Livsmedelsarbetareförbundets policy för dataskydd och informationssäkerhet gällande behandling av personuppgifter enligt General Data Protection Regulation (GDPR)

2018

Innehåll

1. Inledning

Personuppgiftslagen (1998:204) har till syfte att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas. I maj 2018 träder ett nytt motsvarande regelverk i kraft i form av EUs nya dataskyddsförordning GDPR.

Det är upp till Livsmedelsarbetareförbundet (Livs) att se till att lagar och regler följs i samband med att förbundet behandlar olika former av personuppgifter. Av denna anledning är det nödvändigt att förbundet vet hur medlemmars och anställdas personuppgifter behandlas.

- **Vad** förbundet behandlar för typ av personuppgifter
- **Varför** förbundet behandlar dessa personuppgifter
- **Hur** förbundet behandlar personuppgifter
- **Vem** som behandlar personuppgifter
- **Var** förbundet behandlar personuppgifter.

Denna policy innehåller information och anvisningar som gäller alla som behandlar personuppgifter inom Livs. Detta dokument är inte heltäckande utan ska ses som en vägledning och där enskilda fall, som faller utanför den här generella genomgången alltid måste prövas mot GDPR. Förbundet har ett dataskyddsombud som ska rådfrågas i god tid innan personuppgifter behandlas utanför nedan angivna riktlinjer eller vid tveksamheter.

2. Terminologi

Behandling

Begreppet behandling är brett och omfattar allt som görs med personuppgifter så som insamling, registrering, lagring, utskrift och spridning.
Livs behandlingar av personuppgifter samlas i ett behandlingsregister.

Personuppgift

Personuppgift är den eller de uppgifter som direkt eller indirekt kan identifiera en fysisk levande person. Exempel på personuppgift är personnummer, namn, adress, telefonnummer, mailadress, IP-adress och cookies.

Känslig, särskild kategori av personuppgift

Om det till en eller flera personuppgifter läggs på ett känsligt attribut som exempelvis fackligt medlemskap, blir det en känslig personuppgift.

Övriga känsliga personuppgifter är sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse samt personuppgifter som rör hälsa eller sexuell läggning.

Behandlingen av känsliga personuppgifter lyder under striktare regler än behandling av personuppgifter i övrigt.

Laglig grund för behandling av personuppgifter

Med laglig grund menas vilket rättsligt stöd förbundet har för att behandla personuppgifter i förhållande till de ändamål som personuppgifterna i varje enskilt fall behandlas för. De vanligaste lagliga grunderna för behandling av personuppgifter är:

- Samtycke
- Nödvändigt för att fullgöra ett avtal eller en rättslig förpliktelse
- Skydda intressen av grundläggande betydelse för den registrerade eller annan fysisk person
- Intresseavvägning - när den personuppgiftsansvariges berättigade intresse väger tyngre än den registrerades grundläggande rättigheter och friheter.

Personuppgiftsansvarig
Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med, och medlen för, behandling av personuppgifter.

Livs betraktar ur ett GDPR perspektiv hela organisationen (förbund, regioner och klubbar) som ett personuppgiftsansvarsområde. Ombudsman, administrativ personal eller förtroendevald som behandlar personuppgifter inom ramen för sin anställning, roll eller sitt uppdrag gör det för personuppgiftsansvarigs räkning men övertar inte personuppgifts-ansvaret.

Personuppgiftsbiträde
Ett personuppgiftsbiträde, exempelvis en (extern) tjänsteleverantör, är den som inom ramen för utförandet av sitt uppdrag behandlar personuppgifter för den personuppgiftsansvariges räkning.

Dataskyddsombud
Dataskyddsombudets uppgift är att verka för att personuppgifter behandlas på ett korrekt och lagligt sätt inom organisationen. Dataskyddsombudet följer all behandling av personuppgifter inom den personuppgiftsansvariges område.

Tredje man
Tredje man är någon annan än den registrerade, den personuppgiftsansvarige, dataskyddsombudet, personuppgiftsbiträdet eller person som har befogenhet att behandla personuppgifter för organisationen.

