Tillsyn enligt EU:s Dataskyddsförordning 2016/679 – Personuppgiftsbehandling i I-valet 2019

Sammanfattning

Datainspektionen har granskat personuppgiftsbehandling som ska företas i samband med I-valet 2019.

Granskningen visar att det finns brister i säkerhetsåtgärderna hos den underleverantör som ÅDA AB anlitat för att biträda Landskapsregeringen under valet.

Granskningen visar även att ansvarsfördelningen mellan ÅDA AB och Landskapsregeringen inte är reglerad. Samt att även annan dokumentation saknas.

Datainspektionen varnar Landskapsregeringen för att genomförande av I-valet kan innebära brott mot grundläggande principer i Dataskyddsförordningen.

Datainspektionen riktar en reprimand mot Landskapsregeringen på grund av den bristande dokumentation som delgivits Datainspektionen.

Datainspektionen

den 19 september 2019

1 Bakgrund

Datainspektionen blev informerad i samband med Alandica Debatt att I-val skulle genomföras som alternativ till förtidsröstning. Datumet var den 11 juni. Då allmänna val är kärnan i den demokratiska processen och då införlivande av nya sätt att rösta medför nya risker uppfattades det som lämpligt av Datainspektionens myndighetschef att fatta beslut om granskning av personuppgiftsbehandlingen i samband med I-valet.

Redan innan beslut fattades delgav Landskapsregeringen information till Datainspektionen som omfattade bland annat beslut om att fortskrida med I-valet,[1] en säkerhetsanslys av Scytls dokumentation utförd av Deductive Labs,[2] och information om att systemet Scytl tillhandahåller var prövat bland annat via penetrationstester och code reviews.[3]

I säkerhetsanalysen från Deductive Labs konstateras att det inte kan säkerställas huruvida Scytl arbetar efter kraven ställda i ISO 27001 eller ej och att mycket av den information som Scytl delgivit om sitt säkerhetsarbete var verbala framställningar.

I den dokumentation som delgavs Datainspektionen fanns inte information om att behandlingen blivit granskad med utgång i Dataskyddsförordningen.

Den 19 juni 2019 fattade Datainspektionen ett beslut om att granska den planerade personuppgiftsbehandlingen som ska ske i samband med Lagtingsvalet 2019. Särskilt fokus för denna tillsyn var behandlingen som är planerad i samband med I-valet.[4]

Beslutet formulerades på så sätt att det inte specificerades vilken information Landskapsregeringen skulle delge Datainspektionen. Då skyldigheten att visa laglighet i behandling åligger personuppgiftsansvarig är det då i första hand denne som ska delge Datainspektionen den dokumentation som kan antas vara behövlig för Datainspektionen att utföra en granskning. Den dokumentation som kan tänkas vara av intresse är i huvudsak dokumentation som visar att den behandling som är under granskning utförs på ett säkert sätt och att den enskildes rättigheter tillgodoses i den omfattning som behandlingen tillåter.

2 Granskningen

Kontakt mellan Datainspektionen, Landskapsregeringen, ÅDA AB och Scytl har hållits löpande under granskningen via telefon, i personliga möten och via e-post.

2.1 Redogörelse för tidsförloppet vid granskningen

Den 16 juni 2019 fattade Datainspektionen beslut om granskning av personuppgiftsbehandling i lagtingsvalet, med särskilt fokus på I-valet.

Den 24 juni 2019 delgav Landskapsregeringen Datainspektionen underlagsrapporter och upphandlingsdokument som bilagor i två olika mail.

Vid en genomgång av dessa handlingar visade det sig att det saknades en tydlig ansvarsfördelning mellan Landskapsregeringen och ÅDA AB. ÅDA AB framstår som personuppgiftsansvarig till underleverantören Scytl i det enda personuppgiftsbiträdesavtal Datainspektionen fått ta del av i

[1] Se nr9-2019-plenum-rk1a.docx
[2] Utlåtande Deductive Labs juni 2019I.pdf
[3] Aktuellt om systemsäkerhet april 2019.docx
[4] Se Dnr T1-2019

denna granskning.[5] Detta påpekades för Landskapsregeringen den 25 juni 2019, och för ÅDA AB den 26 juni 2019.

Det påpekades även för ÅDA AB att Scytl, som enligt biträdesavtalet agerar biträde gentemot ÅDA AB, inte hade redogjort för tekniska och organisatoriska säkerhetsåtgärder som de ämnar utföra i egenskap av biträde. Därför begärdes även en redogörelse för teknisk specifikation av de säkerhetsåtgärder som underleverantören ämnar vidta vid behandlingen. Datainspektionen påpekade även för ÅDA AB att Landskapsregeringen låtit meddela att en konsekvensbedömning skulle göras, och att Datainspektionens uppfattning är att en sådan redan borde varit gjord.

ÅDA AB lät den 26 juni 2019 att de inte ansåg sig själva ha något ansvar för behandlingen i I-valet och att denna fråga i vart fall fick bero tills augusti 2019. De lät även meddela att de skulle begära ut den begärda tekniska specifikationen från underleverantören Scytl.[6]

Den 11 juli 2019 skickade Datainspektionen en påminnelse till ÅDA AB, och till Landskapsregeringen där Datainspektionen påminde om att teknisk specifikation av säkerhetsåtgärder måste delges Datainspektionen. Det informerades även om att avsaknad av sådan specifikation kan innebära att Datainspektionen måste besluta om ett förbud mot personuppgiftsbehandling i I-valet.[7]

Den 19 juli 2019 bjöd ÅDA AB in Datainspektionen att ta del av handlingar via Microsoft Teams. Då denna tjänst inte används av Datainspektionen och då Datainspektionen inte godkänt att materialet skulle delas på det sättet tidigare avböjdes inbjudan av Datainspektionen. Det begärdes istället att handlingarna skulle överlämnas i pappersformat om handlingarna inte kunde översändas på ett säkert sätt via e-post.

