar förbundet att

- säkerställa att den information som ges kandidater och anställda omfattar samtliga personuppgiftsbehandlingar av de registrerades personuppgifter före, under och efter anställningen,
- säkerställa att den information som ges kandidater och anställda omfattar för vilka ändamål och med vilka lagliga grunder deras personuppgifter behandlas, de registrerades rättigheter med mera (enligt artikel 13-14 GDPR),
- tillse att informationen som ges enligt punkterna ovan finns tillgänglig för de registrerade i skriftlig form, förslagsvis i ”Integritetspolicyn” samt
- (om det inte redan finns) upprätta en rutin för hantering av spontanansökningar och information till spontanansökare. Sådana ansökningar kan ju alltid komma in mejl-ledes till förbundet och behöver då hanteras.
- Överväg om ”Informationssäkerhetspolicyn” ska ligga tillgänglig på hemsidan och i förekommande fall, gör den tillgänglig.

3.1.2 Information riktad till särskilda mottagare utifrån kärnverksamheten

Samordningsförbundet har i huvudsak uppgett att ge särskilt riktad information utifrån kärnverksamheten (till kunder, medborgare, elever, brukare, förtroendevalda m.fl) inte är aktuellt.

Slutsats
Som jag har förstått det sker ingen personuppgiftsbehandling vad gäller de individer som är föremål för samordningsförbundets hjälpinsatser. Så långt delar jag förbundets slutsats att någon information till dessa inte ska ske och inte kan ske eftersom förbundet inte vet och inte ska veta vilka individer som i slutändan tar del av insatserna. Däremot utgörs förbudets styrelse av företrädare för respektive medlem (förtroendevalda), vars personuppgifter förbundet behandlar. Därför ska även denna grupp registrerade informeras om hur och för vilka ändamål deras personuppgifter behandlas.

Dataskyddsombudet rekommenderar förbundet att

- säkerställa att den information som ges styrelsemedlemmar (förtroendevalda) omfattar samtliga personuppgiftsbehandlingar av deras personuppgifter före, under och efter styrelseuppdraget,
- säkerställa att den information som ges styrelsemedlemmar (förtroendevalda) omfattar för vilka ändamål, med vilka lagliga grunder och med vilka lagliga grunder deras personuppgifter behandlas (enligt artikel 13-14 GDPR), samt
- tillse att informationen som ges enligt punkterna ovan finns tillgänglig för de registrerade i skriftlig form, förslagsvis i ”Integritetspolicy”.

3.1.3 Information till webbplatsbesökare, besökare på sociala medier och event/mässor

Samordningsförbundet har i huvudsak uppgett följande. Förbundet informerar i skikt/lager dels vid första besöket på hemsidan genom en pop-up-ruta med länk till integritetspolicy, dels när webbplatsbesökaren ämnar fylla i kontaktformulär. Beträffande sociala medier är det inte aktuellt att lämna de registrerade information eftersom vare sig Facebook eller LinkedIn används för kommunikation. Vid event och mässor lämnas information till de registrerade och i skikt/lager beroende på målgrupp (styrelse, beredningsgrupp eller bredare målgrupp).

Slutsats
Angående webbplatsen är det positivt att förbundet försöker informera i skikt/lager. Däremot saknar jag länkar till integritetspolicyn i anslutning till dels Om integritet och cookies - Samordningsförbunden Jönköping län (finsamjonkopingslan.se), dels sidan för kontaktformulär. Beträffande sociala medier ställer jag mig frågande till svaret om att information till de registrerade inte skulle behövas eftersom de sociala medie-kontona inte används för kommunikation. Det ligger i sociala-mediekontonas natur att personer kan kontakta förbundet samt interagera och kommentera inlägg. Vid sådan interaktion behandlar förbundet personuppgifter för vilka det är personuppgiftsansvarigt, varför information krävs.

Dataskyddsombudet rekommenderar förbundet att

- infoga länkar till rekommenderad ny sistalagers-informationstext (se nedan under 3.2) vid i samband med insamling av personuppgifter,
- lägga till information om förbundets behandling av personuppgifter i sociala medier-kanaler i rekommenderad ny extern sistaslagers-informationstext (se nedan under 3.2).