3. Registrerades rättigheter
Medlemmar och anställda informeras om rättslig grund och ändamål för förbundets behandling av personuppgifter, hur länge personuppgifterna lagras och möjligheten att för den som anser att personuppgifter hanterats felaktigt lämna klagomål till Datainspektionen. Informationen ska vara kortfattad, lättbegriplig och tydlig.

De registrerade har rätt att få tillgång till sina uppgifter, få uppgifter rättade, raderade eller flyttade.

Dessa rättigheter kan inte förvägras den registrerade med mindre än att denne inte kan identifieras. Om det finns rimliga skäl att betvivla identiteten hos en person som begär viss rättighet ska ytterligare information begäras från berörd person så att identitet kan fastställas.

Begärd information ska lämnas inom en månad. Tiden för handläggning kan förlängas med två månader om begäran är komplicerad eller antalet inkomna begäranden är stort. Vid förlängning av tid underrättas den registrerade.

Få tillgång till sina uppgifter
Den registrerade har rätt att en gång per år kostnadsfritt få ett registerutdrag på vilka uppgifter förbundet har registrerat på personen i fråga. För att säkerställa den registrerades identitet måste beställning av ett registerutdrag ske per brev och vara undertecknat av den registrerade.

Genom Mina sidor på förbundets hemsida ges den registrerade tillgång till sina personuppgifter och möjlighet att rätta dem samt få information om vilka behandlingar som görs.

Observera att begärt registerutdrag inte får innehålla personuppgifter om andra personer.

Livs tillhandahåller två former av registerutdrag, ett allmänt och ett särskilt registerutdrag.

Det allmänna registerutdraget innehåller namn, personnummer, medlemsnummer, adress, e-post, telefonnummer, arbetsgivare, anställning, inkomst, kontonummer för autogiro alternativt andra betalsätt, typ av medlemskap och eventuellt fackligt uppdrag.

Särskilt registerutdrag används då begäran om registerutdrag berör förhandlings-, rättsskydds- eller försäkringsärenden. I de fall särskilt registerutdrag tas fram ska ansvarig handläggare kontaktas. Ansvarig handläggare säkerställer att underlaget inte innehåller personuppgifter rörande andra personer och skickar sedan informationen rekommenderat till berörd medlem.

Få felaktiga personuppgifter rättade
En registrerad ska kunna få sina uppgifter rättade genom att kontakta organisationen. Rättningen ska göras i alla led d v s har förbundet skickat felaktiga uppgifter vidare är det förbundets ansvar att se till att även dessa rättas.

Få sina personuppgifter raderade
En utträdd medlem eller anställd som slutat sin anställning i organisationen har rätt att få sina uppgifter raderade, har rätt att bli glömd. Detta gäller under förutsättning att de behandlade personuppgifterna inte längre behövs med tanke på ändamålet och att annan laglig grund inte finns.

En anmälan om radering ska ske per brev och vara undertecknad av den berörda.

Dataportabilitet – flytta personuppgifter från en organisation till en annan
Uppgifter som ska lämnas över till den registrerade eller flyttas till annan personuppgiftsansvarig ska vara i ett allmänt och maskinläsbart format och ske via säker överföring. Detta gäller till exempel vid övergång till annat förbund.

4. Regler för behandling av känsliga personuppgifter

GDPR gäller all form av behandling av personuppgifter oavsett om det sker i exempelvis register, löpande text, e-mail, ljud eller bild.

Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade
Det är som utgångspunkt inte tillåtet att behandla personuppgifter som avslöjar fackligt medlemskap. Trots förbudet är det tillåtet i kombination med de grundläggande principerna att behandla känsliga personuppgifter i följande fall:

Samtycke eller i vissa fall offentliggörande (när den registrerade själv har offentliggjort sina känsliga uppgifter).

Nödvändig behandling - för att den personuppgiftsansvarige ska kunna fullgöra sina skyldigheter eller nyttja sina rättigheter inom arbetsrätten, skydda den registrerades vitala intressen och rättsliga anspråk. Detta följer av unionsrätt, nationell rätt eller kollektivavtal.

Berättigad verksamhet - fackliga organisationer får inom ramen för sin verksamhet behandla känsliga personuppgifter, förutsatt att behandlingen rör medlemmar, tidigare medlemmar eller anställda i organisationen. Behandlingarna ska genomföras med lämpliga skyddsåtgärder.

Uppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett annat sätt
Att samla in information som innehåller personuppgifter bara för att den är bra att ha är inte tillåtet. All insamling och behandling av personuppgifter behöver kunna motiveras utifrån en laglig grund. När ändamålet är definierat får personuppgifterna inte behandlas på ett annat sätt utan att först fastställa en laglig grund för den nya behandlingen.

I samband med medlemsinträdet ger medlemmen fullmakt/medgivande till förbundet och informeras samtidigt om att Livs använder personuppgifterna till följande ändamål:

- Vidarebefordran av inträdesansökan till Livsmedelsarbetarnas A-kassa
- Att lämnade personuppgifter registreras och används i syfte att tillvarata medlemmens intresse och har samband med medlemskapet
- Att personuppgifterna vid utträde på grund av övergång lämnas till det nya förbundet.

Tidigare medlemmar kan ta del av information om hur deras personuppgifter behandlas på förbundets hemsida www.livs.se.

Behandling som faller utanför ovanstående kan vara otillåten.

Uppgifter ska vara adekvata, relevanta och inte för omfattande
De uppgifter som behandlas ska vara nödvändiga för arbetet. Person- eller medlemsnummer bör bara användas när det är motiverat, då det är viktigt med en säker identifiering som exempelvis vid anställning, inträde, utträde eller förhandling. Om personnummer inte behövs för att utföra en uppgift får det inte ingå.

Uppgifter ska vara korrekta och aktuella
Förbundet har ett ansvar för att de uppgifter som behandlas är korrekta. För att säkerställa detta används SPAR-uppdateringar och BISnode. Medlemmar ges även möjlighet att via Mina sidor eller genom annan kontakt med organisationen uppdatera sina uppgifter.

Uppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under längre tid än nödvändigt
Endast den eller de som har behov av personuppgifter ska ha tillgång till dem och det bara under den tid som är nödvändig. System ska gallras från onödiga och daterade uppgifter när lagringen av uppgifterna i fråga inte längre kan motiveras med laglig grund.

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse med användning av lämpliga tekniska eller organisatoriska åtgärder
Förbundet ska tillhandahålla tekniska säkerhetsåtgärder så som säker inloggning och lagring, behörighetsåtkomst och dylikt samt säkra att data inte förstörs eller försvinner genom olyckshändelse. Åtgärderna inbegriper så väl stationära servrar som molntjänster och mobila lösningar.

Endast den eller de som har behov av och behörighet till uppgifterna ska ha tillgång till dem.

Ansvarsskyldighet
Den personuppgiftsansvarige ansvarar för och ska kunna visa att ovanstående efterlevs.

5. Lagring och spridning
Förbundet ska ha kontroll över organisationens material, veta var det finns, lagra det säkert samt förhindra spridning till obehöriga. Exempelvis är det inte tillåtet att utan samtycke från den registrerade att lämna ut känsliga personuppgifter till tredje man.

All behandling som en adressfil i exempelvis Excel måste fylla ett syfte och får inte göras av slentrian. De framtagna registerutdragen ska behandlas efter gällande regelverk och får exempelvis inte sparas lättåtkomligt på datorn eller ligga öppet på skrivbordet. När arbetet med filerna/listorna är klara ska de raderas och utskrivna versioner förstöras.

Medlemslistor
Såväl förtroendevalda som anställda har tillgång till medlemslistor via Mina sidor. Medlemslistor räknas som form av administrering/uppföljning av medlemskapet vilket är internt arbete inom organisationen. Inloggning till Mina sidor är lösenordskyddad och behörighet till olika medlemslistor styrs utifrån vilken roll den sökande har i organisationen.

Vid behandling av medlemslistor ska inte mer uppgifter än vad som behövs användas, är exempelvis personnummer inte nödvändigt för den aktuella aktiviteten ska det tas bort från listorna. Detta gäller även andra uppgifter som hemadress, telefonnummer etc. Uppgifterna får inte spridas vidare eller ses av obehöriga. När arbetet med filerna/listorna är klara ska de raderas och utskrivna versioner förstöras.

Medlemslistor, eller annan känslig information, får inte mailas från förbundet till ett annat företags mailkonto. Eftersom mailet går in på företagets server anses det vara utlämnande till tredje man.

