ÅLANDS IDROTT

Grunder i GDPR

Innehåll

- Vad är GDPR?
- Grundläggande principer
- Hur handläggs uppgifter i vår förening?
- Hur skyddar vi personuppgifter?
- Information till de registrerade
- Om nåt går på tok
- Vanligt förekommande frågor
- Annat
- Checklista

Vad är GDPR?

Behanding?
All hantering av personuppgifter!

ÅLANDS IDROTT

General Data Protection Regulation = GDPR

Dataskyddsförordningen reglerar behandlingen av personuppgifter och har tillämpats i alla EU-länder från och med 25.5.2018.

Tillämpas på samtliga företag och föreningar

Alla samfund som behandlar personuppgifter är skyldiga att rannsaka och redovisa hur man behandlar personuppgifter

Vad är en personuppgift?

En personuppgift är alla uppgifter som kan härledas till en naturlig person, tex. Namn, address, registernummer, medlemsnummer.

Personuppgifter som en egendom

Regleringen utgår från att den registrerade äger sina personuppgifter. En legitim orsak att få ta del av uppgiften.

Nyttiga källor som använts vid skapande av detta dokument: Dataskyddslagen 2018/1050, Dataskyddsförordningen, Dataombudsmannens byrå, Dataombudsmannens Q&A om föreningar, Integritetsmyndigheten (SE) om föreningar, Riksidrottsförbundet om GDPR i idrott, Dataombudsmannens publication om personuppgifter i föreningslivet (på finska)

Vad är GDPR?

Vem är vem? Rollfördelning

Registrerad

Den vars personuppgifter behandlas. Exempelvis en idrottares, en anställd eller stipendiat.

Legitim behandlingsgrund

Registeransvarig

Den som ansvarar över behandlingen av personuppgifter och även bestämmer för vad och hur uppgifter behandlas. Tex. En förening är ansvarig över sina medlemsuppgifter och sina anställda.

Personuppgiftbiträdesavtal som reglerar rättigheter och skyldigheter

Personuppgiftsbiträde

Ofta en underleverantör till den ansvarige. Agerar enligt den ansvariges anvisning och under dess ansvar.

Grundläggande principer

Behandling av personuppgifter förutsätter alltid en legitim grund för behandlingen

- Godkända behandlingsgrunder är
  - ett samtycke av den registrerade
  - ett avtal
  - en rättslig förpliktelse för den personuppgiftsansvarige
  - skydd av vitala intressen
  - ett allmänt intresse och offentlig makt
  - ett berättigat intresse hos den registeransvariga eller en tredje part (förutsätter intresseavvägning)

T.ex. Tillåts cookies

Alla behandlingsgrunder har sina fördelar och nackdelar, överväg dessa. I regel anses rättslig förpliktelse och avtal vara de starkaste grunderna.

Ett samtycke bör alltid ges uttryckligen och kan också återtas. Information I samband med att samtycket ges.

Lagen och dataskyddsprinciperna ska alltid iakttas vid behandlingen av personuppgifter. Känsliga uppgifter får endast behandlas i undantagsfall.

Grundläggande principer

De viktiga dataskyddsprinciperna

- Den registeransvarige bör säkerställa att
  - behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.
  - behandlas konfidentiellt och säkert
  - insamlas och behandlas i ett visst, uttryckligt och lagligt syfte
  - insamlas endast i den grad som de behövs med tanke på syftet med behandlingen av personuppgifter
  - alltid uppdateras vid behov – inexakta och felaktiga personuppgifter ska raderas eller rättas utan dröjsmål
  - förvaras i en form som möjliggör identifiering av den registrerade endast så länge som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Principerna beaktas under hela uppgiftens livscykel – från insamling till radering

Grundläggande principer

Särskilda personuppgifter (sk. känsliga personuppgifter)

- Med särskilda personuppgifter avses
  - ras eller etniska ursprung
  - politiska åsikter
  - religiösa eller filosofiska övertygelse
  - medlemskap i fackförbund
  - hälsorelaterade uppgifter
  - sexuella läggning eller beteende
  - genetiska och biometriska uppgifter för identifiering av personer
- Behandling av känsliga personuppgifter är i regel förbjuden. Till detta finns undantag, varav de vanligaste är: en laglig grund, uttryckligt samtyckte, inom ramen för berättigat intresse
- Särskilda personuppgifter bör skyddas särskilt noga

Notera att även andra än i direktivet uppräknade uppgifter kan i vårt samhälle anses vara känsliga:
- Socialsignum
- Ekonomiska uppgifter

Samtliga undantag HÄR!

