Instruktion

för behandling av personuppgifter i organisationerna inom Svenska Båtunionen

Mellan organisationerna inom Svenska Båtunionen (SBU) - SBU, båtförbund och båtklubbar - gäller följande Instruktion för behandling av personuppgifter hos någon av organisationerna.

INNEHÅLL

1. Instruktionens bakgrund, syfte och omfattning

Till grund för instruktionen ligger Europaparlamentets och Rådets förordning (EU) 20916/679 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (GDPR) och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen, DSL) och andra tillämpliga bestämmelser om behandling av personuppgifter. Instruktionen syftar till att beskriva Organisationernas inbördes åligganden när det gäller behandling av personuppgifter och att säkerställa att behandlingen lever upp till de tillämpliga bestämmelserna. Samtidigt är instruktionen underordnad sådana bestämmelser i händelse av motstridighet.

2. Grundläggande principer för behandlingen

***Laglighet**:* Behandlingen av personuppgifter ska vara förenlig med tillämpliga bestämmelser.

***Ändamålsbegränsning**:* Behandlingen av personuppgifter ska endast ske för i förväg bestämda och dokumenterade berättigade ändamål och får inte därefter behandlas för några ändamål som inte är förenliga med de ursprungliga.

***Uppgiftsminimering**:* Behandlingen får endast omfatta sådana personuppgifter som är nödvändiga för uppfyllandet av de ändamål som ligger till grund för behandlingen.

***Lagringsminimering**:* Personuppgifter får inte behandlas under längre tid än som är nödvändigt för uppfyllandet av de ändamål som ligger till grund för behandlingen eller under sådan tid som gäller enligt tvingande bestämmelser i lag eller annan författning. När uppgifterna inte längre behövs ska de därefter fortlöpande gallras.

***Korrekthet**:* Personuppgifterna ska vara korrekta, fullständiga och uppdaterade och ska vid brister i sådana avseenden rättas eller bli föremål för annan lämplig åtgärd för att åstadkomma undanröjande av sådan brist.

***Säkerhet**:* Organisationerna ska vidta lämpliga tekniska, administrativa eller organisatoriska säkerhetsåtgärder för att skydda personuppgifterna och för att uppnå en hög generell skyddsnivå.

***Transparens**:* Behandlingen av personuppgifter ska ske på ett transparent och öppet sätt gentemot de registrerade, särskilt genom att Organisationerna tillhandahåller klar och tydlig information om behandlingen och de registrerades rättigheter, exempelvis på Organisationernas hemsidor.

3. Behandlingens ändamål, föremål och art

Organisationerna behandlar personuppgifter som angår personal, medlemmar och andra med vilka Organisationerna har ett avtalsförhållande eller med vilka Organisationerna kommunicerar.

Organisationerna behandlar personuppgifter om behörigheter när personal, medlem eller annan omfattas av en skyldighet att inneha viss formell behörighet, såsom förarintyg, maskinbehörighet, försäkringsbevis, olika slags certifikat, tillstånd eller annat dokument som styrker viss kompetens, eller annat därmed jämförligt dokument.

3.1. Behandling av personaluppgifter

Organisationerna behandlar personaluppgifter som omfattar personuppgifter om sin respektive personal, vilken utgörs av anställda, uppdragstagare, funktionärer eller förtroendevalda. Personuppgifterna behandlas för att Organisation ska kunna ingå, administrera och avsluta anställningsavtal, uppdragsavtal och avtal med funktionärer eller förtroendevalda. Personuppgifterna behandlas därutöver för att Organisation ska kunna fullgöra skyldigheter och tillvarata rättigheter inom arbetsrätten, fullgöra skyldigheter och tillvarata rättigheter vad gäller redovisning och bokföring och i övrigt på det skatterättsliga området.

Dessutom behandlas personuppgifter för att upprätthålla nödvändig säkerhet i lokaler, utrymmen, eller anläggning som Organisation äger eller disponerar, jämte för att upprätthålla nödvändig säkerhet vad gäller informationssystem som Organisation äger eller disponerar och information som behandlas i sådana system.

Organisationerna kan för sådana ändamål ha gemensam åtkomst till personuppgifterna.

3.1.1. Personuppgifter som omfattas av behandlingen.

Behandlingen kan omfatta följande kategorier av personuppgifter.