Den 6 augusti 2019 informerade ÅDA AB Datainspektionen om att Teams är ett säkert system att använda. Datainspektionen försökte i detta läge logga in i Teams för att ta del av informationen, men det fanns vid den tidpunkten inga handlingar i Teams att ta del av. ÅDA AB informerades om detta.

Den 15 augusti 2019 fick Datainspektionen tillgång till handlingarna via krypterad E-post. Datainspektionen har i samband med granskningen upphandlat tjänster av sakkunniga för att bistå med granskningen, bolaget TechLaw Sweden AB. Handlingarna skickades till TechLaw Sweden AB för granskning. Efter en granskning av handlingarna kunde konstateras att det var oklart om dokumenten avsåg behandlingen på Åland eller något annat.

Datainspektionen kontaktade den 19 augusti 2019 Scytl och påpekade att det fanns brister i dokumentationen. Scytls representant var vid denna tidpunkt på semester fram till den 28 augusti. ÅDA AB informeras om detta och att de som personuppgiftsansvariga precis som personuppgiftsbiträdet bär ansvaret för att behandlingen utförs på ett säkert sätt. ÅDA AB uppmanades därför ta kontakt med Scytl och säkerställa att relevant information delgavs Datainspektionen.

Den 27 augusti 2019 skickar Landskapsregeringen en behandlingsbeskrivning gällande I-valet hänförlig i första hand till Scytls inblandning.[8]

[5] Se LA0012019 – Scytl Secure Electronic Voting.pdf
[6] Se Sv_DI_s tillsynsbeslut.msg
[7] Se Teknisk specifikation Scytl.msgs
[8] ADA19A_Aland_Specification_06022019.docx

Den 29 augusti 2019 skickar Landskapsregeringen Scytls svar på de krav som ställts i upphandlingen av system för I-valet.[9]

I perioden mellan den 30 augusti och den 10 september hölls löpande kontakt mellan Datainspektionen och Scytl gällande teknisk specifikation av säkerhetsåtgärder som de vidtar i egenskap av biträde vid I-valet. Detta resulterade i en rapport med rekommendationer till Landskapsregeringen, sammanställd av den anlitade sakkunnige. Rapporten finns att läsa som bilaga.[10]

Den 12 september delgav Landskapsregeringen en beskrivning av behandlingen som de kommer att utföra i samband med I-valet, detta dokument är inte fullständigt utan saknar vissa formalia.[11]

Den 12 september 2019 delgav Landskapsregeringen en rapport över relationen mellan behandlarna i förevarande process.[12] Landskapsregeringen förklarade med en skiss:

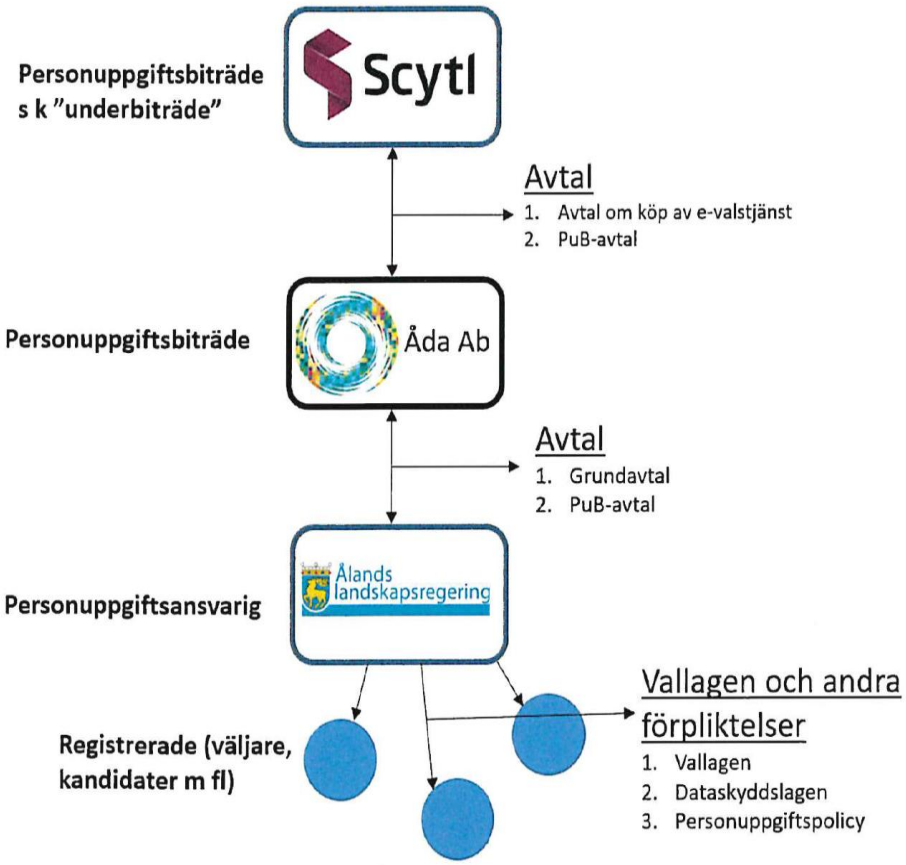


Fig 1

Av Fig 1 går att läsa att avtal mellan ÅDA AB och Landskapsregeringen finns. Datainspektionen hade vid denna tidpunkt ej tagit del av något avtal mellan ÅDA AB och Landskapsregeringen och någon förklaring hade inte givits varför trots upprepade påminnelser.

