Ålands landskapsregering

PROTOKOLL

Nummer	Sammanträdesdatum
42	**26.10.2021**

Protokoll fört vid enskild föredragning

Social- och miljöavdelningen
Miljöbyrån, S4

Beslutande	Föredragande	Justerat
Minister	Naturvårdsintendent	Omedelbart
Alfons Röblom	Maija Häggblom	

....

Nr 71
Avtal om nyttjanderätt för vissa applikationer för hantering och underhåll av information i Natura 2000-datablanketter och om skilda länders skyddade områden.
ÅLR 2021/9097

Beslut

Beslöts att ingå avtal med Forststyrelsen för rätten att använda vissa applikationer i deras system för hantering av SASS-applikationen (Informationssystem för planering och uppföljning av skyddade områden) och SATJ-applikationen (Informationssystem för skyddade områden) inom ULJAS-systemhelhet i enlighet med **bilaga S421E42**.

AVTAL OM NYTTJANDERÄTT TILL SASS- OCH SATJ-APPLIKATIONERNA I FORSTSTYRELSENS ULJAS-SYSTEMHELHET

1 Avtalsparter

Överlåtare av nyttjanderätt: Forststyrelsen (”**Forststyrelsen**”)
FO-nummer: 0116726-7
Adress: PB 94, (Banvägen 11), 01301 Vanda
Kontaktperson för överlåtare av nyttjanderätt:
Heikki Eeronheimo
Kontaktuppgifter: telefon 020-6397696; e-post heikki.eeronheimo@metsa.fi

Mottagare av nyttjanderätt: Ålands landskapsregering (”**Mottagare av nyttjanderätt**”)
FO-nummer: 0145076-7
Adress: Pb 1060, AX-22111 Mariehamn
Kontaktperson för mottagaren av nyttjanderätt:
Naturvårdsintendent Maija Häggblom
Kontaktuppgifter: telefon 018-25458; e-post maija.haggblom@regeringen.ax

(Forststyrelsen och mottagaren av nyttjanderätt nedan kallade tillsammans ”avtalsparter”)

2 Definitioner

”Användare” avser en person i tjänste- eller anställningsförhållande som är Mottagare av nyttjanderätt, eller inhyrd personal eller konsulter som på basis av ett avtal med en Mottagare av nyttjanderätt sköter motsvarande uppgifter.

”ICT-tjänsteleverantör” avser de grundläggande tjänsteleverantörer av datateknik som används av Forststyrelsen och andra Forststyrelsens avtalspartner relaterade till underhåll eller tjänster för de system som avses i detta avtal.

”Forststyrelsens IdM-system” (s.k. Mimmi-system) avser ett system som hanterar både användarnamn för Forststyrelsens slutna företagsnätverk samt systemens nyttjanderätter.

”Avtal” avser detta avtal om nyttjanderätt med dess bilagor.

”Applikationer” avser SASS- och SATJ-applikationer som hör till ULJAS-systemhelheten.

”ULJAS-systemhelhet” avser Forststyrelsens ESRI-baserade geografiska informationssystem som fungerar i en datateknisk miljö, som inkluderar delapplikationer avsedda för olika ändamål.

3 Avtalets syfte och nyttjanderättens innehåll

Avtalsparterna har för avsikt att komma överens om användarvillkoren för SASS-applikationen (Informationssystem för planering och uppföljning av skyddade områden) och SATJ-applikationen (Informationssystem för skyddade områden) för ULJAS-systemhelhet som arbetar i Forststyrelsens IT-miljö som beviljas Mottagare av nyttjanderätt genom IdM-systemet enligt villkoren i detta avtal om nyttjanderätt (Avtalet).

Enligt detta avtal har Mottagare av nyttjanderätt och Användarna rätt att använda applikationerna och behandla de uppgifter som finns däri endast under villkoren i detta Avtal för underhåll av information i Natura 2000-datablanketterna och om privata länders skyddade områden (YSA) och endast under avtalets giltighetstid. För tydlighetens skull konstateras att nyttjanderätten enligt detta Avtal inte är en ensamrätt.

4 Forststyrelsen rättigheter och skyldigheter

ULJAS-systemhelheten som används i Forststyrelsens IT-miljö fungerar i maskinsalen hos Forststyrelsens ICT-tjänsteleverantör. Tjänsteavtalen mellan Forststyrelsen och ICT-tjänsteleverantören definierar tjänstenivåer (SLA), enligt vilka Forststyrelsen strävar efter att erbjuda rätten för Mottagare av nyttjanderätt att använda Applikationerna i enlighet med detta Avtal. Forststyrelsen ger emellertid ingen säkerhet eller garanti enligt detta Avtal avseende applikationernas funktion eller användbarhet i enlighet med någon viss tjänstenivå.

Forststyrelsen har rätten, som beskrivs i detta Avtal, att kontrollera användningen av nyttjanderätter och relaterade åtgärder, bland annat för att förhindra situationer av missbruk och/eller avtalsbrott.

5 Rättigheter för Mottagare av nyttjanderätt

Mottagare av nyttjanderätt kan be om nyttjanderätt för Användarna i sin organisation enligt detta Avtal. På ovanstående begäran kan Forststyrelsen bevilja Användare följande rättigheter till Applikationerna och Forststyrelsens IT-miljö:

1. ID för Windows-nätverket.
2. Reissu-tjänstens Internet-användning.
3. Nyttjanderätter till Applikationer och nätverksenheter som Användaren behöver för att utföra sina arbetsuppgifter.

Mottagare av nyttjanderätt ansvarar för att varje Användare använder rättigheterna endast för de uppgifter som kräver användning av Applikationerna för att kunna utföras. Användning av rättigheterna för andra uppgifter utan separat tillstånd är förbjuden. Avtalsenlig Nyttjanderätt kan inte i något avseende överlåtas utan Forststyrelsens specifika skriftliga godkännande på förhand.

