Nämnden för båtlivsutbildning, NFB
The Swedish Council for the Education and Training of Yachtsmen

Nämnden för båtlivsutbildning (NFB) Informationssäkerhetspolicy

Personuppgiftshantering inom NFB

Bestämmelser om personuppgiftshantering reglerades tidigare i personuppgiftslagen (PuL).

Från 25 maj 2018 gäller Allmänna Dataskyddsförordningen, som även kallas GDPR (General Data Protection Regulation) och kommer gälla som lag i alla EU medlemsländer. Förordningen kommer att innebära en del förändringar för de som behandlar personuppgifter och stärkta rättigheter för den enskilde när det gäller personlig integritet.

NFB hanterar enbart personuppgifter som nämnden behöver för att utfärda och registerhålla behörigheter och intyg för fritidsbåtslivet.

Informationssäkerhet

Med informationssäkerhet avses skydd av konfidentialitet, riktighet och tillgänglighet hos information i NFB verksamhet.

Med konfidentialitet menas:
Förhållandet att information inte görs tillgänglig eller avslöjas för obehöriga.

Med riktighet menas:
Egenskap hos information som innebär att informationen inte förändras obehörigen, av misstag eller på grund av funktionsstörning. I detta sammanhang är spårbarhet ett viktigt begrepp. Med spårbarhet menas en möjlighet att entydigt kunna härleda utförda aktiviteter och vilken person eller systemfunktion som har utfört dessa.

Med tillgänglighet menas:
En möjlighet att kunna använda information i förväntad utsträckning och inom önskad tid.

Mål och inriktning med informationssäkerheten inom NFB

NFB mål med sin informationssäkerhet är följande:

- Konfidentiell information rörande NFB eller dess medlemmar ska aldrig, oavsett orsak, göras tillgänglig eller avslöjas för obehöriga
- Information rörande personuppgifter ska alltid vara riktig och inte möjlig att manipulera. Om information som registreras är felaktig ska rättelse ske omgående så snart felet upptäckts
- Information om NFB verksamhet i dess årsredovisning ska alltid följa gällande lag och vara rättvisande för verksamheten
- NFB ska alltid ha system för sin informationssäkerhet som tillgodoser juridiska och kommersiella krav att i tid få tillgång till nödvändig information

Inriktningen på arbetet med informationssäkerhet ska vara att från externa leverantörer, som är etablerade på marknaden, få tillgång till system med hög funktionalitet, säkerhet och prestanda som främjar NFB mål med sin informationssäkerhet.

Styrelsen ska vid behov fastställa ytterligare instruktioner och riktlinjer som beskriver hur arbetet med informationssäkerhet ska bedrivas för att följa styrelsens angivna mål och inriktning.

Ansvar och samordning vid informationssäkerhet

Styrelsen är ansvarig för att leda och samordna arbetet med informationssäkerhet. I detta ingår att fördela ansvaret inom NFB för de

arbetsuppgifter som ska utföras. Arbetsuppgifter, men inte tilldelat ansvar, får delegeras till andra inom organisationen.

Riskanalys

Kansliet ska årligen och vid förändringar som har betydelse för informationssäkerheten, analysera föreliggande risker i NFB informationssäkerhet. Identifierade risker ska hanteras. Beslut om åtgärder ska fattas av styrelsen.

Interna regler för informationssäkerhet

Kansliet ska fastställa interna regler för arbetet med informationssäkerhet. Dessa interna regler ska bl. a. omfatta fysisk säkerhet, skydd av datakommunikation och drift, spårbarhet i IT-system och regler för åtkomstbehörigheter till IT-system. De interna reglerna kan vara uppdelade på flera dokument och ska utvärderas regelbundet samt vid behov uppdateras i samråd.

Fysisk säkerhet

Kansliets lokaler ska ha ett skalskydd som innebär att obehöriga inte ges otillbörlig tillgång till NFB dokument och IT-resurser.
Skalskyddet ska inkludera brand- och inbrottslarm kopplat till larmcentral med dygnet runt övervakning. För datakommunikation och drift ska det alltid finnas redundans. NFB ska via loggar kunna se vad respektive individ utfört för förändringar och när. När NFB använder externa leverantörer för stöd i olika delar av verksamheten ska leverantörerna upplysas om de krav NFB har beträffande informationssäkerhet.

Åtkomst till information

Grundläggande för åtkomst till information är att anställda och funktionärer endast ska ha tillgång till den information som behövs för att kunna utföra sina

arbetsuppgifter. Samtliga IT-system ska ha möjlighet att tilldela behörighet efter roller eller på individnivå. IT-systemen ska vara utformade så att åtkomst och behörighet kan anges per funktion eller funktionsgrupp. Det ska också vara möjligt att låta vissa användare se information men inte kunna ändra informationen. NFB ska regelbundet, dock minst årligen, kontrollera att befintliga åtkomstbehörigheter är begränsade till behov utifrån tilldelade arbetsuppgifter.

Rapportering & hantering av incidenter relaterade till informationssäkerhet

Alla incidenter som rör verksamhetskritiska störningar eller incidenter rörande personuppgifter ska rapporteras till styrelsen snarast. I och med att EU:s Dataskyddsförordning kommer NFB att omfattas av regler avseende skyldighet att rapportera incidenter som rör personuppgifter till Datainspektionen.

Raderingsrutiner för personuppgifter

I anslutning till den registrerades rättighet enligt GDPR att bli bortglömd och till reglerna om radering behöver NFB upprätta en intern rutin för hur radering av personuppgifter ska ske.

Avlidna individer ska gallras efter 2 år. Allt detta gäller oavsett om det föreligger skulder på betalning av avgifter eftersom NFB inte kräver in obetalda avgifter efter avlidna.

Utvärdering av interna regler

NFB ska regelbundet utvärdera de interna reglerna och uppdatera dessa om det behövs.