Grundläggande principer

Den registrerades rättigheter

- Du kanske minns att GDPR bygger på att registrerade äger sina uppgifter? Utifrån detta har den registrerade har som utgångspunkt rätt till följande:
  - få information om behandlingen av egna personuppgifter
  - få tillgång till uppgifter
  - rätta uppgifter
  - avlägsna uppgifter och bli glömd
  - begränsa behandlingen av uppgifter
  - flytta uppgifterna mellan system
  - göra en invändning mot behandling av personuppgifter
  - inte bli föremål för automatiskt beslutsfattande.
- Notera att beroende på behandlingsgrunden, kan alla rättigheter inte utövas i alla situationer. Ex. en anställd kan inte neka att arbetsgivaren sparar grundläggande uppgifter om den anställda. Detta för att behandlingsgrunden är rättslig förpliktelse.

Vilka uppgifter behandlas?

Uppgifter som vanligtvis behandlas inom idrottsrörelsen

- Uppgifter från registrerade

- Kontaktuppgifter såsom namn, adress, telefonnummer, e-postadress (även föräldrars?)
- Kontonummer för utbetalning av lön, arvoden
- Uppgifter om närvaro på styrelsemöten, träningar, tävlingsresor
- Faktureringsuppgifter
- Bilder
- Cookies, uppgifter om besök på hemsida

- Känsliga personuppgifter

- Uppgifter om allergier eller andra sjukdomar tex. för tävlingsresor
- Hälsorelaterade uppgifter i anknytning till arbetsplatshälsovård och andra arbetsgivarrelaterade ärenden
- Hälsorelaterade uppgifter i anknytning till stipendiater och studerande med specialidrott

Hur skyddar vi personuppgifter?

ÅLANDS IDROTT

Tips på åtgärder att vidta

- Tekniska
  - Behandling av samtliga uppgifter i datasäker omgivning (moln)
  - Alla datorer skyddas med personliga lösenord som byts regelbundet
  - Begränsad åtkomst till känsliga uppgifter
- Organisatoriska
  - Inga onödiga personuppgifter i pappersform
  - Rum med uppgifter låses, likaså skärmar
  - Rutiner kring radering av uppgifter
  - Manuell radering av e-post
  - Utbildning av samtliga som hanterar personuppgifter

Information till de registrerade

Viktigt att de registrerade får tydlig och lättförståelig information om hur uppgifter behandlas

- Personuppgiftansvariges kontaktuppgifter
- Behandlingens syfte och rättsliga grund
- Vilka personuppgifter behandlas och varifrån de samlas
- Delas uppgifterna till en tredje part eller utanför EU?
- Hur länge förvaras personuppgifterna
- Vilka rättigheter har den registrerade

Sammanställs och visas lämpligast på hemsidan och rubriseras ‘’Personuppgiftspolicy’’

Åländska DI har pulicerat en checklista som är lätt att dubbelkolla att allt är med.

Om nåt går på tok

Vad är en incident?

- Med incident avses en situation där personuppgifter förstörs, försvinner, ändras, olovligen överlåts eller hamnar i händerna på en tredje part
- En incident kan vara exempelvis

Om nåt går på tok

Vad behöver man göra om det sker en incident?

- Viktigt att dokumentera alla incidenter, oberoende om de leder till åtgärder eller inte
- Bedöm storleken på risken som orsakats – låg – medel – hög. I detta beaktas hur känslig information som läckt, är det många drabbade, orsakades stor skada eller har läckan pågått länge? Om personer i utsatt ställning (ex. minderåriga), kan detta bidra till att incidenten anses vara allvarligare
- Om incidenten sannolikt orsakar en hög risk för personens rättigheter och friheter, ska den registrerade informeras om incidenten
- En personuppgiftsincident ska anmälas till tillsynsmyndigheten inom 72 timmar, om incidenten kan äventyra fysiska personers rättigheter och friheter

Information om anmälan och blankett

Vanligt förekommande frågor

Vad är ett register? Behöver vi en registerbeskrivning?

- Ett register är ett samlingsbegrepp för att uppgifter som går att koppla ihop under ett tema. Normalt finns några register – medlemmar, idrottare + föräldrar, register över anställda och organ,
- Vilka register man har är något man främst själv ska hålla koll på, inga registerbeskrivningar behöver publiceras. Registerbeskrivning härleds från den tidigare lagstiftningen, men alltså idag onödig
- Samlig information som ska ges till registrerade kan sammanställas I personuppgiftspolicyn
- Notera dock att en förening bör en föreningslagen föra separate medlemsregister. Medlemsregister ska skyddas omsorgsfullt, antingen så att det finns i en enhet som helt är separerad från internet eller så att det är skyddat med en bra brandvägg och antivirusprogram.