- Kontaktuppgifter, bestående i uppgifter om personnamn, adress och postadress, telefonnummer och e-postadress
- Personnummer, när detta är nödvändigt för att säkert kunna identifiera personen eller för att uppgiften måste behandlas vid uppfyllandet av rättslig skyldighet
- Kontouppgifter, bestående i uppgifter om bankkonton och andra konton för att kunna genomföra, mottaga och administrera betalningar, såsom löner, arvoden och andra ersättningar
- uppgifter om hälsa och sjukdom, när detta är nödvändigt för att fullgöra skyldigheter på personalhälsoområdet

3.2. Behandling av medlemsuppgifter

Organisationerna behandlar personuppgifter om medlemmar enligt följande.

3.2.1. BAS-C

Organisationerna behandlar personuppgifter i ett gemensamt informationssystem (Båtunionens Administrationssystem, BAS), där personuppgifterna angår medlemmar hos respektive Organisation och behandlas för ändamål inom respektive Organisations verksamhetsområde. BAS-C är en del i BAS som SBU använder och där SBU behandlar personuppgifter för att:

- registrera, avregistrera, administrera och föra register över medlemmar hos Organisationerna som även utgör medlemmar hos SBU, eller för att genomföra sådana förändringar som SBU överenskommit med medlemmen avseende medlemskapet,

- registrera, avregistrera, administrera och föra register över funktionärer hos Organisationerna,
- kommunicera med funktionärer hos Organisationerna, exempelvis genom e-post,
- fakturera, avisera, administrera, bokföra och redovisa medlemsavgifter jämte hantering av betalning av medlemsavgifterna, samt
- genom postförsändelse eller e-post distribuera medlemstidningen Båtliv till medlemmar hos Organisationerna, där medlemmens namn och adressuppgifter lämnas till sådant tryckeri och distributör som SBU vid varje tid anlitar för att ta fram medlemstidningen och för att tillhandahålla tidningen till medlemmen.

3.2.2. BAS-F

BAS-F är en del i BAS som Båtförbunden använder och där Båtförbunden behandlar personuppgifter för att:

- registrera, avregistrera, administrera och föra register över medlemmar hos Organisationerna som även utgör medlemmar hos Båtförbunden, eller för att genomföra sådana förändringar som Båtförbunden överenskommit med medlemmen avseende medlemskapet,
- registrera, avregistrera, administrera och föra register över funktionärer hos Organisationerna,
- kommunicera med funktionärer hos Organisationerna, exempelvis genom e-post, samt
- fakturera, avisera, administrera, bokföra och redovisa medlemsavgifter jämte hantering av betalning av medlemsavgifterna.

3.2.3. BAS-K

BAS-K är en del i BAS som Båtklubbarna använder och där Båtklubbarna behandlar personuppgifter för att:

- registrera, avregistrera, administrera och föra register över medlemmar hos Organisationerna som även utgör medlemmar hos SBU, eller för att genomföra sådana förändringar som Båtklubbarna överenskommit med medlemmen avseende medlemskapet,
- registrera, avregistrera, administrera och föra register över funktionärer hos Organisationerna,
- kommunicera med funktionärer hos Organisationerna, exempelvis genom e-post,
- fakturera, avisera, administrera, bokföra och redovisa medlemsavgifter jämte hantering av betalning av medlemsavgifterna,

3.2.4. Ytterligare ändamål för behandling av medlemsuppgifter

Behandlingen av personuppgifter i BAS, BAS-C, BAS-F och BAS-K ska även ske för att informera medlemmarna om olika förhållanden som kan vara av intresse för medlemmarna. Behandlingen ska utöver detta ske för att värva medlemmar till Organisationerna.

Behandlingen ska därutöver ske för att Organisation ska kunna fullgöra skyldigheter och tillvarata rättigheter vad gäller redovisning och bokföring och i övrigt på det skatterättsliga området.

Dessutom behandlas personuppgifter för att upprätthålla nödvändig säkerhet i lokaler, utrymmen, eller anläggning som Organisation äger eller disponerar, jämte för att upprätthålla nödvändig säkerhet vad gäller informationssystem som Organisation äger eller disponerar och information som behandlas i sådana system.

Organisationerna kan för sådana ändamål ha gemensam åtkomst till personuppgifterna.

3.2.5. Personuppgifter som omfattas av behandlingen.

Behandlingen kan omfatta följande kategorier av personuppgifter.

- Kontaktuppgifter, bestående i uppgifter om personnamn, adress och postadress, telefonnummer och e-postadress
- Personnummer, när detta är nödvändigt för att säkert kunna identifiera personen eller för att uppgiften måste behandlas vid uppfyllandet av rättslig skyldighet
- Kontouppgifter, bestående i uppgifter om bankkonton och andra konton för att kunna genomföra, mottaga och administrera betalningar, såsom löner, arvoden och andra ersättningar

4. Huvudansvarig Organisation

För behandling av personuppgifter som sker i Organisations verksamhet ska den Organisationen vara huvudansvarig.