3.1.4 Övrig information

Samordningsförbundet har i huvudsak uppgett följande. Kamerabevakning eller marknadsföring förkommer inte. Förbundet informerar de registrerade i skikt/lager i bland annat e-postsignaturer, prenumeration på nyheter samt vid inspelning av filmer (exempelvis Samverkanskoppen).

Slutsats

Dataskyddsombudets slutsats är att det finns utvecklingspotential vad gäller information i det första lagret såsom e-postsignatur och vid prenumeration på nyheter från hemsidan.

Dataskyddsombudet rekommenderar förbundet

- gällande e-postsignaturen, att säkerställa att informationstexten
  - beskriver att kontakt med samordningsförbundet innebär behandling av personuppgifter där förbundet är personuppgiftsansvarig,
  - begränsar att förbundet får in känsliga personuppgifter via e-post, och
  - innehåller en länk till kompletterande information och de registrerades rättigheter exempelvis till extern personuppgifts-/integritetspolicy på hemsidan,
- i samband med prenumeration på nyheter från hemsidan, att säkerställa att
  - ”första lagersinformation” med hänvisning till kompletterande information och de registrerades rättigheter förslagsvis till extern personuppgifts-/integritetspolicy på hemsidan tillhandahålls de registrerade, se vidare 3.2.

3.2 Kvalitativ analys av en informationstext

För den kvalitativa analysen har styrdokumentet ”Integritetspolicy” daterat 2018-11-19 (hädanefter benämnd ”Integritetspolicyn”) valts.

3.2.1 Generellt Integritetspolicyn

I majoriteten av förbundets övriga informationstexter i tidigare lager hänvisas de registrerade vidare till Integritetspolicyn som finns tillgänglig på förbundets webbplats. Det är också till den

webbplatsbesökare slussas via länken ”Om integritet och cookies” fäst längst ned på webbplatsen under rubriken ”Information”. Som det får förstås utgör denna information det sista lagret av information som de registrerade kan ta del av när det gäller förbundets behandling av personuppgifter.

Slutsats

Beaktat att jag som registrerad inte förstår vilka personuppgifter som behandlas för vilka ändamål, med vilken laglig grund med mera, vissa direkta felaktigheter samt flera brister i Integritetspolicyn, kan den inte tillfyllest anses uppfylla den personuppgiftsansvariges informationsskyldighet gentemot de registrerade, se vidare avsnitt 3.2.2–3.2.3 nedan. Samtidigt vill jag betona att innehållet i aktuell Integritetspolicy till stor del utgör relevant information om att och hur anställda (och även styrelsemedlemmar) ska värna de registrerades integritet vid förbundets personuppgiftsbehandling. Med tanke på att Integritetspolicyn upprättades för snart 5 år sedan, den rättsutveckling[5] som därefter skett samt att kraven nu är tydligare för vad den personuppgiftsansvarige är skyldig att informera om, är min övergripande rekommendation att se över Integritetspolicyn och anpassa den för interna personuppgiftsbehandlingar (anställda och styrelsemedlemmar) samt ta fram en ny informationstext för hemsidan för externa behandlingar (webbplats- och sociala mediebesökare, eventbesökare, kandidater med flera).

”Integritetspolicy”, ”Externt integritetsmeddelande”, ”Extern personuppgiftspolicy”, ”GDPR-information”, ”Information om personuppgiftsbehandling”, ”Privacy policy” – kärt barn har många namn, vilket inte sällan leder till begreppsförvirring. Oavsett vad förbundet väljer att kalla informationen till de registrerade saknar jag en lättillgänglig och begriplig fullständig sistalagers-informationstext på hemsidan som innehåller de delar som krävs enligt artikel 13-14 GDPR. Därför rekommenderar jag att förbundet tar fram en Informationstext som gör att jag som registrerad förstår hur mina personuppgifter hanteras i de olika personuppgiftsbehandlingarna. Exempelvis, för behandlingen ”prenumeration på nyheter”, behandlar vi din e-postadress för ändamål X, med den lagliga grunden Y och sparar den i Z månader mer mera. Informationstexten delas således med fördel upp per behandling. Texten ska bland annat ange ändamålet med behandling och vilken rättslig grund som behandlingen baseras på, eventuella mottagare av personuppgifterna, eventuell tredjelandsöverföring, lagringstid, de registrerades möjlighet att inge klagomål till tillsynsmyndigheten och de registrerades samtliga rättigheter med mera[6].