[9] Tender_Aland_Scytl_16.11.2018_.pdf
[10] Se Rapport-Åland-Scytl-190916.pdf
[11] Registerbeskrivning version 3 sept 2019.docx
[12] Se Yttrande gällande e-valet 12.9.2019.pdf

Den 17 september 2019 delgav Landskapsregeringen Datainspektionen ett personuppgiftsbiträdesavtal mellan Landskapsregeringen och ÅDA AB,[13] samt dokument om en pågående konsekvensbedömning[14].

2.2 Sammanfattning

Datainspektionen har vid upprepade tillfällen haft kontakt med samtliga behandlare i samband med granskningen. Datainspektionen har i ett tidigt skede i granskningen informerat om att personuppgiftsbiträdesavtal mellan Landskapsregeringen och övriga parter behöver finnas för att reglera ansvarsrelationen mellan parterna.

I de avtalshandlingar som finns mellan ÅDA AB och Scytl saknas specifikation över de säkerhetsgarantier som Scytl utlovar. Specifikation begärdes den 26 juni av ÅDA AB, den 10 september delgavs Datainspektionen specifikationen. En oberoende granskning de handlingar som underleverantören tillhandahållit Datainspektionen färdigställdes av TechLaw Sweden AB den 12 september 2019.[15]

Det saknas i dagsläget information om hur ansvarsförhållanden mellan främst ÅDA AB och Landskapsregeringen är reglerade, det saknas även en fullständig behandlingsbeskrivning och konsekvensanalys över behandlingen.

3 Redogörelse för sakomständigheter

I detta kapitel redogörs för vilka lagar Datainspektionen grundar sitt beslut på och de sakomständigheter som ligger till grund för beslutet.

3.1 Lagar

Datainspektionen har i huvudsak tre lagar att förhålla sig till i samband med utredningar:

1. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (Dataskyddsförordningen), och
2. Landskapslag om dataskydd inom landskaps- och kommunalförvaltningen ÅFS 2019:9 (Dataskyddslagen),

Då tillsynen i förevarande fall rör särskilt förtidsröstningen via internet aktualiseras även:

3. Vallag för Åland ÅFS 2019:45 (Vallagen).

3.2 Datainspektionens mandat

I Dataskyddslagen framgår det att Datainspektionen är tillsynsmyndigheten som lyder under dessa två lagar.[16] Tillsynsmyndigheten ska inrättas i lag vilket gjorts i samband med Dataskyddslagens ikraftträdande den 1 maj 2019.[17]

Dataskyddslagen hänvisar till Dataskyddsförordningen i frågor om Datainspektionens behörighet, befogenhet och uppgifter.[18]

[13] 4655_001.pdf
[14] Konsekvensbedömning – E-röstning.xlsx
[15] Se Rapport-Åland-Scytl-190916.pdf
[16] Dataskyddslagen kap. 3 § 14 st. 1
[17] Dataskyddförordningen art. 54 p. 1 a)
[18] Dataskyddslagen kap. 3 § 19

Tillsynsobjektet i förevarande fall är Ålands landskapsregerings allmänna förvaltning. Detta är en av landskapet Ålands myndigheter. Datainspektionen är behörig att utöva tillsyn över denna myndighet.[19]

Datainspektionens uppgift är bland annat att övervaka och verkställa tillämpningen av Dataskyddsförordningen.[20]

Datainspektionen har genom Dataskyddsförordningen utredningsbefogenheter och korrigerande befogenheter. Bland annat har Datainspektionen mandat att utföra så kallad dataskyddstillsyn, i samband med en sådan tillsyn har Datainspektionen rätt att ta del av all information, inbegripet personuppgifter, från både personuppgiftsansvariga som biträden som behövs för att genomföra denna tillsyn.[21] I Dataskyddslagen förtydligas att denna tillsyn även inbegriper rätten att ta del av sekretessbelagda uppgifter.[22]

Som stöd vid en dataskyddstillsyn har Datainspektionen möjlighet att på eget initiativ anlita sakkunniga.[23]

De korrigerande befogenheter som Datainspektionen har i samband med en dataskyddstillsyn av förevarande art är: varning, reprimander, krav på laglighet samt införande av begränsning.[24]

Om Datainspektionens befogenheter inte hörsammas kan Datainspektionen utfärda ett vite.[25]

3.3 Kartläggning över aktörer

Landskapsregeringen har det övergripande ansvaret för valets genomförande.[26] Detta torde innebära att Landskapsregeringen även är ansvarig för att säkerställa att kraven uppställda i Vallagens kapitel 10, som gäller förtidsröstning via internet, uppfylls. Det är därmed Datainspektionens uppfattning att Landskapsregeringen är personuppgiftsansvarig för personuppgiftsbehandling som sker i samband med E-valet.[27]

Parter som får genom upphandling får i uppdrag av Landskapsregeringen att utföra personuppgiftsbehandlingar i samband med I-valet är att se som personuppgiftsbiträden till Landskapsregeringen.[28]

Personuppgiftsbiträden kan om det finns särskilt eller allmänt tillstånd från personuppgiftsansvarig anlita övriga biträden för att bistå vid behandling.[29]

