

Riktlinjer och rutiner för GT Vikingarnas personuppgiftsbehandlingar

1. Bakgrund

Dataskyddsförordningen, eller GDPR som den också kallas, började gälla för samtliga av EU:s medlemsländer den 25 maj 2018. Förordningen ersätter det tidigare Dataskyddsdirektivet som implementerats i Sverige genom Personuppgiftslagen (PuL).

Syftet med den nya dataskyddsförordningen är bland annat att stärka skyddet för registrerade, det vill säga enskilda personer vars personuppgifter behandlas. Förordningen innebär också skärpta krav för hur företag och organisationer ska hantera personlig data. Höga sanktionsavgifter kan drabba de företag som inte följer reglerna.

I nästa stycke följer en kort beskrivning av dataskyddsförordningens grundprinciper och andra viktiga bestämmelser i förordningen.

2. Grundprinciper och viktiga bestämmelser i GDPR

Den nya dataskyddsförordningen anger några grundläggande principer som gäller för all behandling av personuppgifter. Kortfattat innebär principerna att personuppgifter endast får samlas in och behandlas för i förväg bestämda ändamål, att det ska finnas en laglig grund för behandlingen och att mängden personuppgifter som behandlas ska begränsas till vad som är nödvändigt för ändamålet. Uppgifterna får heller inte sparas längre än nödvändigt eller lagras i länder utanför EU, om inte länderna har motsvarande personskydd i lagstiftningen.

Enligt dataskyddsförordningen har registrerade rätt att få information om när och hur deras personuppgifter behandlas. De har också rätt att veta vilken data man har sparat om dem, få tillgång till personuppgifterna och i vissa fall att få sina uppgifter rättade, raderade eller flyttade.

En annan viktig bestämmelse är att alla leverantörer som hanterar eller lagrar personuppgifter för ett företags eller en organisations räkning också måste följa dataskyddsförordningen. För att säkerställa detta måste företaget eller organisationen (den personuppgiftsansvarige) ha ett så kallat personuppgiftsbiträdesavtal med varje sådan leverantör (personuppgiftsbiträdet).

Slutligen måste dataläckor och andra så kallade personuppgiftsincidenter rapporteras till Integritetsskyddsmyndigheten. Myndigheten är tillsynsmyndighet och ska övervaka att de som behandlar personuppgifter följer dataskyddsförordningen.

En nyhet med dataskyddsförordningen jämfört med PuL är principen om ansvarsskyldighet. Det innebär att Integritetsskyddsmyndigheten inte behöver visa att de företag och organisationer som behandlar personuppgifter har gjort fel. Istället måste dessa visa att de gjort rätt, dvs. att bestämmelserna i dataskyddsförordningen följs.

För GT Vikingarnas del betyder det att vi måste ha skriftlig dokumentation för hur vi hanterar personuppgifter. Till exempel ska alla personuppgiftsbehandlingar som vi utför i föreningen finnas i en gemensam registerförteckning. Vi måste också ha policyer och rutiner som bidrar till att vi följer dataskyddsförordningen.

3. Specifika rutiner/riktlinjer för GT Vikingarna

3.1 Allmänt

Personuppgifter är all slags information som kan knytas till en fysisk person som är i livet. Det kan vara namn, e-post, adress men även en bild om den på något sätt kan användas för att identifiera den enskilda personen.

GT Vikingarna behandlar anställdas, medlemmars, gymnasters och målsmäns personuppgifter, samt köande. Anställdas personuppgifter behandlas i egenskap av arbetsgivare för utbetalning av lön och säkerställande av uppfyllande av arbetsgivaransvar. Gymnasters och målsmäns uppgifter hanteras för uppföljning av närvaro, LOK-stöd och administration och överblick av föreningens verksamhet. Personuppgifter som kan bli aktuella för ovanstående kategorier är exempelvis namn, personnummer, adress och fotografier.

3.2 Insamling av personuppgifter

En av de grundläggande principerna i dataskyddslagstiftningen är principen om lagringsminimering, det vill säga att man ska samla in så få personuppgifter som möjligt. Det innebär att vi bara får samla in de uppgifter som behövs för att kunna sköta föreningen.