6 Skyldigheter för Mottagare av nyttjanderätt

Mottagare av nyttjanderätt för kvaliteten och riktigheten på all data/material som Användarna matar in i Applikationerna

a) De rättigheter som Användarna har blivit beviljade är personliga. Mottagaren av nyttjanderätt ansvarar för Användarnas aktiviteter till Forststyrelsen. Mottagaren av nyttjanderätt ska tillhandahålla Användarna med information om följande skyldigheter, Mottagaren ansvarar för Forststyrelsen att de följs. Mottagaren av nyttjanderätt förbinder sig att följa Forststyrelsens principer för informationssäkerhet och dataskydd (**bilaga 1**) Mottagaren av nyttjanderätt förbinder sig att göra dem kända för Användaren, Mottagaren av nyttjanderätt ansvarar för att Användaren följer principerna.
b) Det är förbjudet att logga in i systemet med felaktigt/någon annans personliga användarnamn och att överskrida behörigheterna för sitt eget användarnamn.
c) Det är strängt förbjudet att överlåta identifierare, lösenord eller nycklar.

d) Det är förbjudet att kringgå eller försöka kringgå kvoter och andra användningsrestriktioner.
e) Obehörig modifiering eller försök att modifiera hårdvara eller programvara är förbjuden.
f) Tillvägagångssätt som av den internationella nätgemenskapen allmänt anses vara olämpliga, inklusive osakliga masspostningar, kedjebrev samt spridande av datavirus är förbjudna.
g) Obehörig kopiering, innehav eller distribution av program eller filer är förbjudet.

Mottagare av nyttjanderätt och Användare är även skyldiga att följa andra instruktioner som utfärdats av Forststyrelsen relaterade till användningen av Applikationerna under giltighetstiden för detta Avtal. Mottagare av nyttjanderätt måste hålla Användarna medvetna om eventuella instruktioner och ändringar i instruktionerna. Dessutom kräver Forststyrelsen att Användare undertecknar ett separat personligt sekretess- och informationssäkerhets-åtagande i enlighet med modellen i **bilaga 2** innan de börjar använda applikationerna.

7 Immateriella rättigheter

På basis av detta Avtal överlåts inga immateriella rättigheter till den andra avtalsparten. Alla rättigheter till Applikationerna hör ändå till Forststyrelsen och/eller till deras avtalsparter. För tydlighetens skull konstaterats att Forststyrelsen har nyttjanderätten till det datamaterial som finns i Applikationerna eller som matas in i dem, och mottagare av nyttjanderätt i enlighet med omfattningen av deras nyttjanderätt.

8 Användarhantering och användarstöd

Mottagaren av nyttjanderätt lämnar in ett sekretess- och informationsskyddsåtagande enligt bilaga 2, undertecknat av Användaren, varefter Forststyrelsen ger Användarna nyttjanderätt enligt detta Avtal. Forststyrelsen ska bli informerade om ändringar i användardata och uppsägning av användningsrättigheter på ett sätt som avtalas separat.

För tydlighetens skull konstateras att det enligt detta Avtal inte är Forststyrelsens uppgift att hålla jour eller annan tjänst som påminner om helpdesk/servicedesk för Mottagare av nyttjanderätt eller Användare. [.]

9 Övervakning av nyttjanderätt och påföljder

Forststyrelsen har rätt att med de metoder som de har i sin användning övervaka att nyttjanderätterna följs. Otillåten användning av nyttjanderätterna (inkl. missbruk av informationssystem och datanätverk) annat avtalsbrott som begås av Mottagaren av nyttjanderätt ger Forststyrelsen rätt att säga upp detta avtal med en skriftlig anmälan med omedelbar verkan och omedelbart ta bort alla Användares nyttjanderätter till Applikationerna. För tydlighetens skull konstateras att Användares verksamhet som strider mot Avtalet betraktas som avtalsbrott av Mottagare av nyttjanderätt. Om förseelsen som nämns ovan är mindre och kan åtgärdas kan Forststyrelsen ge Mottagaren av nyttjanderätt möjlighet att rätta till sitt förfarande innan avtalet sägs upp.

Ovan nämnda missbruk av informationssystem och datanätverk innebär all aktivitet som stör användningen av systemen för deras avsedda ändamål, stör datanätverket som systemet är anslutet till eller annat system som hör till detta nätverk, bryter mot reglerna, använder delar eller funktioner av systemet som är förbjudna i instruktionerna, eller är annars förbjudet av Forststyrelsen eller systemadministratören.

10 Avtalsparternas bidrag

Avtalsparterna ansvarar för sin egen del för att avtalsparten fattar nödvändiga beslut i samband med detta Avtal utan onödigt dröjsmål och åtar sig att utan onödigt dröjsmål skriftligen informera den andra Avtalsparten om alla frågor som kan försena eller försvåra fullgörandet av deras skyldigheter enligt detta Avtal.

Om en avtalspart försummar sin bidragsskyldighet och den andra avtalsparten på grund av detta inte kan genomföra sina skyldigheter enligt avtalet, måste denna avtalspart utan dröjsmål skriftligen meddela avtalsparten som försummat sin bidragsskyldighet om detta.

11 Skadeståndsansvar

Avtalsparten är skyldig att ersätta den andra avtalsparten för direkta skador som avtalsparten själv eller Användare i dess organisation har orsakat. Om avtalsparten eller en Användare i dess organisation har orsakat skadan avsiktligt eller genom grov vårdslöshet eller brott mot tystnadsplikten (punkt 12), ansvarar avtalsparten även för indirekta skador. I andra avseenden är avtalsparten inte skyldig att ersätta indirekta skador orsakade av Användaren i dess organisation.

Mottagare av nyttjanderätt har inte rätt att erhålla skadestånd från Forststyrelsen för skador orsakade av overksamhet, förseningar och/eller fel i nyttjanderättigheterna, Applikationerna och/eller ULJAS-systemhelheten.

12 Informationshantering och sekretess

Forststyrelsen är en informationshanteringsenhet enligt lagen om informationshantering inom den offentliga förvaltningen (906/2019), som är skyldig att följa informationssäkerhets- och andra skyldigheter relaterade till informationshantering i lagen i fråga. Avtalsparterna åtar sig att följa skyldigheterna enligt lagen om informationshantering samt övriga informationssäkerhetsarrangemang som avtalsparterna har kommit överens om för att säkerställa informationssäkerhet och dataskydd vid användningen av Applikationerna och vid behandlingen av de datamängder som finns där.