Att vara huvudansvarig innebär att Organisationen själv gentemot övriga Organisationer ska svara för att behandlingen av personuppgifter som utförs för Organisationens verksamhet sker i enlighet med tillämplig lag eller annan författning och det avtal, överenskommelser, denna instruktion eller andra dokument som gäller mellan Organisationerna.

För behandling av personuppgifter i BAS-C är SBU huvudansvarig. För behandling av personuppgifter i BAS-F är respektive båtförbund huvudansvarigt. För behandling av personuppgifter i BAS-K är respektive båtklubb huvudansvarig.

5. Dataskyddsombud, kontaktpersoner

5.1. Dataskyddsombud

Organisationerna har bedömt att det inte föreligger någon skyldighet eller behov som medför att Organisationerna måste utse och anmäla något dataskyddsombud till Datainspektionen.

Organisationerna bedriver ingen sådan verksamhet och inte heller behandlas några sådana slags personuppgifter i sådan omfattning där skyldighet att utse och anmäla dataskyddsombud föreligger.

Om dataskyddsombud ändå utses ska denne anmälas till Datainspektionen och information om dataskyddsombudet jämte dennes kontaktuppgifter ska finnas på Organisationernas hemsidor.

Organisationerna kan utse gemensamt dataskyddsombud eller dataskyddsombud för respektive Organisation.

Organisationerna ska tillse att dataskyddsombud som utses och anmäls till Datainspektionen har den kompetens och intar den ställning hos Organisationerna som vid varje tid krävs enligt tillämplig lag eller annan författning för behandling av personuppgifter.

5.2. Kontaktpersoner

Organisationerna kan utse kontaktpersoner som ska vara kontaktyta mellan Organisationerna och de registrerade, mellan Organisationerna och allmänheten och mellan Organisationerna och Datainspektionen.

Kontaktpersonens roll kan i så fall exempelvis vara att svara på frågor angående Organisationernas behandling av personuppgifter, att lämna information och rådgivning till Organisationerna i frågor som angår behandling av personuppgifter och att ha insyn i den behandling av personuppgifter som sker hos Organisationerna.

Organisationerna kan utse gemensam kontaktperson eller kontaktperson för varje Organisation.

Om kontaktperson utses ska information om kontaktpersonen jämte dennes kontaktuppgifter ska finnas på Organisationernas hemsidor.

6. Register över behandling av personuppgifter

Det ska finnas register över den behandling av personuppgifter som sker hos respektive Organisation.

Av registret ska framgå

a) Organisationens namn och kontaktuppgifter,

b) Behandlingens ändamål,

c) Vilka kategorier registrerade och personuppgifter det är fråga om,

d) Vilka kategorier av mottagare som personuppgifterna kan komma att lämnas ut till,

e) Överföring till tredjeland eller internationell organisation,

f) Tidsfrister för gallring, samt

g) Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

Registret ska fortlöpande uppdateras så att det innehåller korrekt, aktuell och adekvat information om behandlingen. Registret ska dokumenteras och finnas tillgänglig på sådant sätt att det snarast kan tillhandahållas, exempelvis i samband med en tillsyn från Datainspektionen.

7. Särskilda krav på behandlingen av personuppgifter

Organisationerna ska undvika att behandla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Detsamma gäller för behandling av uppgifter om fällande domar i brottmål och överträdelser, samt för personnummer.

7.1. Särskilda kategorier eller känsliga personuppgifter

Organisationerna kan behöva behandla särskilda kategorier eller känsliga personuppgifter för ändamål i enlighet med punkt 3 ovan. För det fall sådana slags personuppgifter behandlas, ska Organisationerna särskilt tillse att endast särskilt utsedd personal är behöriga att ha åtkomst till personuppgifterna, att antalet behöriga personer begränsas till vad som är absolut nödvändigt och att åtgärder med sådana slags personuppgifter loggas.

7.2. Personnummer

Personnummer kan i vissa fall vara nödvändiga för att säkerställa identiteten hos den registrerade och för att tillse att personuppgifter inte utlämnas till någon obehörig eller att någon annan åtgärd inte vidtas obehörigen gentemot den registrerade. För det fall personuppgifter innehållande personnummer behandlas, ska Organisationerna särskilt tillse att endast särskilt utsedd personal är behöriga att ha åtkomst till personuppgifterna, att antalet behöriga personer begränsas till vad som är absolut nödvändigt och att åtgärder med sådana slags personuppgifter loggas.