För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett stöd i dataskyddsförordningen, en så kallad laglig grund för behandlingen. I praktiken finns det fyra lagliga grunder som är relevanta vår verksamhet; avtal (anställningsavtal), rättslig förpliktelse (till exempel bokföringsskyldighet) samtycke och berättigat intresse (när vårt eller annans berättigade intresse väger tyngre än den registrerades integritet).

När föreningen samlar in personuppgifter måste vi lämna viss information till de personer vi samlar in uppgifter om. Som huvudregel ska informationen lämnas skriftligen. Så sker i föreningen.

I förhållande till gymnaster, tränare och målsmän samlar föreningen in personuppgifter baserat på samtycke som informeras om i samband med fakturering då informationen finns på fakturan (skriftlig) och uppgifter sparas därefter baserat på detta samtycke och/eller på berättigat intresse.

3.2.1 Fotografier

Fotografier på individer som behandlas i dator kan vara personuppgifter. Det innebär att man måste ta hänsyn till bestämmelserna i dataskyddsförordningen. Det kan till exempel krävas samtycke från den person uppgifterna avser. Fotografier finns enbart på gymnaster och tränare och samtycke insamlas när fakturorna går ut, samt muntligen när fotografierna tags och läggs in i Sportadmin.

3.2.2 Känsliga personuppgifter

Det är bara tillåtet att behandla känsliga uppgifter i vissa undantagsfall. Med känsliga personuppgifter avses uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

Föreningen behandlar inte några känsliga personuppgifter. Skulle anställd vara medlem i fackförening, skulle sådan uppgift inhämtas som ett led de skyldigheter föreningen har som arbetsgivare. Sådan uppgift skulle endast relevanta personer i styrelsen ha tillgång till.

I vissa fall insamlas uppgifter om allergier eller sjukdom som diabetes. Det görs för att tränarna ska kunna hjälpa och skydda gymnasterna. Sådana uppgifter raderas när gymnasten inte längre är aktiv.

3.2.3 Särskilda personuppgifter – personnummer

Även om ett personnummer inte är en känslig personuppgift så betraktas den som extra skyddsvärd och därför får den inte användas hur som helst. Användningen av personnummer måste enligt dataskyddsförordningen vara klart motiverat med (i) ändamålet med behandling (ii) vikten av en säker identifiering eller (iii) något annat beaktansvärt skäl.

Personnummer behövs inom föreningen för säker identifiering av gymnaster, då gymnasterna täcks av försäkringar som kräver personnummer för sin giltighet. Personnummer är också nödvändigt för att erhålla LOK-stöd.

Personnummer behövs också för tränare, där de senare erhåller lön som inte kan utbetalas utan denna uppgift. Personnummer är också klar motiverat då alla personer som tränar barnen måste inkomma med ett särskilt utdrag ur polisregistret för arbete med barn, varvid det inte är möjligt att matcha utdraget till rätt person utan personnummer, detta för att skydda barnen.

Föreningen överväger alltid om det är nödvändigt att notera personnummer och gör inte detta på andra ställen än i Sportadmin. Målsmäns som inte är tränare, personnummer noteras exempelvis inte. Det är möjligt att ta bort de fyra sista siffrorna i Sportadmin utan att systemet varnar, så görs när personen inte är aktiv mer.

3.4 E-post

Föreningen skickar inte integritetskänsliga uppgifter via e-post, t.ex. uppgifter om personliga och ekonomiska förhållanden. Om känsliga personuppgifter skulle inkomma bör du till exempel inte utan vidare vidarebefordra eller svara på mailet när det innehåller uppgifterna, utan fundera på om du kan ta bort dessa i vidarebefordrans- eller svarsmejlet.

3.5 Dokumenthantering

Även i Dropbox sker behandling och lagring av personuppgifter, som omfattas av samma krav som övrig behandling/behandling i system. Personuppgifterna som behandlas ska vara korrekta och är de inte det måste de uppdateras eller rättas utan dröjsmål. Åtkomsten till personuppgifter ska begränsas till de som behöver det för att kunna utföra sina arbetsuppgifter och sättet att arbeta måste vara utformat efter den principen. Det är föreningens bedömning att så sker.

Behörigheterna till föreningens system och övriga personuppgiftsbehandlingsframgångar av nedan, Gallring och behörigheter.