Vanligt förekommande frågor

Får föreningar/förbund marknadsföra sina kurser till sina medlemmar?

- I regel ja, det är frågan om berättigat intresse. Det är även tillåtet att informera mer allmänt om sin verksamhet. Medlemsuppgifter får inte utlämnas till tredje parter i direktmarknadsföringssyfte utan medlemmens tillstånd.

Vanligt förekommande frågor

Kan massinbjudningar etc. skickas så, att samtliga mottagare syns?

- I regel inte, använda BCC-funktionen (dold kopia). Undantag om tex. medlemmarna kan anses behöva uppgifterna för kommunikation eller anslutande till frivillig diskussionsgrupp

Vanligt förekommande frågor

Vad ska vi tänka på om vi anlitar underleverantörer och dessa behandlar våra personuppgifter?

- Kom ihåg att ingå skriftligt avtal och använd personuppgiftsbiträdesavtalet där era och underleverantörens rättigheter och skyldigheter redogörs
- Vid behov komplettera personuppgiftspolicyn

Vanligt förekommande frågor

Kan man publicera bilder om man inte får samtycke till alla som finns på bilden?

- I detta fall utgår man från registeransvariges berättigade intresse (intresseavvägning). Om frågan om minderåriga ska man avväga om det verkligen är nödvändigt. Kan man använda en bild varur barnet inte kan identifieras?
- Då bilden tas behöver personen/föräldern informeras om att deras personuppgifter, alltså bilderna, kan komma att användas av föreningen för att informera om verksamheten på webbplats och/eller sociala medier. Personerna behöver också få information att de har möjlighet att invända mot behandlingen, samt vem de då ska kontakta.
- Föreningen måste inte samla in namn på alla som är med på bilderna, men om någon identifierar sig själv och vill utöva sina rättigheter, så gäller individens rättigheter.
- När det gäller publicering av barns personuppgifter på hemsida eller sociala medier kan det vara lämpligt att inhämta samtycke från vårdnadshavare.
- Notera att om personen inte kan identifieras på bilden är det inte frågan om en personuppgift

Vanligt förekommande frågor

Får man publicera tävlingsresultat?

- Arrangören behöver informera alla registrerade innan publicering av resultatlistor sker.
- Resultatlistorna ska inte innehålla mer personuppgifter än vad som behövs för ändamålet med publiceringen (tex. Adress, soc-sign)
- Om en individ begär att bli raderad från en publicerad resultatlista bör föreningen ha rutiner för att anonymisera den individens personuppgifter i resultatlistan.

Annat

Informera och uppdatera

- Viktigt att alla som behandlar personuppgifter inom föreningen känner till grunderna I hur personuppgifter behandlas enligt GDPR och hur detta i praktiken fungerar inom föreningen
- Detta material är en del av inlärningen av nyanställda och gås igenom regelbundet med anställda
- Materialet hålls uppdaterat

Checklista

Vilka frågor ska man börja att ställa sig?

- 1. Är er organisation medveten om EU:s nya dataskyddsförordning?
- 2. Vilka personuppgifter hanterar ni?
- 3. Använder ni missbruksregeln idag?
- 4. Vilken information lämnar ni?
- 5. Hur ska ni tillmötesgå de registrerades rättigheter?
- 6. Med vilket rättsligt stöd behandlar ni personuppgifter?
- 7. Hur inhämtar ni samtycke?
- 8. Behandlar ni personuppgifter om barn?
- 9. Vad ska ni göra vid personuppgiftsincidenter?
- 10. Vilka särskilda integritetsrisker finns med er behandling?
- 11. Har ni byggt in skydd för personuppgifter i era it-system?
- 12. Vem ansvarar för dataskyddsfrågor i er organisation?
- 13. Har ni verksamhet i flera länder?

Frågorna tagna härifrån

Checklista

Vad behöver ni har på plats

- ❑ Uppfattning om vilka personuppgifter som behandlas i verksamheten
- ❑ Uppfattning om olika grupper på sina registrerade - behandlas barn olika?
- ❑ Den legala behandlingsgrunden (för alla uppgifter!)
- ❑ Personuppgiftspolicy på hemsidan med information
- ❑ Rutiner för att utbilda ny personal som handlägger uppgifter
- ❑ Rutiner för att säkerställa datasäkerhet
- ❑ Rutiner för att hantera incidenter
- ❑ Personuppgiftsbiträdesavtal om personuppgifter överförs på biträde

Frågorna tagna härifrån

Tack!