8. Gallring

Organisationerna eller respektive Organisation ska tillse att personuppgifter gallras när de inte längre behövs för de ändamål personuppgifterna behandlats, i enlighet med nedanstående.

8.1. Personaluppgifter

Personuppgifter som avser personal ska gallras senast ett år efter anställningens, uppdragets eller avtalsförhållandets upphörande, om inte annan tid för gallring blir nödvändig till följd av fullgörande av skyldighet eller utövande av rättigheter enligt avtalet eller enligt lag eller annan författning. Om detta föranleder att personuppgifterna behandlas under längre tid ska gallring ske först efter det att de inte längre behövs för uppfyllandet av sådan skyldighet eller utövandet av sådan rättighet.

8.2. Medlemsuppgifter

Personuppgifter som avser medlemskap ska gallras senast ett år efter medlemskapets upphörande, om inte annan tid för gallring blir nödvändig till följd av fullgörande av skyldighet eller utövande av rättigheter enligt avtalet eller enligt lag eller annan författning. Om detta föranleder att personuppgifterna behandlas under längre tid ska gallring ske först efter det att de inte längre behövs för uppfyllandet av sådan skyldighet eller utövandet av sådan rättighet.

9. Säkerhetsåtgärder

9.1. Tekniska säkerhetsåtgärder

Personuppgifterna ska skyddas genom sådana tekniska åtgärder som behövs med hänsyn till personuppgifternas art, behandlingens omfattning och de risker för de registrerades integritet som behandlingen innebär.

9.2. Organisatoriska och administrativa säkerhetsåtgärder

Organisationerna ska vidta sådana organisatoriska och administrativa säkerhetsåtgärder som behövs för att skydda de personuppgifter som behandlas. Detta innefattar bland annat begränsning av behörighetstilldelning så att tillgång till personuppgifterna endast medges sådan personal som behöver ha sådan tillgång för utförandet av sina arbetsuppgifter.

9.3. Automatiserade åtgärder (privacy by design, privacy by default)

Organisationerna ska så långt möjligt och rimligt använda sig av inbyggda säkerhetsåtgärder som inte kräver personella åtgärder, såsom automatisk gallring efter en i förväg bestämd tid, begränsningar avseende registrering av uppgifter i fritextfält, automatisk begränsning av användarbehörigheter eller blockering av vissa slags ord.

9.4. Säkerhetskopiering

Personuppgifterna ska regelbundet säkerhetskopieras. Säkerhetskopior ska förvaras på mellan Organisationerna överenskommet säkert och lämpligt sätt.

9.5. Loggning

Åtgärder med personuppgifter ska loggas. Av sådan logg ska framgå vid vilken tid åtgärden vidtogs, vilken användaridentitet som företog åtgärden och vilket slags åtgärd det varit fråga om. Loggning ska regelbundet följas upp och onormala avvikelser ska föranleda lämpliga åtgärder. Organisationerna ska informera om att loggning sker och följs upp samt att loggningen kan föranleda åtgärder för att hindra obehörig eller otillåten behandling av personuppgifter.

10. Anlitande av personuppgiftsbiträde

Om personuppgiftsbiträde anlitas ska ett personuppgiftsbiträdesavtal ingås med denne som uppfyller de krav på innehåll som anges i GDPR eller annan tillämplig lagstiftning. Respektive Organisation ska ha förteckning över vilka personuppgiftsbiträden denne anlitat. På begäran från annan Organisation ska denne få tillgång till sådan förteckning eller uppgift däri.

11. Den registrerades rättigheter

GDPR tillförsäkrar den registrerade ett antal rättigheter som måste uppfyllas av den personuppgiftsansvarige. Den registrerades rättigheter ska uppfyllas enligt följande.

11.1. Information

Den registrerade ska informeras om behandlingen av dennes personuppgifter i samband med den första kontakten som förekommer med denne. Information om behandlingen ska även finnas lätt tillgänglig på respektive Organisations hemsida och vara tydligt och klart utformad. Information om den registrerades rätt och möjlighet att framföra klagomål hos Organisationerna eller till datainspektionen ska tillhandahållas på motsvarande sätt.

11.2. Registerutdrag

Om begäran om registerutdrag inkommer från en registrerad ska begäran skyndsamt vidarebefordras till den Organisation som är huvudansvarig för den aktuella behandlingen av personuppgifterna. Den huvudansvarige Organisationen ska därefter skyndsamt behandla begäran och uppfylla skyldigheterna att tillhandahålla registerutdraget.

