Stockholm 20180409
rev. 20220918

Riktlinjer för hantering av personuppgifter

Latinamerikagrupperna

Tegelviksgatan 40, 116 41 Stockholm
info@latinamerikagrupperna.se
www.latinamerikagrupperna.se

Hantering av personuppgifter inom Latinamerikagrupperna som förening styrs av den europeiska dataskyddsförordningen GDPR (General Data Protection Regulation) som trädde i kraft den 25 maj 2018. För att Latinamerikagrupperna inte ska bryta mot förordningen ska följande riktlinjer följas:

Vad är en personuppgift
Personuppgifter är all information som kan vara direkt eller indirekt knuten till dig som person. Det varierar från personnummer, namn och adress till uppgifter som exempelvis ansökningshandlingar vid rekrytering, medlemsgåvor och bankuppgifter.

Användande av personuppgifter
Latinamerikagrupperna ska inte dokumentera personuppgifter om det inte är nödvändigt enligt lag eller finansiella avtal med givare.

Personuppgifterna sparas olika länge beroende på vad de används till eller om det finns lagar som kräver att vi måste spara dem en viss tid.

Registrerade personers rättigheter
Den registrerade har rätt att få veta vilka uppgifter som finns sparade hos Latinamerikagrupperna samt att få felaktiga uppgifter rättade eller raderade. Viss hantering av den registrerades uppgifter kräver personens godkännande. Ett sådant godkännande ska dokumenteras.

Utlämnande av information
Latinamerikagrupperna lämnar inte ut information om medlemmar eller anställda till icke behöriga personer. Behörig person är exempelvis myndigheter (Skatteverket, Försäkringskassan, A-kassan) och föreningens auktoriserade revisor. Undantag görs endast om överenskommelse finns med medlemmen eller den anställde i fråga. Vid varje tillfälle av utlämnande av information ska Latinamerikagrupperna säkerställa hur mottagande part använder kommer använda sig av informationen.

Hantering av medlemsregister
När en blivande medlem registrerar sig ska det tydlig framgå vilken information föreningen behöver, hur den används och sparas, samt hur medlemmen kan radera denna information om så önskas. Medlemmen ska vid utträde raderas ur medlemsregistret skyndsamt, men senast inom ett (1) år efter avslutat medlemskap ska medlemmen vara raderad ur medlemsregistret.

Medlemsregistret ska enbart vara åtkomligt för dem som av verksamhetsledaren har fått ansvar och kunskap om hantering av registret. Vem som har tillgång till medlemsregistret samt dennes ansvar ska dokumenteras skriftligen.

Hantering av personalakter
Anställningsbevis och tidrapporter för anställda hålls åtkomliga endast för verksamhetsledare och ekonom. Efter avslutad anställning sparas dokumenten fysiskt och digitalt i tre (3) år för att sedan sparas enbart digitalt i upp till sju (7) år. De sparas som verifikationer i bokföringen som enligt bokföringslagen ska sparas i sju (7) år.

Övriga dokument, så som bland annat anteckningar från medarbetarsamtal, har enbart verksamhetsledare eller annan ansvarig chef tillgång till. Dessa dokument raderas efter att medarbetarens anställning upphört. Verksamhetsledaren ansvara för att detta görs.

Vem som har tillgång till personalakter samt dennes ansvar ska dokumenteras skriftligen.

Hantering av ansökningshandlingar
Inkomna handlingar hålls åtkomliga endast för dem som ingår i den rekryteringsgrupp som är tillsatt för den specifika rekryteringen. Verksamhetsledare ska försäkra sig om att alla inom rekryteringsgruppen är medvetna om sin tystnadsplikt samt hantering av ansökningsdokument.

Rekryteringsgruppen ansvarar för att senast inom tre (3) veckor efter varje rekryteringstillfälle radera alla ansökningar och all dokumentation med koppling till personuppgifter.

Vem som har tillgång till ansökningshandlingar samt dennes ansvar ska dokumenteras skriftligen.

Hantering av lönesystemet

Personuppgifter i lönesystemet sparas i sju (7) år i enlighet med bokföringslagen och hålls åtkomliga endast för verksamhetsledare och ekonom. Efter sju (7) år raderas uppgifterna.

Vem som har tillgång till lönesystemet samt dennes ansvar ska dokumenteras skriftligen.

Protokollföring och rapportering

Latinamerikagrupperna har skyldighet att till olika aktörer, såsom banker, finansiärer och revisorer, lämna ut information om exempelvis firmatecknare och styrelsemedlemmar. Detta medför att Latinamerikagrupperna behöver lämna ut personuppgifter till utomstående part. Innan sådan information lämnas ut ska personen i fråga vars uppgifter lämnas ha blivit informerad om detta samt även syftet med utlämnandet.

Protokoll eller andra dokument som innehåller personuppgifter ska hållas åtkomliga endast för verksamhetsledare och ekonom.

Utlämnande av information ska dokumenteras.

Incidentrapportering

Vid misstanke om eller vetskapen av att personuppgifter har hamnat i orätta händer ska Latinamerikagrupperna omedelbart informera registrerad person om detta omgående samt dokumentera denna händelse, i enlighet med bilaga 1, och vid vissa typer av incidenser ska incidensen även anmälas till Dataskyddsinspektionen inom 72 timmar från att händelsen inträffat. Vilken typ av incidenser som ska anmälas till Dataskyddsinspektionen framgår på www.datainspektionen.se och där hittas även den e-tjänst där anmälan upprättas.

Incidentrapport ska upprättas av den som upptäcker incidenten i samverkan med den som innehar ansvarsområdet där incidenten upptäckts.

Efterlevnad av riktlinjerna och Dataskyddsförordningen

Verksamhetsledaren ansvarar för att årligen utvärdera efterlevnaden av Dataskyddsförordningen samt behovet av utbildning och utveckling inom området för personal och system.

Bilaga 1

Incidentrapport – personuppgiftsincidenter

Datum för upprättande av incidentrapporten:
Rapporten upprättad av:

Personuppgiftsincidenten
- Har personuppgiftsincidenten medfört en risk för de registrerades fri- och rättigheter?
- När inträffade personuppgiftsincidenten?
- När upptäcktes personuppgiftsincidenten?
- Vad har hänt vid personuppgiftsincidenten?
- Hur upptäcktes personuppgiftsincidenten?
- Varför inträffade personuppgiftsincidenten enligt din uppfattning?
- Inom vilket verksamhetsområde inträffade personuppgiftsincidenten?
- Har personuppgiftsincidenten anmälts till Dataskyddsinspektionen? Om inte, varför?

Personuppgifterna och de registrerade
- Hur många registrerade har påverkats?
- Hur många personuppgiftsposter har personuppgiftsincidenten påverkat?
- Vilken sorts personuppgifter berörs av personuppgiftsincidenten?
- Var personuppgifterna krypterade?

Konsekvenser
- Vad kan bli konsekvenserna av personuppgiftsincidenten?
- Hur allvarlig bedöms personuppgiftsincidenten vara?

Information till de registrerade
- Har de registrerade om personuppgiftsincidenten informerats? När?
- Om inte, varför inte?