3.6 Gallring

Personuppgifter får inte lagras under längre tid än nödvändigt med hänsyn till ändamålen med behandlingen. När uppgifterna inte längre behövs måste de alltså gallras, vilket innebär att de antingen måste raderas eller avidentifieras. Det är viktigt för oss att se över och ha väl övervägda tidsfrister för gallring.

Nedan några tumregler för gallring av olika behandlingar som sker i föreningen:

3.6.1 Leverantörer

- Personuppgifter som är hänförliga till kontaktperson hos leverantören (namn, e-postadress, telefonnummer) får sparas i fem år från senaste interaktionen med leverantören efter avtalets upphörande.
- Leverantörsavtal: får sparas i fem år efter avtalets upphörande. Avtalen kan dock sparas upp till tio år om det finns klausuler rörande garantier, sekretess eller immaterialrätt som är utsträckta i tiden. Glöm inte att e-postkorrespondens kan utgöra avtalsinnehåll!
- E-post-korrespondens med leverantörer sparas så länge avtalsrelationen pågår men gallras efter att det upphört utan onödigt dröjsmål. Vid potentiell tvist kan man spara uppgifterna till det att risken för tvist inte längre föreligger eller tvisten är slutligen avgjord. Om e-posten innehåller avtalsvillkor kan man spara korrespondensen i enlighet med reglerna för avtal (se ovan).

3.6.2 Gymnaster

Föreningens värdeord är glädje, gemenskap och utveckling. En del av gymnasternas utveckling är att själva kunna bli tränare. Många av föreningens tränare är f.d. gymnaster som gjort ett uppehåll. För att fortsätta kunna vara med i gemenskapen och för att kunna hitta tränare till våra grupper har därför har föreningen ett starkt intresse av att kunna identifiera familjer och personer som tidigare varit gymnaster eller tränare. Så länge någon medlem av familjen är engagerad i föreningen finns därmed ett starkt intresse av att spara de harmlösa personuppgifter som föreningen samlat in. De fyra sista siffrorna i personnumret tas bort när gymnasten slutar / inte är aktiv mer. Detsamma gäller uppgifter om allergier. Det är föreningens uppfattning att föreningens intresse av att spara uppgifter om att man varit gymnast väger tyngre än den ”kränkning” av integriteten som det innebär att dessa uppgifter sparas.

3.6.3 Anställda

Anställdas personuppgifter sparas så länge som det enligt lag är nödvändigt för att kunna fullgöra åtaganden som arbetsgivare.

3.7 Personuppgiftsbiträdesavtal

Ett personuppgiftsbiträde är en extern aktör, ofta en leverantör av ett IT-system, en molntjänstlösning eller något annat, som behandlar eller lagrar personuppgifter för vår räkning. Om föreningen vill använda oss av sådana leverantörer måste vi teckna ett skriftligt avtal med leverantören/personuppgiftsbiträdet som måste uppfylla vissa krav. Bland annat ska avtalet innehålla instruktioner för hur biträdet får behandla personuppgifterna.

Föreningen har personuppgiftsbiträdesavtal med Sportadmin.

3.8 Ändringar i registerförteckning och i datainsamlingen

Föreningens behandlingar av personuppgifter har kartlagts i en registerförteckning. I denna registrerar vi all behandling av personuppgifter, både det som sker i system och det som sker manuellt. På så sätt får vi en översikt över alla register, system och dokument där personuppgifter förekommer.

Förteckningen hjälper oss ha kontroll över vilka personuppgiftsbehandlingar vi utför i föreningen. Den hjälper oss också att, på ett systematiskt sätt, kontrollera att vi till exempel har en laglig grund att behandla uppgifterna. Styrelsen ser till att registerförteckning är kvalitetssäkrad, men registret är ett levande dokument som måste uppdateras eller justeras vid förändringar i personuppgiftsbehandlingarna.

3.9 Rutiner för personuppgiftsincidenter

En personuppgiftsincident är en händelse som leder till att personuppgifter kommer i orätta händer, förloras eller uppdateras felaktigt. Det kan röra sig om att någon obehörig har kommit över lösenordet till ett system som behandlar personuppgifter, att systemet blivit hackat eller drabbats av virus, eller att ett mejl med känsliga personuppgifter skickas till fel mottagare. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt.