Dataskyddsombudet rekommenderar förbundet att

- se över befintlig Integritetspolicyn och anpassa den för dess interna personuppgiftsbehandlingar (gällande anställda och styrelsemedlemmar), samt

[5] Se bland annat Klarna Bank AB, bristande information (imy.se) från 2022.
[6] Artikel 13-14 GDPR.

- ☐ ta fram en ny fullständig informationstext för hemsidan för externa behandlingar (gällande webbplats- och sociala mediebesökare, eventbesökare, kandidater m.fl.).

3.2.2 Felaktigheter i Integritetspolicyn

Felaktigheter i befintlig Integritetspolicy som behöver åtgärdas är följande.

- Under rubriken ”Dataskyddsorganisation” anges att
  - ”Styrelsen för Samordningsförbundet Södra Vätterbygden är personuppgiftsansvarig för förbundet”. Det är samordningsförbundet som är personuppgiftsansvarigt i egenskap av myndighet. Styrelsen och dess medlemmar företräder visserligen förbundet, men kan när det kommer till dataskydd inte hållas personligen ansvariga för förbundets personuppgiftsbehandlingar.
  - ”Datainspektionen” har bytt namn till Integritetsskyddsmyndigheten (IMY).

Dataskyddsombudet rekommenderar förbundet att

- ☐ Åtgärda felaktigheterna (som nämns ovan) i Integritetspolicyn.

3.2.3 Brister i Integritetspolicyn

Som redan nämnts ovan är Integritetspolicyn daterad och saknar viktiga delar i förhållande till kraven i artikel 13-14 GDPR. Bland de delar som saknas ska följande nämnas:

- Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen,
- Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall,
- I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland, om adekvat skyddsnivå föreligger, hänvisning till lämpliga skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga,
- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period,
- Att det föreligger en rätt för de registrerade att begära rättelse eller begräsning och att invända mot behandling, och
- Rätten att inge klagomål till en tillsynsmyndighet

Dataskyddsombudet rekommenderar förbundet att

- ☐ Stämma av Integritetspolicyn med artikel 13-14 samt addera relevanta delar som saknas.

4. Bilageförteckning

Bilaga 1 Integritetspolicy 2018-11-19

Samordningsförbund Södra Vätterbygden
c/o Jönköpings kommun
Tändsticksgränd 23
551 89 Jönköping
Mobil: 072-741 58 00
E-post: samordning.sv@jonkoping.se

Integritetspolicy

Behandling av personuppgifter hos Samordningsförbundet Södra Vätterbygden

Bakgrund

Samordningsförbundet Södra Vätterbygden är ett samordningsförbund enligt lagen om finansiell samordning (lag 2003:1210).

Den 25 maj 2018 trädde dataskyddsförordningen som kallas GDPR (General Data Protection Regulation) i kraft i Sverige och övriga EU. Den ersatte då personuppgiftslagen (PuL).

Samordningsförbundet har sett över och systematiserat sina rutiner för hur vi hanterar personuppgifter, så att vi uppfyller GDPR.

Detta dokument med bilagor beskriver förbundets integritetspolicy samt hur via arbetar med dataskydd och personuppgifter.

Med personuppgift menar vi all slags information som är lagrade elektroniskt som kan knytas till en fysisk person som är i livet. Exempelvis personnummer, namn, adress, behov av specialkost, foton och filmer.

Hantering av personuppgifter

Samordningsförbundet värnar varje människas okränkbara, lika värde och rätt till integritet.
De personuppgifter vi hanterar berör anställda och ledningsgrupper inom förbundet och insatser som förbundet finansierar, kontaktuppgifter inom Arenasamverkan och andra samverkansgrupper, personer som bjuds in till och anmäler sig till evenemang samt uppgifter på hemsidan och i mailkontakter.

Samordningsförbundet följer GDPR med gällande lagstiftning i Sverige för hantering av personuppgifter.