11.3. Rättelse

Om begäran om rättelse inkommer från en registrerad ska begäran skyndsamt vidarebefordras till den Organisation som är huvudansvarig för den aktuella behandlingen av personuppgifterna. Den huvudansvarige Organisationen ska därefter skyndsamt behandla begäran och uppfylla skyldigheterna att genomföra rättelsen.

11.4. Radering eller begränsning

Om begäran om radering av personuppgifter eller begränsning av behandling av personuppgifter inkommer från en registrerad ska begäran skyndsamt vidarebefordras till den Organisation som är huvudansvarig för den aktuella behandlingen av personuppgifterna. Den huvudansvarige Organisationen ska därefter skyndsamt behandla begäran och uppfylla skyldigheterna att radera eller begränsa behandlingen av berörd personuppgift.

11.5. Invändning

Om invändning mot behandling av personuppgifter inkommer från en registrerad ska begäran skyndsamt vidarebefordras till den Organisation som är huvudansvarig för den aktuella behandlingen av personuppgifterna. Den huvudansvarige Organisationen ska därefter skyndsamt behandla invändningen och genomföra de åtgärder som invändningen föranleder.

11.6. Identifiering av den registrerade

Om begäran eller invändning inkommer från en registrerad enligt ovanstående ska rimliga åtgärder vidtas för att identifiera den registrerade och för att säkerställa att begäran eller invändningen verkligen har framställts av den registrerade. Om begäran eller invändningen avser känsliga personuppgifter eller personuppgifter som kan anses särskilt skyddsvärda, ska uppgifter som begärts sändas genom rekommenderad försändelse till av den registrerade angiven postadress. Alternativt ska den registrerade erbjudas att hämta uppgifterna mot uppvisande av giltig legitimationshandling, eller att uppgifterna tillhandahålls den registrerade på annat därmed jämförligt säkert sätt.

12. Ömsesidig informationsplikt

Organisationerna ska ömsesidigt och utan dröjsmål informera varandra om sådana förhållanden som inte oväsentligt kan påverka behandlingen av personuppgifter. Organisationerna ska särskilt informera varandra om personuppgiftsincident eller annan incident som kan påverka behandlingen av uppgifterna och innebära risk för skada eller annan negativ konsekvens för den registrerade.

13. Vid personuppgiftsincident

Organisation som är huvudansvarig för behandlingen av personuppgifterna ska inge en anmälan om personuppgiftsincident till Datainspektionen och informera de registrerade i enlighet med vad som krävs enligt tillämpliga regelverk för behandling av personuppgifter.

13.1. Personuppgiftsincident

Med personuppgiftsincident förstås en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

13.2. Information mellan Organisationerna

Organisation som fått kännedom om personuppgiftsincident eller annan händelse som kan ha betydelse för behandlingen av personuppgifter ska snarast informera övriga Organisationer härom.

13.3. Anmälan till Datainspektionen

Anmälan om personuppgiftsincident ska inges till Datainspektionen utan onödigt dröjsmål och senast inom 72 timmar efter det att Organisation fått kännedom om incidenten.

Anmälan ska innehålla:

a) beskrivning av personuppgiftsincidentens art, jämte uppgift om vilka kategorier registrerade och personuppgifter med en uppskattning av antalet registrerade och personuppgifter som berörs,

b) namn och kontaktuppgifter till dataskyddsombud eller annan kontaktperson hos den Organisation som är huvudansvarig för den berörda behandlingen,

c) uppgift om de sannolika konsekvenserna av personuppgiftsincidenten, samt

d) beskrivning av de åtgärder som vidtagits eller ska vidtas.

13.4. Information till de registrerade

Information om personuppgiftsincident som sannolikt kan medföra hög risk för fysiska personers fri- och rättigheter tillhandahållas de registrerade utan onödigt dröjsmål. Om detta skulle innebära en oproportionerligt stor arbetsinsats ska informationen i stället ske via allmänt tillgängliga media och på Organisationernas hemsida.

Informationen ska åtminstone innehålla:

a) namn och kontaktuppgifter till dataskyddsombud eller annan kontaktperson hos den Organisation som är huvudansvarig för den berörda behandlingen,

b) uppgift om de sannolika konsekvenserna av personuppgiftsincidenten, samt

c) beskrivning av de åtgärder som vidtagits eller ska vidtas.

Svenska Båtunionen
af Pontins väg 6
115 21 Stockholm