Av den dokumentation som delgivits Datainspektionen framkommer det att Landskapsregeringens avsikt var att en etablerad leverantör skulle biträda Landskapsregeringen med personuppgiftsbehandling i I-valet.[30] Denna leverantör får antas vara Scytl. Det saknas dock avtal mellan Scytl och Landskapsregeringen. ÅDA AB har istället i egenskap av personuppgiftsansvarig tecknat biträdesavtal med Scytl för den berörda behandlingen.[31] Åda AB har på fråga från

[19] Dataskyddslagen kap. 1 § 2 st. 1 st, Dataskyddsförordningen artikel 55
[20] Dataskyddsförordningen art. 57 p. 1 a)
[21] Dataskyddsförordningen Artikel 58, särskilt 1. a), b) och e)
[22] Dataskyddslagen kap. 3 § 21
[23] Dataskyddslagen kap. 3 § 22
[24] Dataskyddsförordningen art. 58 p. 2 a), b), d) och f)
[25] Dataskyddslagen kap. 4 § 25
[26] Vallagen kap. 2 § 7 st. 1
[27] Se Dataskyddsförordningen art. 4 p. 7 för definitionen av personuppgiftsansvarig.
[28] Se Dataskyddsförordningen art. 4 p. 8 för definitionen av personuppgiftsbiträde
[29] Dataskyddsförordningen art. 28 p. 2
[30] Se nr9-plenum-rk1a.docx
[31] Se LA0012019 – Scytl Secure Electronic Voting.pdf

Datainspektionen dementerat att de skulle vara personuppgiftsansvariga, men ej presenterat dokumentation som stödjer deras påstående.

Av det biträdesavtal mellan Landskapsregeringen och ÅDA AB framgår följande av p. 3 i avtalet: ”Avsikten med detta avtal är att reglera behandlingen av de personuppgifter som finns på de servrar och inom de system som Personuppgiftsbiträdet upprätthåller för Personuppgiftsansvarig enligt särskilda avtal”.[32]

Datainspektionens uppfattning av den dokumentation som Datainspektionen tagit del av samt av konversation med ÅDA AB att ÅDA AB inte upprätthåller det system som används för I-valet och att några personuppgifter hänförliga till detta system inte sparas på ÅDA AB:s servrar. Om ÅDA AB biträder Landskapsregeringen på det något sätt som detta biträdesavtal syftar till bör det finnas ett särskilt avtal som tydliggör relationen ytterligare, något sådant avtal har inte Datainspektionen tagit del av.

Det framgår även att ÅDA AB i egenskap av personuppgiftsbiträde till Landskapsregeringen har rätt att behandla personuppgifter för att ”utveckla och förvalta systemen”, vilka system som åsyftas är inte tydliggjort i avtalet. ÅDA AB ges även möjlighet att lagra, organisera, skydda och utföra säkerhetskopieringar av personuppgifter. Vilka personuppgifter som ÅDA AB får behandla är inte tydliggjort, men det framkommer att det är identifikatorer, bland annat personbeteckning. Om detta avtal avser förtydliga relationen mellan ÅDA AB som mellanhand mellan Landskapsregeringen och Scytl i behandlingen avseende I-valet kan det konstateras att ÅDA AB ges möjlighet att utföra behandling som riskerar att leda till att valsekretessen bryts.

Det finns heller ingen referens till att Scytl skulle vara anlitade av ÅDA AB att agera biträde i någon specifik behandling som kan omfattas av personuppgiftsbiträdesavtalet mellan ÅDA AB och Landskapsregeringen. Det går därför inte att knyta detta biträdesavtal till behandlingen som Scytl ska utföra i samband med I-valet.

Datainspektionens bedömning av biträdesavtalet mellan ÅDA AB och Landskapsregeringen är att detta syftar till att reglera en annan relation än den mellan Scytl och Landskapsregeringen. Om ÅDA AB biträder Landskapsregeringen på annat sätt än genom att vara mellanhand mellan Landskapsregeringen och Scytl kan personuppgiftsbiträdesavtalet fungera för att reglera den situationen, men Datainspektionen har inte tagit del av dokumentation som tyder på att detta är fallet, och biträdesavtalet är i sig för generellt skrivet för att utan ytterligare dokumentation som hänvisar till detsamma knytas till någon särskild behandling. Biträdesavtalet mellan Landskapsregeringen och ÅDA AB ligger därför inte som grund för beslut.

Datainspektionens uppfattning är att det inte går att utläsa någon förbindelse mellan Scytl och Landskapsregeringen av den dokumentation som kommit Datainspektionen till handa. Det är dock klarlagt i dialog mellan Landskapsregeringen och Datainspektionen att den etablerade leverantör som hänvisats till av Landskapsregeringen är Scytl.[33] Datainspektionen har därför i granskningen utgått från att det inte rör sig om två parallella I-val som ska utföras, utan enbart att viss dokumentation som styrker relationen mellan Scytl och Landskapsregeringen saknas.

Datainspektionens uppfattning vilken även bekräftats av Landskapsregeringen är att ÅDA AB biträder Landskapsregeringen med personuppgiftsbehandling i I-valet, ÅDA AB står i sin tur som personuppgiftsansvarig i relation till Scytl, vilka i sin tur biträder ÅDA AB med personuppgiftsbehandling.[34] I praktiken agerar ÅDA AB mellanhand och bär ansvaret gentemot

[32] Se 4655_001.pdf
[33] Se nr9-2019-plenum-rk1a.docx
[34] Se Fig 1 samt Yttrande gällande e-valet 12.9.2019.pdf

Landskapsregeringen för Scytls behandling.[35] Biträdesavtalet mellan Landskapsregeringen och ÅDA AB tydliggör ej relationen mellan Landskapsregeringen och Scytl.