Mottagaren av nyttjanderätt ser till att den utrustning som används och tjänsteproduktionens utrymmen är tillräckligt skyddade mot säkerhetsrisker och att förfaranden relaterade till kryptering och datasäkring följs. Mottagaren av nyttjanderätt ser till att de uppgifter som hanteras är tillräckligt skyddade mot olaglig eller oavsiktlig förlust eller förstörelse.

I den utsträckning som uppgifterna i Applikationerna innehåller personuppgifter som avses i dataskyddslagstiftningen har Mottagare av nyttjanderätt eller Användarna ingen rätt att behandla dessa uppgifter utanför EU eller EES, och inte heller överföra eller överlåta dessa uppgifter till tredje parter utan Forststyrelsens skriftliga medgivande i förhand. Dessutom ska Mottagaren av nyttjanderätt följa bestämmelserna om god databehandling och dataskydd som krävs enligt tillämplig dataskyddslagstiftning med

avseende på personuppgifter. Mottagaren av nyttjanderätt ansvarar för att behandlingen av personuppgifter som den ansvarar för följer gällande dataskyddslagstiftning och kraven i Avtalet.

Avtalsparterna iakttar tystnadsplikt för uppgifterna i Applikationerna enligt vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet. Avtalsparterna ansvarar för att alla Användare i deras organisationer iakttar denna skyldighet. Tystnadsplikten gäller även efter att avtalet har upphört- Tystnadsplikten gäller inte sådan information som är allmänt tillgänglig eller offentlig, eller som avtalsparten lagligen har fått tillgång till på annat sätt än från den andra avtalsparten.

13 Överföring och ändring av avtalet

En Avtalspart har inte rätt att överföra ens en del av avtalet, eller de avtalsenliga rättigheterna eller skyldigheterna till en tredje part utanför Avtalet utan den andra partens skriftliga godkännande i förhand.

Ändring av avtalet är endast möjligt genom ett ändringsavtal som är undertecknat av båda avtalsparterna.

14 Avtalet och avtalsorder

Detta Avtal består av detta avtalsdokument och följande bilagor:
1. Forststyrelsens principer för informationssäkerhet och dataskydd
2. Sekretess- och säkerhetsåtagande (mall)

I händelse av en konflikt mellan avtalsdokumentet och bilagorna, är det formuleringen i avtalsdokumentet som avgör. I händelse av en konflikt mellan bilagorna ska företrädesordningen vara deras nummerordning så att vid en konflikt ska bilagan med den lägre ordningsföljden ha företräde.

15 Avgörande av tvister

Man strävar efter att lösa tvister som uppstår på grund av tolkningen eller tillämpningen av detta avtal genom samråd mellan parterna. Tvister som uppstår till följd av eller i samband med avtalet och som inte kan lösas genom förhandlingar, ska i första hand lösas av tingsrätten i Östra Nyland.

16 Giltighet

Detta avtal är giltigt tills vidare.

Vardera parten kan säga upp detta avtal skriftligen med två (2) månaders uppsägningstid, varmed Användarnas nyttjanderätt upphör då Avtalet upphör.

17 Kopior av avtalet och underskrifter

Detta Avtal har uppgjorts i två (2) likalydande exemplar, ett (1) för vardera avtalsparten.

Datum: _____.10.2021

Ålands landskapsregering

_____
Bengt Michelsson
Avdelningschef för
Social- och miljöavdelningen

_____
Maija Häggblom
Naturvårdsintendent

Datum: _____.10.2021

Forststyrelsen

_____
Henrik Jansson
Direktör för naturtjänster

_____
Minja Vitikka
Direktör för digitala och
kundtjänster

Bilagor:
1. Forststyrelsens principer för informationssäkerhet och dataskydd
2. Sekretess- och säkerhetsåtagande (mall)

METSÄHALLITUS
FORSTSTYRELSEN
MEAHCIRÁÐÐEHUS

12.2.2019

Principer för informationssäkerhet och dataskydd

Innehåll

Mål

Forststyrelsens principer för informationssäkerhet och dataskydd är en del av Forststyrelsens informationshanteringspolicy. Principerna definierar Forststyrelsens centrala linjedragningar, praxis och arbetsmetoder i frågor som gäller informationssäkerhet och dataskydd. Principerna gäller för hela
Forststyrelse-koncernen, alla dess ansvarsområden och övriga funktioner, inklusive dotterbolag (ägandeandel > 50 %). Förutom de som är i anställnings- och tjänsteförhållande med Forststyrelsen gäller principerna även de personer som har blivit beviljade separat nyttjanderätt till Forststyrelsens informationssystem.

Genom att följa dessa principers säkerställs lagenlig behandling av personuppgifter och andra uppgifter, samt att informationssäkerheten och dataskyddet är på en tillräcklig nivå. Principerna täcker de olika faserna av databehandlingsaktiviteter, från planering av informationssystem till långvarig eller permanent lagring av nödvändiga data och snabbt avlägsnande av onödig data. I all verksamhet och på alla ställen genomförs tillräcklig säkerhet och dataskydd enligt standard (security by default, privacy by default).

Dessa principer och andra anvisningar som har utfärdats i frågan ska följas på alla organisationsnivåer och i all verksamhet. Förutom vid anställning måste principerna också följas bl.a. vid resa och fritid om tjänster och system som är avsedda för användning inom Forststyrelsen, eller om Forststyrelsens uppgifter som inte är offentliga behandlas.

Informationssäkerhetens mål är att hos den information och de digitala funktioner som behövs i Forststyrelsens verksamhet garantera:

- Tillgänglighet, användbarhet och funktionalitet: informationen är tillgänglig för de som har rätt till den och kan användas vid behov, de digitala funktionerna fungerar på det sättet som processen förutsätter.
- integritet, bevarande, noggrannhet, originalitet, ursprunglighet och obestridlighet: uppgifterna ändras inte och förstörs inte okontrollerat, uppgifterna är vad de borde vara och kommer varifrån de hävdas komma, innehållet är oförändrat och förekomsten och innehållet av relaterade händelser kan bevisas även på efterhand, samt
- Tillförlitlighet: användning av- och behandlingsrättigheter till uppgifterna har begränsats på basis av arbetsuppgifterna endast till de som har rätt att använda dem.