Vid personuppgiftsincidenter där obehöriga har fått tillträde till personuppgifter ska Integritetsskyddsmyndigheten underrättas inom 72 timmar från upptäckten. Detta gäller även om incidenten inträffat hos ett av våra personuppgiftsbiträden, det vill säga någon av våra leverantörer som behandlar eller lagrar personuppgifter för vår räkning.

- Därför är det mycket viktigt att varje anställd, tränare eller styrelseledamot rapporterar inträffad personuppgiftsincident till ordföranden omgående efter att du fått vetskap om en sådan incident.

3.10 De registrerades rättigheter

Personer vars personuppgifter behandlas har ett antal rättigheter som har utökats, förstärkts och specificerats i dataskyddsförordningen. De viktigaste rättigheterna är rätt till information om behandlingen samt rätt att få tillgång till sina personuppgifter. De registrerade har också rätt att få felaktiga uppgifter rättade eller raderade, rätt att invända mot att personuppgifterna används, rätt till begränsning av behandlingen och rätt att få ut personuppgifter i maskinläsbart format (dataportabilitet).

Dessa rättigheter är inte absoluta och en begäran om utövande av rättigheterna resulterar därför inte alltid i någon åtgärd. Det är dock viktigt att vi hanterar och dokumenterar förfrågningar från registrerade.

Om förfrågan eller begäran om utövande av ovan nämnda rättigheter kommer in till föreningen eller kansliet från en registrerad bör du kontakta styrelsen för vidare hantering. Det finns tidsfrister inom vilka återkoppling till den registrerade bör ske, därför bör sådan kontakt tas snarast möjligt.

Gallring och behörigheter

System / behandling	System- ansvarig	Vem/vilka har behörighet till systemet / behandlingen? <i>Åtkomsten till personuppgifter ska begränsas till de som behöver det för att kunna utföra sina arbetsuppgifter.</i>	Utförare av gallringen	Gallringsfrister <i>Personuppgifter ska gallras när syftet med behandlingen har upphört.</i>	Gallringsrutiner <i>En instruktion om hur den faktiska gallringen genomförs i systemet ska anges nedan.</i>
SYSTEM					
Sportadmin – anställd	Styrelsen	Tränare	Styrelsens sekreterare	Tills anställningen upphör.	Uppgifterna rensas senast två styrelsemöten (normalt tre månader) efter anställningens upphörande.
Sportadmin – gymnaster och tränare	Styrelsen	Styrelse och tränare	Styrelsens sekreterare	När syftet med behandlingen upphört och föreningens intresse av att spara harmlösa uppgifter inte längre är större än ”kränkningen”. Känsliga uppgifter rensas årligen.	Årligen enligt årshjulet.
Sportadmin – medlemmar	Styrelsen	Styrelse och tränare	Styrelsens sekreterare	När personen avslutar medlemskapet	Uppgifterna rensas senast två styrelsemöten (normalt tre månader) efter anställningens upphörande.
Dropbox – anställd	Styrelsen (HR ansvariga)	Styrelsen	Styrelsens sekreterare	Tills anställningen upphör, men så länge som krävs enligt lag.	Årligen enligt årshjulet.
Dropbox – övrig information	Styrelsen	Styrelsen	Styrelsens sekreterare	När syftet med behandlingen upphört och föreningens intresse av att spara harmlösa	Årligen enligt årshjulet.

Gallring och behörigheter					
				uppgifter inte längre är större än "kränkningen".	
ÖVRIGA PERSONUPPGIFTSBEHANDLINGAR					
N/A					

GT VIKINGARNA FÖRTECKNING ÖVER PERSONUPPGIFTSBEHANDLINGAR

1. Sportadmin

System:	Sportadmin
Systemägare:	Ordförande Eva Unger
Beskrivning av system och databehandlingar:	System för heltäckande administration av föreningar, grupper, schemaläggning, LOK-stöd, närvaro, köregistrering mm. Behandling sker när gymnasterna ställer sig i kö till föreningen.
Kategorier av registrerade:	Aktiva gymnaster, Köande gymnaster, Målsmän, Tränare, Styrelseledamöter, Domare, Tidigare gymnaster, Medlemmar, Anställda
Inhämtning av uppgifter:	Manuell registrering
Rättelse av uppgifter:	Kontakta kansliet@gtvikingarna.se
Gallringsrutin:	Finns och process upprätthålls i samband med årshjulets genomgång
Överföring av personuppgifter:	Nej. Sker endast i samband med anmälan till tävling.