4 Beslutsunderlag

Granskningen har berört huvudsakligen fyra delar. Biträdets specifikation över tekniska och organisatoriska säkerhetsåtgärder, ansvarsfördelningen mellan behandlarna, behandlingsbeskrivningen över I-valet och konsekvensbedömningen över behandling i I-valet.

Landskapsregeringens interna säkerhetsarbete är delvis lagstiftat i Vallagen:
Bland annat finns det alltid möjlighet för Centralnämnden för Lagtingsval att besluta om avbrott i I-valsprocessen.

Det finns en tydlig behörighetsbegränsning gällande vem som får öppna valurnan, och säkerhetsåtgärder gällande identifiering av dessa personer som leder till att Landskapets interna behandling i huvudsak upplevs säker.

Landskapsregeringen ska även kontinuerligt under pågående behandling säkerställa att systemen fungerar och säkerställa efter behandlingens fullbordande att systemets integritet bibehållits.

En oberoende instans ska även granska att rösterna registrerats som avsetts.

Datainspektionen har ingenting att invända mot dessa säkerhetsåtgärder, snarast anser Datainspektionen att det är uppenbart att lagstiftarens avsikt varit att säkerställa att personuppgiftsbehandlingen i valet ska ske på ett säkert sätt.

Landskapsregeringen har i huvudsak muntligen förklarat hur dessa säkerhetsåtgärder appliceras i praktiken.

4.1 Specifikation över tekniska och organisatoriska säkerhetsåtgärder

Den personuppgiftsansvarige ska enbart anlita personuppgiftsbiträden som ger ”tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas”[36].

[35] Dataskyddsförordningen art. 28 p. 4
[36] Dataskyddsförordningen Art. 28 p. 1

Av de handlingar som Datainspektionen inledningsvis tog del av framgick det av biträdesavtalet mellan ÅDA AB och Scytl följande:

The Processor shall:

(i) implement all technical, physical and organisational measures necessary to ensure the highest level of data security;

(ii) implement and maintain, at all times, all necessary technical, physical and organisational measures to protect the Personal Data against accidental, unauthorized or unlawful destruction, loss, alteration, disclosure, access and other unauthorized or unlawful processing;

Fig 2

Datainspektionens översättning av texten i Fig 2 är som följer:
Personuppgiftsbiträdet skall:

(i) Implementera alla tekniska, fysiska och organisatoriska åtgärder nödvändiga för att försäkra högsta nivå av dataskydd;
(ii) Implementera och underhålla, vid alla tillfällen, alla nödvändiga, fysiska och organisatoriska åtgärder för att skydda persondata mot oavsiktlig, olovlig eller olaglig förstöring, förlust, ändring, tillgång eller annan otillåten eller olaglig behandling.

Ovan skrivelse är delvis hämtad från Dataskyddsförordningens Artikel 32.[37] Någon specifikation vad dessa säkerhetsåtgärder omfattade rent praktiskt finns dock inte att återfinna i avtalet. Varför Datainspektionen begärde från ÅDA AB att specificera vilka åtgärder som vidtagits. ÅDA AB förde därefter frågan vidare till Scytl.

Datainspektionen har anlitat sakkunnig för att granska de säkerhetsåtgärder som presenterats av Landskapsregeringen, ÅDA AB och Scytl. Denna granskning resulterade i en rapport som finns att läsa bifogad detta beslut.

Granskningen gjordes i två etapper, då Scytl inte i första skedet delgav Datainspektionen den efterfrågade dokumentationen. Del av de brister som presenteras i granskningens första led har genom kompletterande dokumentation kunnat repareras.

Sammanfattningsvis framgår följande brister av rapporten:

1. Scytl har brister i sin dokumentation, den är delvis oorganiserad, otydlig och ospecifik,
2. Erforderliga garantier för att det system som ska användas vid I-valet på Åland inte har samma brister som Scytls övriga system har inte givits,

[37] Lagtexten: 2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från 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.

3. Det finns säkerhetsåtgärder, men det finns brister, huvudsakligen i säkerhetspolicy och behörighetsfrågor inom företaget.

Den samlade bedömningen i rapporten är följande:
”Sammantaget verkar det finnas ett systematiskt säkerhetsarbete hos Scytl. Det finns dock många frågetecken kvar för att kunna bedöma huruvida Scytls tekniska och organisatoriska säkerhetsåtgärder in sin helhet kan anses lämpliga enligt artikel 32 för den planerade behandlingen.”

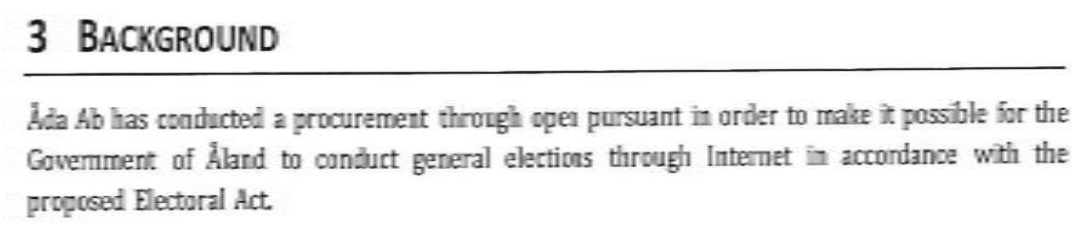
Datainspektionen delar uppfattningen i rapporten och rekommenderar precis som den sakkunnige att de frågetecken som finns kvar gällande tekniska och organisatoriska säkerhetsåtgärder undanröjs innan behandlingen påbörjas. Landskapsregeringen riskerar annars att utföra en behandling i strid mot principen om integritet och konfidentialitet.[38] Landskapsregeringen i egenskap av personuppgiftsansvarig har dock att själva avgöra vilken risk som anses vara godtagbar i den stundande behandlingen.