Med hjälp av dataskyddsprinciperna skyddar Forststyrelsen kundernas, avtalspartnerna och de anställdas rättigheter samt även rättigheterna för de personer som hör till andra intressentgrupper. Med principerna säkerställs dessutom att behandlingen av personuppgifter inom Forststyrelsen görs enligt EU:s allmänna dataskyddsförordning och kompletterande lagstiftning samt att skyldigheten att tillhandahålla information i enlighet med förordningen uppfylls.

Ansvar och organisation

Informationssäkerhetsarbetet koordineras centraliserat från koncernens informationshantering. Dataskyddsarbetet har däremot separerats från informationstjänsterna till en del av riskhanteringen. Genomförandet av informationssäkerheten och dataskyddet är ändå en kontinuerlig och omfattande verksamhet där allas samarbete behövs.

Varje anställd på Forststyrelsen eller användare av Forststyrelsens system eller tjänster deltar i genomförandet och övervakandet av informationssäkerheten samt ansvarar för att ta hänsyn till informationssäkerhet och dataskydd i all sin verksamhet. Varje person som

använder Forststyrelsens system bör vara medveten om behovet av informationssäkerhet och dataskydd samt förstå vad han eller hon kan göra för att främja dem. Alla måste följa de anvisningar som har utfärdats i relation till informationssäkerhet och dataskydd.

Dessutom måste varje anställd på Forststyrelsen som i samband med sina uppgifter hanterar personuppgifter känna till och behärska den centrala dataskyddslagstiftningen.

Genom att utbilda personalen säkerställs tillräckligt kunnande. Alla deltar i den utbildning som erbjuds på den nivå som krävs för ens uppgifter.

Den verkställande direktören har övergripande ansvar för genomförandet av informationssäkerheten och dataskyddet som en del av Forststyrelsens övergripande säkerhet.

IT-direktören ansvarar för resurser och organisering av informationssäkerhet på koncernnivå. IT-direktören förstärker anvisningar relaterade informationssäkerhet. Ekonomidirektören ansvarar för dataskyddet.

Ansvarsområdens chefer ansvarar för att tillhandahålla informationssäkerhet och dataskydd för sitt ansvarsområde i den mån detta inte görs på koncernnivå. I rollen som ägare av informationssystem fungerar cheferna också som ägare av informationen i systemen.

Ledningsgruppen för informationshantering förbereder besluten för utvecklingsprojekt relaterade till informationssäkerhet och dataskydd samt prioritering av dem i Forststyrelsens ledningsgrupp på dataskyddschefens och den dataskyddsansvariges förslag. Direktören för informationssäkerhet och dataskyddsansvarige rapporterar om viktiga frågor relaterade till informationssäkerhet och dataskydd direkt till Forststyrelsens ledningsgrupp och styrelsens revisionskommitté.

Dataskyddschefen ansvarar för ledning, utveckling, vägledning, övervakning och kontroll av informationssäkerheten samt även kommunikation och stöd av informationssäkerheten. Dataskyddschefens uppgift är att säkerställa och övervaka genomförandet av Forststyrelsens informationssäkerhet. Dataskyddschefen är gemensam för hela Forststyrelsekoncernen och han eller hon rapporterar till IT-direktören. Till hans eller hennes uppgifter hör även att utbilda och vägleda personalen, säkerställa att informationssäkerhetsskyldigheterna följs i Forststyrelsens vardaglig verksamhet, och verka som kontaktperson till myndigheters och samarbetsparter i frågor relaterade till informationssäkerhet. Direktören för informationssäkerhet upprätthåller situationsbilden över Forststyrelsens informationssäkerhetsrisker.

Enheten för informationstjänster stöder i sin verksamhet dataskyddschefen och utser från sin grupp en reservperson för dataskyddschefen.

Den dataskyddsansvarige ansvarar för ledning, utveckling, vägledning, övervakning och kontroll av dataskyddsarbetet samt för kommunikation av dataskyddet och stöd av dataskyddsarbetet.
Dataskyddsansvariges uppgift är att säkerställa och övervaka genomförandet av Forststyrelsens dataskydd. Dataskyddsansvarige är gemensam för hela Forststyrelsekoncernen. Dataskyddsansvarige arbetar självständigt. Han eller hon rapporterar direkt till Forststyrelsens högsta ledning. Till hans eller hennes uppgifter hör att utbilda och vägleda personalen, säkerställa att dataskyddsskyldigheterna följs i Forststyrelsens vardagliga verksamhet och verka som kontaktperson till myndigheter och registrerade.

Enheten för juridiska frågor stöder den dataskyddsansvarige i dess verksamhet och utser en biträdande dataskyddsansvarig bland sina medlemmar.

Direktören för verksamhetslokalerna ansvarar för verksamhetslokalernas fysiska informationssäkerhet, till exempel åtkomstkontroll och förvaringslösningar i verksamhetslokalerna samt säker återvinning av material från det fysiska datamaterialet som

ska avlägsnas från användning. Direktören för verksamhetslokalerna ser till att informationssäkerhet och dataskydd har beaktats i avtal relaterade till verksamhetslokalerna på den nivå som verksamheten förutsätter.

Utomstående aktörer som har att göra med Forststyrelsens informationssystem, eller som har blivit beviljade åtkomsträtt till Forststyrelsens faciliteter följer de riktlinjer de har fått från Forststyrelsen eller de allmänna riktlinjerna för informationssäkerhet från statsförvaltningen, om inte annat anges.
Vid behov avtalas det om säker behandling av information i avtal med de organisationer och övriga samarbetsparter som behandlar Forststyrelsens uppgifter.

Forststyrelsen har rätt att övervaka uppfyllandet av principerna och riktlinjerna för informationssäkerhet och dataskydd, och riskhanteringschefen koordinerar övervakningen av verksamheten.