Kategorier av registrerade:	Behandlade personuppgifter:	Syfte med behandlingen	Laglig grund	Intresseavvägning
Aktiva gymnaster:	Namn Adress Personnummer Mobilnummer Epost Målsmän Närvaro Allergier	Organisera och genomföra arbetet i föreningen, kompetensutveckling, barns trygghet och säkerhet, hantera försäkring, LOK-stöd	Samtycke / Intresseavvägning	Barns utveckling, trygghet och säkerhet
Köande gymnaster	Namn Adress Personnummer Mobilnummer Epost Målsmän	Organisera föreningen,	Samtycke	
Målsmän	Namn Adress Personnummer Mobilnummer Epost	Organisera och genomföra arbetet i föreningen, barns trygghet och säkerhet	Samtycke / Intresseavvägning	Barns trygghet och säkerhet

Tränare / anställda	Namn Adress Personnummer Mobilnummer Epost Närvaro Allergier Utbildningsnivå / licenser Uppgift om uppvisat utdrag ur från polisregister	Organisera och genomföra arbetet i föreningen, barns trygg- och säkerhet	Intresseavvägning, nödvändigt för att uppfylla förpliktelser enligt lag	Barns utveckling, trygg- och säkerhet
Styrelse- ledamöter	Namn Adress Personnummer Mobilnummer Epost Uppgift om uppvisat utdrag ur från polisregister	Organisera och genomföra arbetet i föreningen, barns trygg- och säkerhet	Samtycke, intresseavvägning	Barns trygg- och säkerhet
Domare	Namn Förening Utbildningsnivå Epost	Organisera och genomföra arbetet i föreningen, barns trygg- och säkerhet	Samtycke, intresseavvägning	Barns trygg- och säkerhet
Medlemmar	Namn Adress Födelsedag Mobilnummer Epost	Organisera och genomföra arbetet i föreningen	Samtycke	
Tidigare aktiva	Namn Adress Födelsedag Mobilnummer Epost	Organisera och genomföra arbetet i föreningen, barns trygg- och säkerhet	Samtycke, intresseavvägning	Barns utveckling, trygg- och säkerhet

2. Dropbox

System:	Dropbox
Systemägare:	Ordförande Eva Unger
Beskrivning av system och databehandlingar:	System för att spara dokumentation hänförlig till föreningens verksamhet, avtal, protokoll mm.
Kategorier av registrerade:	Styrelseledamöter, Anställda, Gymnaster i vissa fall, Leverantörer, Kontaktpersoner på kommunen / andra föreningar.
Rättelse av uppgifter:	Kontakta kansliet@gtvikingarna.se
Gallringsrutin:	Finns och process upprätthålls i samband med årshjulets genomgång
Överföring av personuppgifter:	Nej.

Kategorier av registrerade:	Behandlade personuppgifter:	Syfte med behandlingen	Laglig grund	Intresseavvägning
Styrelseledamöter	Namn Närvaro	Organisera och genomföra arbetet i föreningen.	Samtycke / Intresseavvägning	Barns utveckling, trygg- och säkerhet
Anställda	Namn Adress Personnummer Mobilnummer Epost Kontouppgifter	Organisera och genomföra arbetet i föreningen, arbetsgivaransvar	Nödvändigt för att uppfylla förpliktelser enligt lag	
Gymnaster i vissa fall	Namn Uppgifter om skada	Organisera och genomföra arbetet i föreningen, barns trygg- och säkerhet	Samtycke / Intresseavvägning	Barns trygg- och säkerhet
Leverantörer	Namn Mobilnummer Epost	Organisera och genomföra arbetet i föreningen	Intresseavvägning	Uppfyllande av åtagande
Kontaktpersoner	Namn Mobilnummer Epost Förening / titel	Organisera och genomföra arbetet i föreningen, barns trygg- och säkerhet	Samtycke, intresseavvägning	Barns trygg- och säkerhet