4.2 Ansvarsfördelningen mellan behandlarna

Datainspektionen har redogjort för sakomständigheterna och vilka aktörer som utför personuppgiftsbehandling i I-valet under avsnitt 3.3.

Eftersom Landskapsregeringen är personuppgiftsansvarig biträder övriga aktörer Landskapsregeringen med behandlingen. Till dags dato har dock inget material presenterats för Datainspektionen där Landskapsregeringens relation till Scytl reglerats. På grund av detta framgår det i dokumentationen som att ÅDA AB är personuppgiftsansvarig för en behandling där Landskapsregeringen inte är inblandad. ÅDA AB verkar till synes biträda Landskapsregeringen med viss behandling, men det framgår inte av biträdesavtalet mellan Landskapsregeringen och ÅDA AB med vilken.

Ett I-val av lagtingsledamöter administrerat av någon annan än en behörig valmyndighet är troligen inte ett legitimt val enligt den åländska Vallagen.[39] Det system som ska användas för I-valet ska enligt Vallagen tillhandahållas Landskapsregeringen.[40] Det finns i förevarande fall inga handlingar som tyder på att systemet tillhandahålles Landskapsregeringen. Det enda avtal om tillhandahållande av system är mellan ÅDA AB och Scytl. Det nämns i bakgrunden till avtalet att syftet är att tillhandahålla Landskapsregeringen med ett system för I-val.[41]



3 BACKGROUND

Åda Ab has conducted a procurement through open pursuant in order to make it possible for the Government of Åland to conduct general elections through Internet in accordance with the proposed Electoral Act.

Fig 3

Datainspektionens översättning av texten i Fig 3:
ÅDA AB har genomfört en offentlig upphandling för att möjliggöra för Ålands landskapsregeringen att genomföra allmänna val genom internet i enlighet med den föreslagna vallagen.

[38] Dataskyddsförordningen art. 5 p. 1 f)
[39] Se Vallagen Kap. 2 § 7 för en lista på valmyndigheter inom Landskapet Åland.
[40] Vallagen Kap. 10 § 78
[41] Se Fig 3

Det kan alltså utläsas av avtalet en viljeförklaring att tillhandahålla systemet till Landskapsregeringen, men något avtal som innebär ett införlivande av denna viljeförklaring har inte presenterats för Datainspektionen. Därmed får det antas att systemet inte i dagsläget är tillgängligt för Landskapsregeringen.

Om Landskapsregeringen inte har ett system för genomförande av I-valet kan inte I-valet genomföras på ett lagligt sätt. Om ÅDA AB avser att tillhandahålla sitt upphandlade system till Landskapsregeringen behöver erforderliga garantier för dataskydd ställas av ÅDA AB genom ett personuppgiftsbiträdesavtal för att säkerställa att personuppgiftsbehandlingen kan genomföras på ett säkert sätt. Detta kan till exempel göras genom att hänvisa till personuppgiftsbiträdesavtalet mellan ÅDA AB och Scytl samt den dokumentation som Scytl delgivit Datainspektionen som garantier för att behandlingen följer säkerhetskraven i Dataskyddsförordningens art 32. Observera att rapporten redogjord för i avsnitt 4.1 visar att det kan finnas vissa brister i Scytls dokumentation, men att det åligger Landskapsregeringen att avgöra om dessa brister är acceptabla eller ej.

Datainspektionens slutsats baserat på den information som delgivits Datainspektionen är att det inte i dag finns möjligheter att genomföra I-valet eftersom Landskapsregeringen inte har ett system tillgängligt. Genomförande av valet trots detta skulle stå i strid med principen om laglighet, korrekthet och öppenhet.[42] Denna brist löses på enklast vis genom upprättandet av ett personuppgiftsbiträdesavtal mellan antingen Landskapsregeringen och Scytl eller mellan Landskapsregeringen och ÅDA AB. I det senare alternativet behöver det specificeras vilken behandling som överlåts till annat personuppgiftsbiträde av ÅDA AB, ett godkännande från Landskapsregeringen att Scytl utför behandlingen istället för ÅDA AB behöver även författas. Oavsett lösning måste det framgå av personuppgiftsbiträdesavtalet vilken personuppgiftsbehandling som Landskapsregeringen överlåter till den andra parten.

Om dessa handlingar lämnas in till Datainspektionen ser inte Datainspektionen anledning att ifrågasätta valets legitimitet.

4.3 Behandlingsbeskrivningen

Datainspektionen har inte erhållit en fullständig behandlingsbeskrivning över I-valet. I det utkast till behandlingsbeskrivning saknas vissa formalia, men i övrigt anser Datainspektionen att behandlingen förklaras på ett tillräckligt sätt. Särskilt den processbeskrivning som författats av Scytl är tydlig och omfattande. Den muntliga beskrivningen som givits som förtydligande av säkerhetsåtgärderna i Vallagen finns inte heller anledning att kommentera på. Det ska alltså konstateras att det finns vidtagna och tillräckliga åtgärder för den behandling som Landskapsregeringen själva utför i samband med valet. Det har dock inte delgivits Datainspektionen någon skriftlig dokumentation över Landskapsregeringens självständiga behandling i I-valet.