Dataskyddsorganisationer

Forststyrelsen är en särskild dataskyddsorganisation som består av dataskyddsansvarig, representant för juridiska frågor samt av representanter för enheten för Informationstjänster och registeransvariga inom Forststyrelsens koncernenhet och ansvarsområden. Denna dataskyddsorganisation har det övergripande ansvaret för organisationen och hanteringen av dataskydd i Forststyrelsen.
Registeransvariga sörjer för lagenlig behandling av personuppgifterna för de personregister som de ansvarar för. Dataskyddsorganisationen ansvarar även för dataskyddet då behandlingen av uppgifterna utlokaliseras. Den ser till att den valda partnern följer dessa dataskyddsprinciper. Då behandlingen av personuppgifter utlokaliseras utarbetas alltid ett skriftligt avtal där parternas ansvar och skyldigheter definieras.

Anmälningsskyldighet

Verksamhet som strider mot informationssäkerhets- och dataskyddsprinciperna samt övriga säkerhetsavvikelser, till exempel anordningar, lösenord och nycklar som har hamnat i fel händer måste omedelbart anmälas till förmannen eller dataskyddschefen (tietoturva@metsa.fi) och dessutom måste man omedelbart vara i kontakt med användarstödet eller så bör man agera enligt andra instruktioner.

Avvikelser i dataskyddet måste omedelbart anmälas till dataskyddsansvarige (tietosuoja@metsa.fi) eller så bör man agera enligt andra instruktioner.

Informerande av personal, registrerade och intressenter

Forststyrelsens personal informeras om dessa informationssäkerhets- och dataskyddsprinciper samt om ändringar i dem via intranet, och annars vid behov. Principerna för Informationssäkerhet och dataskydd granskas och uppdateras vid behov till exempel när lagstiftningen eller dess tillämpningspraxis ändras. Vid informering av registrerade och intressenter iakttas, då det är tillämpligt, det som anges nedan vid punkten Informering av registrerade.

Dataskyddspraxis

Behandlingskriterier och -principer

Behandlingen av personuppgifter baserar på sig på kriterier som definieras i dataskyddsförordningen eller -lagen. Personuppgifter behandlas endast för definierade ändamål och i enlighet med principerna i dataskyddsförordningen. När uppgifterna inte längre är nödvändiga för ändamålet arkiveras eller förstörs uppgifterna på ändamålsenligt sätt.

Uppgifterna används för de ändamål som beskrivs när de samlas in. Forststyrelsen överför inte personuppgifter utanför EES. Forststyrelsen kräver det samma av sina utlokaliseringspartners. Endast i enskilda fall och i fall som motiveras av Forststyrelsens verksamhet, såsom i fall av utlokalisering, kan personuppgifter överföra personuppgifter

utanför EES. På så sätt säkerställs att överföringen sker i enlighet med dataskyddsförordningen.

Informering av registrerade

Personuppgiftsansvarig för de personuppgifter som behandlas av Forststyrelsen är Forststyrelsekoncernen, eller ett företag som hör till Forststyrelsekoncernen för vars ändamål personuppgifterna har samlats in. Enligt gällande lagstiftning utarbetas dokumentation över behandlingen av personuppgifter för att påvisa ansvarsskyldighet. Vid insamling av uppgifter, samt även på andra sätt, t.ex. på Forststyrelsens nätsidor får den registrerade information som avses i förordningen eller som övrigt är nödvändig för behandling av personuppgifter.

Säkerställande av dataskydd

Användningen av informationssystem som innehåller personuppgifter kontrolleras av Forststyrelsekoncernens lösning för användarhantering. Alla register och system skyddas med tekniska lösningar (bland annat brandväggar) på ett sätt som fastställs i lag och god datahanteringspraxis.
Loggdata samlas in separat från alla register med lagstadgad eller på annat sätt tillräcklig noggrannhet och de övervakas regelbundet. Om det finns en misstanke om, eller man lägger märke till att dataskyddet har äventyrats ska saken undersökas omedelbart. Dessutom informeras det om saken på ett sätt som krävs enligt dataskyddsförordning. Alla aktiviteter som strider mot lagstiftningen om behandling av personuppgifter, dataskyddsprinciper eller riktlinjer som utfärdas på grundval av dessa undersöks så att Forststyrelsen kan reagera på informationssäkerhetsöverträdelser med nödvändiga åtgärder.

Informationssäkerhetspolicy

Allmänna informationssäkerhetspolicyer

Att skydda information och informationssystem är en del av Forststyrelsens riskhantering och säkerställande av verksamhetens kontinuitet. Informationssäkerhetsåtgärder baserar sig på riskhantering av objekt som ska skyddas (t.ex. system, funktion, datamängd).

Vid informationssystemens utvecklingsprocesser måste avtalade verksamhetsmodeller- och sätt följas. Processen innehåller också nödvändiga kontrollpunkter för tillräcklig informationssäkerhet och dataskydd.

Alla system som innehåller personuppgifter måste genomgå en dataskyddsgranskning och en informationssäkerhetsgranskning och tjänster som bedöms vara viktiga för verksamheten måste genomgå en informationssäkerhetsgranskning innan de förs vidare för produktion.

Befintliga system som är viktiga för verksamheten genomgår regelbundet återställningstester samt dataskydds- och informationssäkerhetsgranskningar, minst en gång i året för system som bedömts som kritiska. För system i produktion ligger ansvaret på direktören för tjänsteområdet.

Hantering av nyttjanderätter och lösenordspraxis

Alla användarnamn och beviljade tillstånd är personliga. Forststyrelsens användarnamn och nyttjanderätter samt radering av användardata har separata principer som personaladministrationen beslutat om.

Det är strängt förbjudet att överlåta eller låna ut användarnamn, lösenord och nycklar relaterade till tillstånd. Det enda undantaget från ovanstående är överlåtande till underordnad av ett nytt lösenord som förmannen gjort, om lösenordet inte har kunnat levereras direkt till användaren på grund av att den underordnade saknar mobiltelefonnummer.

Forststyrelsens använder centraliserad hantering av användarrättigheter alltid när det är möjligt. Målet är att nyttjanderättighets- och åtkomsthantering av alla Forststyrelsens system

genomförs med en gemensam lösning för identitetshantering (IdM). Systemens ägare definierar kriterierna för beviljande av nyttjanderätt. Även utomstående användares rättigheter hanteras centraliserat.