För att förbundet ska uppfylla regelverket:

- samlar vi bara in personuppgifter som krävs för verksamheten och som det finns rättslig grund för att samla
- lagrar vi nödvändiga personuppgifter i väl specificerade former
- lagrar vi personuppgifterna på ett säkert sätt enligt förbundets Informationssäkerhetspolicy
- finns det en utsedd kontaktperson för behandlingen av uppgifterna (förbundschefen)
- har styrelsen utsett ett dataskyddsombud (se nedan)

Vi för ett register över samtliga våra persondatabehandlingar, en registerförteckning. Av förteckningen framgår vem som är registeransvarig, beskrivning av databehandling, varför vi samlar in och lagrar persondata,

tidsbegränsning för lagring av persondata, rensningsrutin, vilken rättslig grund som persondatabehandlingen åberopar samt vilka personuppgiftsbiträden förbundet anlitar.

Dataskyddsorganisation

Styrelsen för Samordningsförbundet Södra Vätterbygden är personuppgiftsansvarig för förbundet, ett ansvar som inte kan delegeras.

Styrelsen har utsett ett dataskyddsombud (DSO) som fungerar som en internrevisor när det gäller behandling av personuppgifter inom förbundet och som även har kontakten med Datainspektionen. Kontaktuppgifterna till DSO finns bl a angivna på förbundets hemsida.

Styrelsen har utsett förbundschef till att vara företrädare för styrelsen vad gäller personuppgiftshanteringen.

Förbundet har personuppgiftsbiträdesavtal med externa tjänsteleverantörer som vi anlitar. I avtal regleras att de följer dataskyddsförordningen och gällande lagstiftning.

Till vad används personuppgifter som vi samlat in?

Uppgifterna används för särskilda uttryckligt angivna och berättigade ändamål. Det betyder att uppgifter som samlas in för ett visst redovisat syfte inte får användas för helt andra syften.

Vi samlar in personuppgifter för att kunna sprida information och kommunikation om förbundet, arrangemang och verksamheter vi finansierar, för uppföljning, tjänstetillsättningar, löne- och arvodeshantering, uppgifter till skattemyndigheter och Försäkringskassan, annan personaladministration och ekonomihantering.

Riktlinjer och rutiner

Hur vi samlar in personuppgifter och hanterar dem

Vi samlar in personuppgifter genom anmälningar till evenemang eller begäran om information, genom anmälan av valda representanter till ledningsgrupper (styrelsen, beredningsgrupp, styrgrupper mm), anmälan av utsedda representanter i Arenasamverkan, anställningar i förbundet och av förbundet finansierade verksamheter hos parterna och i mail som skickas till förbundet.

För de persondata som kräver samtycke, så ges samtycket i samband med anmälning/beställning. Förbundet hanterar inga uppgifter om deltagare i verksamheter som finansieras av förbundet.

I förbundets registerförteckning anges hur och på vilken rättslig grund som data sparas och hur samtycke ges (där så krävs). Ingen i förbundet får samla in personuppgifter utan förbundschefens godkännande.

Lagring

Var de insamlade uppgifterna lagras beror på reglerna för respektive register. Detsamma gäller tiden för hur länge uppgifterna kommer att lagras. Faktorer som kan påverka lagringstiden är oftast lagar, exempelvis bokföringslagen och arkivlagen.

Samordningsförbundet lagrar aldrig personuppgifter längre än vad som behövs. Lagringstiderna för respektive persondatabehandling framgår av registerförteckningen. Där framgår även om det sker automatisk radering av data efter en viss tid.

Rätten att bli bortglömd

Var och en som är registrerad har rätt att få tillgång till sina uppgifter och få felaktiga uppgifter rättade. Man har också rätt att ta tillbaka sitt samtycke till insamling och, om inga lagliga hinder finns, få sina uppgifter raderade.

Lagring och säkerhet

Samtliga anställda ska följa förbundets Informationssäkerhetspolicy och de säkerhetsåtgärder som finns beskrivna där.

För personuppgiftsbiträden som förbundet anlitar regleras lagring och säkerhet i avtal som innebär att biträdet uppfyller GDPR och gällande lagstiftning.

Relaterade dokument:

- Registerförteckning (uppdateras löpande av förbundschef)
- Samordningsförbundet Södra Vätterbygdens Informationssäkerhetspolicy

Styrelsen fastställde policyn 2018-11-19