Landskapsregeringen har presenterat ett dokument[43] där de redogör för relationen mellan parterna inblandade i I-valet. Där hänvisas till att ÅDA AB biträder Landskapsregeringen med I-valet och Scytl biträder ÅDA AB. Det är Datainspektionens uppfattning att ÅDA AB inte har för avsikt att utföra behandling i I-valet, utan snarast enbart agera mellanhand mellan Landskapsregeringen och Scytl. Det är också Datainspektionens förståelse att ÅDA AB sköter Landskapsregeringens webhosting, och att detta inte tagits i beaktan när Landskapsregeringen presenterat behandlingsbeskrivningen och dokumentet i fråga.

Datainspektionen rekommenderar att Landskapsregeringen färdigställer behandlingsbeskrivningen och tillhandahåller de röstberättigade i valet information om hur personuppgiftsbehandlingen kommer att gå till i I-valet, även Landskapsregeringens behandling, vilka personuppgiftbiträden Landskapsregeringen anlitar för behandlingen och vad dessa har för uppdrag samt vilka

[42] Se Dataskyddsförordningen Art 5 p. 1 a)
[43] Se Yttrande gällande e-valet 12.9.2019.pdf

personuppgifter som Landskapsregeringens biträden har tillgång till. I enlighet med principen om laglighet, korrekthet och öppenhet.[44]

4.4 Konsekvensbedömningen

Skyldigheten att utföra en konsekvensbedömning framgår av Dataskyddsförordnigen artikel 35. Skyldigheten föreligger när en behandling särskild med ny teknik, med beaktande av dess art och omfattning sannolikt leder till hög risk för fysiska personers rättigheter och friheter.

Under tredje punkten stadgas särskilt att en konsekvensbedömning ska krävas särskilt i fall gällande en omfattande behandling av särskilda kategorier av personuppgifter.[45]

I samband med I-valet kommer uppgifter om politiska åsikter att behandlas. Detta är en känslig kategori personuppgifter, och personkretsen som har rösträtt i valet omfattar samtliga röstberättigade individer som bor utanför Åland. Exakt hur många personer det rör sig om kan inte Datainspektionen uppskatta på ett tillförlitligt vis, men det får antas att det i relation till Ålands befolkning rör sig om en behandling i stor omfattning.

Den konsekvensbedömning som till dags dato presenterats för Datainspektionen tyder på en medvetenhet om risker hos Landskapsregeringen och en vilja att minimera desamma. Denna bedömning är i skrivande stund inte färdigställd och det finns därför en eventualitet att vissa risker som presenterats ej kan minimeras samt att vissa risker ännu ej är upptäckta. Då valet är nära förestående kan inte Datainspektionen avvakta tills konsekvensbedömningen är färdig för färdigställa detta beslut.

Det får konstateras att det i en perfekt värld gått att avstyra de risker som presenteras i konsekvensbedömningen i ett tidigare skede. Samt att beslutet om genomförande av val enligt Datainspektionen delvis borde ha grundats på en genomförd konsekvensbedömning.

Det framkommer av den ännu ofullständiga rapporten att penetrationstester genomförs och att resultatet av dessa kommer att vara färdigställt den 9 oktober 2019, vilket är samma dag som I-valet inleds. Det är Datainspektionens uppfattning att en sådan lösning innebär att centralnämnden för lagtingsval antingen måste acceptera eventuella brister som penetrationstestet visade och fortskrida med valet eller att besluta om avbrott av I-valet.[46] Alternativ för att läka eventuella brister som penetrationstestet visar finns inte med den tidsplanen som presenterats.

Datainspektionen rekommenderar att den konsekvensbedömning som inletts av Landskapsregeringen färdigställs så snart som möjligt och att eventuella risker som identifierats begränsas i den grad att valet kan genomföras på ett sätt som garanterar den enskildes rättigheter och friheter under Dataskyddsförordningen. Det finns annars en risk att Landskapsregeringen utför behandlingen i I-valet i strid mot principen om integritet och konfidentialitet.[47]

4.5 Bristen på dokumentation

Enligt principen om ansvarsskyldighet ska den personuppgiftsansvarige ansvara för och kunna visa att övriga principer i Dataskyddsförordningen följs.[48]

I förevarande fall saknas det dokumentation som tydligt visar att principerna i Dataskyddsförordningen efterföljs. Särskilt saknas dokumentation som knyter systemet för

[44] Se Dataskyddsförordningen Art 5 p. 1 a)
[45] Vad som är särskilda kategorier av personuppgifter framgår av Dataskyddsförordningen art. 9. Politisk åsikter är en särskild kategori personuppgifter.
[46] Vallagen § 83
[47] Dataskyddsförordningen art. 5 p. 1 f
[48] Dataskyddsförordningen art. 5 p. 2

behandling i I-valet till Landskapsregeringen. Det finns även otydligheter gällande säkerheten hos personuppgiftsbiträdet och en slutgiltig behandlingsbeskrivning har inte presenterats.

Över lag har det varit svårt att få tillgång till den dokumentation som efterfrågats, dels av Landskapsregeringen, men även av ÅDA AB och Scytl.

Scytl har på frågor om deras säkerhetsåtgärder på ett reflekterande vis svarat att frågorna är vagt ställda istället för att redogöra för säkerhetsåtgärder har de kortfattat radat upp vissa av dess utan vidare förklaring och avslutat med ”etc…” vilket försvårat Datainspektionens granskning och föranlett ett behov av följdfrågor.

Landskapsregeringen och ÅDA AB har vid flera tillfällen blivit informerade om att det saknas kritisk dokumentation. I de fall som svar givits har det konstaterats att det är under bearbetning eller att det får vänta till ett senare tillfälle. Vissa av de dokumenten som begärts, till exempel konsekvensbedömningen och behandlingsbeskrivning av I-valsprocessen har presenterats till Datainspektionen så sent som den 16 och 12 september 2019 respektive och då i ej färdigställd form. I samband med att processen inleds är det Datainspektionens förhoppning att denna dokumentation ska vara färdigställd, och att enskilda ska kunna delges tydlig information enligt Datainspektionens art. 13.