Vid rättigheter följs principen om minst privilegium. Varje användare har de rättigheter och tillstånd som han eller hon behöver på basis av sina arbetsuppgifter. Rättigheter som blir överlopps måste tas bort när de inte längre behövs. Vid normal användning får endast användarnamn som är avsedda för normal användning användas. Administratörs-ID som möjligen har beviljats separat får endast användas vid enskilda åtgärder då det behövs.

När man försöker identifiera en användare strävar man alltid efter engångsinloggning och efter att använda den centraliserade användarkatalogen (Windows AD) eller andra av Forststyrelsens standardiserade autentiseringsmetoder. I de nyare systemen är separat inloggning endast tillåtet med undantagstillstånd av IT-direktören.

I internettjänsterna strävar man efter att alltid använda stark användarautentisering (till exempel tvåstegsautentisering).

Kraven på lösenorden har registrerats i separata instruktioner och måste implementeras som tekniska begränsningar, om det är möjligt.

Det är förbjudet att försöka komma in i systemet med ett felaktigt användarnamn och att överskrida eller försöka överskrida behörigheten för sina egna användarkoder. Det är förbjudet att kringgå eller försöka kringgå kvoter och andra användningsrestriktioner. Användarkoderna och rättigheterna är endast avsedda för det sitt specifika ändamål och får inte användas för något som strider mot ändamålet eller på annat sätt är olämpligt.

Det personliga arbetsrelaterade användarnamnet och lösenordet får inte användas för att registrera sig i andra tjänster i personliga syften.

Logghantering

När man använder Forststyrelsens informationssystem och nätverk lagras data på servrar och arbetsstationer. Logginformation genereras i t.ex. e-postsystem, brandväggar, av serverinloggningar, då man använder databaser, webbplatser och informationssystem.

I Forststyrelsens informationssystem och nätverken kan man samla in och hantera loggar:

- för att reda ut problem i systemet och hos dess användare,
- för att övervaka systemets funktion och problem för att stödja förebyggande åtgärder,
- för att övervaka organisationens säkerhet och dataskydd,
- för att reda ut interna och externa missbruk och trakasserier i organisationen,
- för att samla in faktureringsinformation,
- för att utveckla systemen,
- för kapacitetmätningar och
- statistikföring

Hanterare av loggdata är begränsade loggspecifikt till de som behöver dem i sitt arbete. Hanterarna av loggdata har lagenlig tystnadsplikt om den information de erhåller.

Vid behov måste ett sekretessavtal ingås med personerna, i de fall då den lagstadgade skyldigheten inte är tillräcklig för ändamålet. Detta gäller också t.ex. samarbetspartners och journalister.

Sekretessavtalen måste även gälla tredje parter samt fortsätta en tillräckligt lång tid efter att avtalet har upphört. Ett personuppgiftsregister utformas alltid av användarnas loggdata och vid behandling av uppgifterna måste kraven i dataskyddsförordningen alltid följas.

Kontinuitetshantering, beredskap och återhämtning

Ansvarsområdena och koncernfunktionerna ansvarar för det egna områdets kontinuitets- och återhämtningsplanering. Ansvarsområdena och koncernfunktionerna måste identifiera de tjänster, system och processer som är kritiska för verksamheten och kärnprocesserna, samt utarbeta kontinuitets- och beredskapsplaner för dessa i syfte att trygga verksamhetens kontinuitet både i normala situationer samt vid störnings- och undantagssituationer. Planerna måste vara uppdaterade och att agera enligt dem måste tränas tillräckligt regelbundet. Koncernfunktionerna koordinerar planeringen och genomförandet. När det kommer till ICT-frågor är det direktören för tjänsteområdet som har koordineringsansvaret. Direktören för informationssäkerhet hjälper till vid utarbetandet och upprätthållandet av kontinuitetsplanerna.

Databehandling

Forststyrelsens principer och ansvar för hantering av data- och dokumentmaterial definieras i principerna för dokumenthantering och arkivering. Databehandlingen styrs av Forststyrelsens informationsstyrningsplan, som bl.a. inkluderar kriterier för lagring av material samt offentlighetsklasser.

Information kan förekomma bl.a. i elektroniskt eller pappersformat, på film, lagringsanordning eller i tal. Oberoende av dess format måste informationen behandlas omsorgsfullt under hela dess livscykel. Informationsmaterialet måste klassificeras på basis av dess innehåll, och relaterade begränsningar måste beaktas i alla av informationens behandlingsskeden- och ställen. Utomståendes åtkomst till informationsmaterialet eller systemen måste förhindras i enlighet med informationens offentlighet. Om sekretessbelagd information och personuppgifter hamnar i fel händer måste det omedelbart anmälas på det sätt som beskrivs vid punkten anmälningsskyldighet.

Distansbehandling av sekretessbelagd information ska undvikas. Om detta ändå är oundvikligt måste man se till att utomstående inte får tillgång till informationen bland annat genom att hindra att det inte finns extra ögon, kameror, öron eller mikrofoner i omgivningen. Speciell noggrannhet bör iakttas på offentliga platser, så som i kollektivtrafik, på stationer och caféer.

Gällande behandlingsinstruktioner måste alltid följas vid behandling av personuppgifter. Ansvarspersonen för varje system, som utarbetar och upprätthåller behandlingsinstruktionerna, ansvarar för behandlingsinstruktionerna. Dataskyddsansvarige hjälper till vid utarbetandet och upprätthållandet av instruktionerna och övervakar deras lagenlighet och att de följs.

Användning av datamaskin

Datamaskin och system får endast användas med personliga användarnamn eller med ett separat ID för samanvändning, i de fall då en sådan har utfärdats för användning. Obehörig användning av maskinen och systemen medan man är borta måste förhindras genom att stänga av eller låsa maskinen varje gång man lämnar den. Anordningar får inte lämnas oövervakade i offentliga utrymmen.

Det är förbjudet att använda och installera andra program och applikationer än de som Informationstjänsterna har godkänt. Detta gäller i första hand även sådana applikationer som man inte måste installera, till exempel lagringstjänster som finns på Internet. Installationerna sker centraliserat av tjänsteleverantören.