Förhandlings-, försäkrings- och rättsskyddsärenden
Förhandlings-, försäkrings- och rättskyddsärenden ska kommuniceras internt i förbundet via förbundets ärendehanteringssystem Liva där ärendena också lagras säkert med skydd för

obehörig åtkomst. I de fall ett ärende ska kommuniceras utanför organisationen ska det ske säkert via krypterad mail eller traditionell postgång. Arbetskopior får dock användas i de fall det behövs men ska efter fullgjort arbete raderas/förstöras.

6. Gallring och arkivering

Ett grundläggande krav enligt GDPR är att lagring av personuppgifter i systemen inte får ske längre än nödvändigt. Av den anledningen ska förbundets utträdda medlemmar rensas ur förbundets ärendehanteringssystem tolv månader efter utträdesdatum. Anledningen till denna tidsgräns är:

- Kunna kontakta utträdda medlemmar för uppföljning
- Eventuell inkassering av obetalda utgifter
- Medlemmar ska kunna ångra utträdet och göra ett återinträde
- Säkra uttag av statistiska uppgifter.

Icke medlemmar

Ickemedlemmars personuppgifter är typiskt sett inte känsliga.
Register med ickemedlemmar som potentiella medlemmar genom intresseanmälan eller ej erlagd medlemsavgift ska i möjligaste mån undvikas. I de fall ett sådant register anses nödvändigt ska uppgifterna endast lagras så länge det är ändamålsenligt motiverat. I de fall en person värvats som medlem men inte betalat medlemsavgiften och därmed inte blivit medlem ska personuppgifterna rensas inom skälig tid men senast inom tre månader efter ansökningsdatum.

Genom kollektivavtal är det reglerat att Livs lokala organisation ska informeras om anställningar på berörd arbetsplats. Detta ger lokal facklig organisation laglig grund för behandling av personuppgifter enligt GDPR men organisationen har en informationsplikt till den berörda då uppgifterna samlas in från en annan källa än personen själv. Det finns dock i GDPR undantag från informationsplikten för sådan information som den registrerade redan känner till.

Personuppgifterna får endast behandlas i den omfattning, och för de ändamål, som den registrerade initialt informerats om i samband med insamlingen av uppgifterna.

Anställda

Livs som arbetsgivare använder personuppgifter i många olika sammanhang, allt ifrån löneregister och adresslistor till behörighetssystem och olika databaser. Den anställdes integritet i arbetet regleras på flera olika sätt till exempel genom kollektivavtal och annan arbetsrättslig lagstiftning, Arbetsmiljöverkets föreskrifter samt allmänna råd och riktlinjer som skapas på arbetsmarknaden. Det är viktigt att finna en rimlig balans mellan behovet av att behandla personuppgifter och den anställdes anspråk på personlig integritet. GDPR tar vid där andra lagar slutar och gäller där det inte finns särskilda regler för arbetsgivarens behandling av de anställdas personuppgifter.

Personuppgifter om en anställd bör inte bevaras efter det att anställningen upphört men ibland måste vissa uppgifter bevaras under längre tid om andra lagar kräver det. Arbetsgivaren får också behålla uppgifter under den tid som en tvist med en tidigare anställd

kan bli aktuell. Det kan också vara nödvändigt att bevara vissa uppgifter för administrativa ändamål, till exempel utbetalning av pension från arbetsgivaren eller om referenser ska lämnas till andra arbetsgivare. Arbetsgivaren får bevara rena faktauppgifter som ”uppsägning på grund av arbetsbrist”, ”avsked” och ”uppsägning på grund av personliga skäl” samt betyg och tjänstgöringsintyg med omdömen som arbetsgivaren har gett till arbetstagaren efter det att anställningsförhållandet har upphört.

När en anställning upphör finns ingen grund för att spara e-postkonto och uppgifterna om en anställd på företagets webbplats, dessa uppgifter ska tas bort inom en månad.

Publicering av anställdas namn, befattning, telefonnummer och e-post på internet behöver vanligtvis inget samtycke. Samtycke krävs då befattningen är av en mer känslig natur som gör den anställde mer utsatt. Normalt sett krävs samtycke för att publicera bilder på anställda på internet.