Endast anordningar som har blivit godkända av Informationstjänsterna får kopplas till Forststyrelsens informationsnät, och inget sekretessbelagt material får finnas på dem. Detta gäller inte nätverk som publiceras separat för dessa ändamål, t.ex. nätverk avsedda för användning av besökare på vilka separata riktlinjer tillämpas.

Obehörig kopiering, innehav eller distribution av program eller dokument är förbjudet. Obehörig modifiering eller försök att modifiera hårdvaran och programvaran är förbjuden.

Att söka efter och använda kända eller nya informationssäkerhetsbrister är förbjudet utan systemadministratörens specifika tillstånd. Upptäckta eller misstänkta informationssäkerhetsbrister ska utan dröjsmål rapporteras till den person som är ansvarig för systemet och till direktören för informationssäkerhet.

En tillräcklig nivå av informationssäkerhet och dataskydd måste beaktas i alla Forststyrelsens nätverk eller Forststyrelsens enheter för databehandling. Enheternas livscykler måste också hanteras ur ovanstående synvinkel. Ovanstående gäller även för så kallade IoT-enheter.

Utomstående personer får inte använda Forststyrelsens datatekniska enheter, informationssystem, och inte heller datanät utan ett separat avtal om nyttjanderätt. Undantag är kundterminaler som godkänts av enheten för Informationstjänster.

Användning av e-post och Internet

Forststyrelsen har en e-postadress för organisationen kirjaamo@metsa.fi, dit meddelanden som gäller organisationen och myndighetsverksamhet styrs. Vid behov grundas även andra organisationsadresser, för vars del det måste definieras om de även fungerar från Internet.

Forststyrelsens personal har en arbetsrelaterad e-postadress i sin användning med formatet fornamn.efternamn@metsa.fi. Den arbetsrelaterade e-postadressen är endast avsedd för kommunikation som har att göra med arbetsuppgifter.

All Forststyrelsens inkommande och utgående officiell post måste registreras i ärendehanteringssystemet, där ärenden hanteras och distribueras. För att säkerställa dokumentens beständighet och integritet måste de dokument som tas emot via e-post och som hör till ärendehanteringssystemet matas in i systemet utan dröjsmål.

Användning av arbetsrelaterad e-postadress för privata ändamål är i princip förbjuden.

Det är förbjudet att vidarebefordra meddelanden som kommit till organisationens eller den arbetsrelaterade e-postadressen till en privat e-postadress.

I händelse av förutsebar frånvaro är arbetstagaren skyldig att ta hand om korrekt hantering av hans eller hennes e-post (frånvaroanmälan och vem som kommer att ta hand om saker under frånvaron).

Då ett anställningsförhållande upphör är personen skyldig att överföra dokument i sina e-postmappar som tillhör organisationen till ärendehanteringssystemet eller organisationens e-post och att radera alla eventuella personliga meddelanden. Dessutom är det bra att meddela kommunikationspartners om borttagandet av e-postadressen och att kommunicera vem på Forststyrelsen som i fortsättningen kommer att sköta motsvarande ärenden, i de fall då man har kännedom om detta.

Ett e-postmeddelande som ligger utanför Forststyrelsens befogenhet, och som skickats i misstag eller på grund av bristande kunskap, ska vidarebefordras till den myndighet som anses behörig enligt 8 § i förvaltningslagen, om det är känt och avsändaren underrättas om överföringen. Övriga e-postmeddelanden som uppenbarligen inte hör till Forststyrelsen och mottagaren, returneras till sändaren och förstörs. Den person som får tillgång till informationen i meddelandet har tystnadsplikt och förbud mot att utnyttja innehållet i och existensen av meddelandet.

Forststyrelsen har rätt att ta bort skräppost som är för stora eller av fel typ, eller meddelanden och filer som skadar eller hotar Forststyrelsens informationssäkerhet, så som skadeprogram.

Forststyrelsens arbetsgivare har rätt att läsa e-postmeddelanden som andra, eller han eller hon själv, skickat till en arbetstagare efter att han eller hon har mottagit ett skriftligt samtycke från arbetstagaren i fråga.

Huvudregeln är ändå att dokument som klassificeras som konfidentiella (icke-offentliga) inte får

skickas eller tas emot via e-post. Men om det ändå finns ett tvingande behov för detta måste det sekretessbelagda materialet, t.ex. material som innehåller personuppgifter skickas med Forststyrelsens befintliga krypteringstjänst för e-post eller så måste materialet exporteras till en bilaga som krypteras enligt en separat krypteringsinstruktion.

Endast dokument som innehåller offentlig information överförs som e-post eller som annan dataöverföring över datanätverket utan kryptering. Sekretessbelagd information kan överföras om tillräckligt stark kryptering används. De krypteringsmetoder som används bör vara godkända för användning av enheten för Informationstjänster.

Vid behov måste ett riktigheten och autenticitet hos ett dokument som tas emot via e-post verifieras, till exempel via telefon, eftersom bland annat avsändarens information kan förfalskas relativt enkelt.

Tillvägagångssätt som allmänt anses olämpliga, till exempel osakliga masspostningar, kedjebrev samt avsiktlig spridning av felaktig information, är förbjudna.

Distansanvändning och arbete utanför kontoret

Det är frågan om distansarbete då Forststyrelsens datanät eller en del av det används med hjälp av datatrafikförbindelse utanför organisationen. Med distansarbete avses arbete som utförs på annat ställe än på Forststyrelsens fasta kontor. När man använder en fjärranslutning måste man vid databehandling ta hänsyn till samma saker som då man arbetar i Forststyrelsens faciliteter. Men mer uppmärksamhet måste ägnas den fysiska verksamhetsmiljön.

Säkerhet i verksamhetslokalerna

Med verksamhetslokalernas säkerhet säkerställs att data, dokument och datamaskiner förvaras och hanteras ändamålsenligt i säkra utrymmen. Säkerhet i verksamhetslokalerna innefattar bland annat åtkomstövervakning, teknisk övervakning och bevakning, bekämpning av brand-, vatten-, el-, luftkonditionering, och inbrottsskador samt säkerheten hos de försändelser som innehåller datamängder.

Instruktioner gällande åtkomstkontroll och annan säkerhet i verksamhetslokalerna måste följas. Alla personers om rör sig i Forststyrelsens verksamhetsutrymmen måste ha ett identitetskort med bild eller ett besökarkort. Besökare får inte släppas in i Forststyrelsens utrymmen utan övervakning, detta gäller särskilt kontorsutrymmen och även t.ex. personal för underhåll eller reparationer.

Sekretess- och säkerhetsåtagande

1. Bakgrundsinformation och uppgifter för den som erhåller nyttjanderätt

Detta sekretess- och säkerhetsåtagande (nedan kallad ”Åtagande”) undertecknas av de parter utanför Forststyrelsen som enligt ett avtal som har gjorts tillsammans med Forststyrelsen (Avtal om nyttjanderätt till SASS- och SATJ-applikationerna i Forststyrelsens systemhelhet Uljas, FS 2659/2021, nedan kallad ”Avtal”) eller enligt motsvarande användningsändamål i enlighet med avtalet har tillgång till Forststyrelsens informationssystem och/eller konfidentiell information.

Mottagare av nyttjanderätt

Arbetsgivare/företag som företräds:	
Alla förnamn:	
Efternamn:	
Mobiltelefonnummer:	
E-postadress:	
Arbetsgivarens/det företrädda företagets ansvarsperson (motsvarar förman):	
Ansvarsperson på Forststyrelsen:	
Startdatum för användning av identifieringskoderna:	
Slutdatum för identifieringskodernas giltighet:	

2. Definitioner

Med konfidentiell information avses all Forststyrelsens eller dess dotterbolags, avtalspartners eller andra samarbetspartners affärs- och yrkeshemligheter, konfidentiell information i relation till dataskydd eller informationssäkerhet inklusive personuppgifter, information om s.k. utrotningshotade arter samt övrig sekretessbelagd eller konfidentiell information enligt lagen om offentlighet i myndigheters verksamhet (621/1999) som skriftligen, muntligen, elektroniskt eller i annat format överlåts till de som undertecknat Forststyrelsens Avtal eller som de får tillgång till.

Med avtal avses det Avtal som definieras ovan i punkt 1.

Med partner avses företag eller organisationer (här i synnerhet organisationer inom miljöförvaltning) i vars tjänst eller på vars begäran den person som skriver under Åtagandet arbetar.

3. Användning av konfidentiell information

Undertecknaren av Åtagandet har rätt att använda Konfidentiell information endast för att utföra arbetsuppgifter som förverkligar Avtalet eller Avtalets syfte och endast i den utsträckning som krävs för att fullgöra arbetsuppgifterna. Undertecknaren av Åtagandet har inte rätt att använda Konfidentiell information i andra än ovan nämnda syften. Undertecknaren av Åtagandet förbinder sig till att behandla och förvara Konfidentiell information särskilt omsorgsfullt och med beaktande av tillräcklig informationssäkerhet.

Undertecknaren av Åtagandet förbinder sig till att återlämna eller bevisligen förstöra all Forststyrelsens Konfidentiella information som de besitter omedelbart då Forststyrelsen så kräver, dock senast när behovet av användning i enlighet med deras arbetsuppgifter har upphört, med förbehåll för obligatorisk lagstiftning. Undertecknaren av Åtagandet har inte rätt att kopiera eller på annat sätt reproducera det mottagna materialet.

4. Tystnadsplikt

Undertecknaren av Åtagandet förbinder sig till att inte överlåta eller avslöja Konfidentiell information till tredje parter utan skriftligt tillstånd från Forststyrelsen på förhand. Detta inkluderar sådana Partners arbetstagare och företag som hör till samma koncern inklusive deras anställda, som inte behöver Konfidentiell information till ett ändamål enligt Åtagandet och som inte har gjort ett avtal om tystnadsplikt på minst motsvarande nivå.

Tystnadspliktens giltighet är permanent, dock för varje enskild Konfidentiell information till den tidpunkt då den Konfidentiella informationen har kommit till allmän kännedom på annat sätt än på grund av förseelse av undertecknaren av Åtagandet.

5. Anmälningsskyldighet

Undertecknaren av Åtagandet är skyldigt att utan dröjsmål informera Forststyrelsen om den Konfidentiella informationens konfidentiella karaktär är äventyrad eller hotad, eller om det finns skäl att misstänka att Åtagandet har brutits, stulits eller missbrukats av Partnerns anställda eller av något annat skäl som äventyrar informationssäkerheten eller dataskyddet.

6. Användning av informationssystem

Undertecknaren av Åtagandet har rätt att använda Forststyrelsens informationssystem endast i enlighet med Avtalet eller för genomförande av arbetsuppgifter som grundar sig på Avtalets syfte, samt endast i den omfattning som arbetsuppgifterna förutsätter och genom att iaktta de anvisningar och bestämmelser som är relaterade till användningen av Forststyrelsens informationssystem.

Undertecknaren av Åtagandet måste sörja för de personliga användarnamnen och lösenorden som Forststyrelsen har gett så att inte en tredje part får tillgång till dem.

7. Efterlevnad av lagstiftning, bestämmelser och anvisningar

Undertecknaren av Åtagandet förbinder sig till att iaktta den finska lagstiftningen gällande sekretess, dataskydd och informationssäkerhet som är giltig vid denna tidpunkt, Forststyrelsens informationssäkerhets- och dataskyddsprinciper (Bilaga 1) samt andra bestämmelser och anvisningar gällande informationsskydd och-säkerhet som Forststyrelsen tillhandahåller separat.

8. Påföljder

Om undertecknaren av Åtagandet bryter mot sina skyldigheter enligt detta Åtagande kan de nyttjanderätter som undertecknaren av Åtagandet beviljats till Forststyrelsens informationssystem begränsas, eller så kan de nämnda nyttjanderätterna återkallas helt. Dessutom är överträdelsen föremål för rättsmedel i enlighet med Avtalet och Forststyrelsen kan vidta andra nödvändiga åtgärder i samband med överträdelsen.

9. Underskrift

Jag förbinder mig att följa ovanstående villkor.

_____	_____
Namnförtydligande och underskrift	Företag eller organisation

Bilaga 1. Forststyrelsens principer för informationssäkerhet och dataskydd 12.2.2019