Personuppgifter i en ansökan, intervjuanteckningar och uppgifter från referenser får registreras och sparas så länge de är nödvändiga för ansökningsförfarande, därefter ska uppgifterna gallras. Arbetsgivaren får dock spara uppgifterna så länge som sökande som inte har anställts kan vidta rättsliga åtgärder, till exempel om den sökande inte fått jobbet och vill vidta rättsliga åtgärder med anledning av diskriminering.

Om uppgifterna ska sparas under en längre tid för eventuell framtida rekrytering krävs den sökandes samtycke.

7. Kommunikation och informationsöverföring

All känslig personuppgiftsbehandling ska ske via säkra kanaler. Känsliga personuppgifter får inte skickas via e-post/sms utan att vidta särskilda säkerhetsåtgärder. Livs krypterar sin e-post inom samma domän @livs.se och har även kryptering på organisationens datorer.

Dokument innehållande känslig information, exempelvis förhandlings- och rättskyddsärenden som kan kopplas till en individ får inte skickas fritt över internet utan kryptering. Livs anställda ska använda sig av ärendehanteringssystemet LIVA för att kommunicera denna typ av frågor internt. I de fall material skickas per brev ska mottagaren adresseras och kuvertet förslutas av den som handlägger ärendet. Brevet kan som en extra säkerhetsåtgärd skickas rekommenderat.

8. Dataskydd och personuppgiftsincidenter

Förbundets IT-systemet ska följa reglerna för integritetsskydd vilket ställer krav på att systemen är utformade utifrån olika säkerhetsaspekter så som skydd för insyn från obehöriga, skydd av uppgifter, spårbarhet av användare, möjlighet till uppföljning och lämpliga säkerhetsåtgärder vid intrång.

Förbundet ser löpande över vilka externa parter som har åtkomst till förbundets material samt behörigheterna i förbundets mappstruktur vad gäller lagrat material.

All loggning som är möjlig på servrarna är påslagen och brandväggarna skickar meddelande till en angiven e-postadress vid eventuella attacker och intrång. Alla incidenter ska

dokumenteras av IT-avdelningen och omgående rapporteras till personuppgiftsansvarig och dataskyddsombudet.

En personuppgiftsincident som kan medföra en risk för fysiska personers rättigheter och friheter ska anmälas till Datainspektionen inom 72 timmar efter incidenten.

9. Molntjänster

Användandet av molntjänster är en stor och komplicerad fråga som alltid ska bedömas utifrån förutsättningarna i varje enskilt fall. Den typ av molntjänster som kan vara problematiska ur ett dataskyddsperspektiv är särskilt de publika molntjänster som tillhandahålls av globala leverantörer såsom Microsoft, Amazon och Google.

Den personuppgiftsansvarige måste bedöma om den personuppgiftsbehandling som man vill låta molntjänstleverantören utföra kommer att vara tillåten enligt GDPR. Innan tjänsten tas i bruk behöver en risk- och sårbarhetsanalys upprättas och i samband med det:

- säkerställa att personuppgifter inte kommer att behandlas på annat sätt än det ursprungliga ändamålet
- säkerställa att uppgifterna inte kommer att överföras utanför EU/EES
- bedöma vilka säkerhetsåtgärder som måste vidtas för att skydda personuppgifterna
- upprätta ett personuppgiftsbiträdesavtal.

10. Konsekvensbedömning

Om en ny och omfattande behandling ska göras och denna sannolikt medför en stor risk för fysiska personers rättigheter och friheter ska en konsekvensanalys göras. Detta gäller särskilt om ny teknik ska användas.

En konsekvensbedömning ska minst innehålla:

- en systematisk beskrivning av behandlingen och dess ändamål
- en bedömning av behov och proportionalitet hos behandlingen i förhållande till ändamålet
- en bedömning av risker för medlemmarna
- planera åtgärder för att skydda uppgifterna och minimera risker samt visa att GDPR efterlevs.

Konsekvensbedömningen ska göras gemensamt med systemägaren, personuppgiftsansvarig, dataskyddsombud, IT-avdelningen och relevant personal på Livs.

11. Ansvariga

Denna policy uppdateras och fastslås av styrelsen varje år. Ansvariga för att uppdatering görs är personuppgiftsansvarig och dataskyddsombudet.