Det personuppgiftsbiträdesavtal som är författat mellan Landskapsregeringen och ÅDA AB är daterat den 16 augusti 2019 och delgavs Datainspektionen först den 17 september 2019. Om detta avtal är tänkt att reglera relationen mellan Landskapsregeringen och Scytl så hade detta eventuellt kunnat åstadkommas om Datainspektionen blivit informerad om avtalets existens i samband med dess upprättande. I dagsläget kan som påpekats i avsnitt 3.3 avtalet ej anses vara applicerbart på behandlingen i förevarande fall och sakinnehållet har därför ej beaktats i beslutet.

Datainspektionens uppfattning är att Landskapsregeringen direkt bryter mot principen om ansvarsskyldighet enligt Dataskyddsförordningen artikel 5 p. 2, då de inte kunnat visa att övriga principer uppfylles på ett tillräckligt sätt. Denna brist går att åtgärda om erforderlig dokumentation upprättas eller färdigställs innan behandlingen inleds.

5 Beslut

5.1 Val av korrigerande åtgärd

Inledningsvis bör konstateras att det finns omfattande säkerhetsåtgärder gällande personuppgiftsbehandling i I-valet stadgade i Vallagen och att Datainspektionens uppfattning är att Landskapsregeringens avsikt är att genomföra ett val där väljarnas rättigheter och friheter värnas. All personuppgiftsbehandling innebär risker, ibland mänsklig faktor och i andra fall yttre angrepp. Det är alltid den personuppgiftsansvariges ansvar att säkerställa att riskerna i behandlingen är acceptabla i förhållande till nyttan. Risken vid allmänna val måste mätas särskilt stor betydelse eftersom yttre åverkan i dessa kan innebära att en av demokratins bärande pelare faller.

Av den anledningen är det särskilt viktigt att den part som är ansvarig för personuppgiftsbehandlingen i valet, Landskapsregeringen i detta fall, kan visa att de aktivt arbetar för att förebygga risker och att den dokumentation som krävs för att uppfylla formkraven i lagstiftningen är i sin ordning.

Om Datainspektionen vid en granskning upptäcker att en behandling kan vara förknippad med risk är det Datainspektionens ansvar att varna den personuppgiftsansvarige att så är fallet. Detta är en av Datainspektionens korrigerande befogenheter.[49] Syftet med detta är att informera den personuppgiftsansvarige i första hand om dessa risker så att åtgärder kan vidtas för att förebygga desamma.

Datainspektionen kan även uttrycka kritik, eller som det står i förordningen rikta reprimand, i fall brister i den personuppgiftsansvariges efterlevnad av lagstiftningen uppmärksammats i en granskning.[50] Syftet med dessa är att tydliggöra ansvaret som den personuppgiftsansvarige har att följa lagstiftningen och att även kunna visa att lagstiftningen följs.

I förevarande fall har Datainspektionen genom granskningen blivit varse om vissa risker som personuppgiftsbehandlingen i I-valet kan medföra. Det är därför i sin ordning att Datainspektionen varnar Landskapsregeringen om detta.

Brister i dokumentation och ansvarsfördelning har även uppmärksammats under granskningen. Dessa brister innebär dels en risk för Landskapsregeringen och övriga parter, då det inte är klarlagt vem som är ansvarig för vad eller om valet kan genomföras på ett lagenligt sätt, men i en behandling av den här arten så måste brist i dokumentation även föranleda kritik från Datainspektionen.

5.2 Beslutssammanfattning

Datainspektionens uppfattning är även att om valet genomfördes under rådande omständigheter skulle det strida mot principen om laglighet, korrekthet och öppenhet.[51]

Slutligen är Datainspektionens uppfattning att Landskapsregeringen idag bryter mot principen om ansvarsskyldighet eftersom de inte presenterat erforderlig dokumentation som tyder på motsatsen.[52]

På urval av ovanstående risker beslutar Datainspektionen att utfärda en varning och en reprimand till Landskapsregeringen enligt de korrigerande befogenheter som Datainspektionen har enligt Dataskyddsförordningen artikel 58 2 a) och 2 b) respektive.

[49] Se Dataskyddsförordningen art. 58 2 a)
[50] Se Dataskyddsförordningen art. 58 2 b)
[51] Se avsnitt 4.2 och 4.3
[52] Se avsnitt 4.5

5.3 Varning

Datainspektionen varnar härmed Landskapsregeringen för att utföra personuppgiftsbehandlingen i I-valet. Det är tveksamt om valet idag ens kan genomföras på ett lagligt sätt eftersom ansvarsfördelningen mellan parterna inte verkar vara reglerad. Det har också i samband med granskningen av Datainspektionens sakkunnige framkommit att det finns brister i dokumentationen hos personuppgiftsbiträde vilket medför att valets integritet inte idag garanteras utan vidare åtgärder från Landskapsregeringen. Slutligen har Landskapsregeringen inte själva färdigställt riskbegränsande åtgärder, vilket typiskt sett inom Dataskyddsförordningens ram görs via konsekvensbedömning, vilket innebär att det kan finnas risker med behandlingen som inte kartlagts eller övervägts. Den pågående konsekvensbedömningen identifierar dessutom risker som inte ännu undanröjts.

Vilka av dessa risker som anses godtagbara är genom Vallagen upp till Centralnämnden för lagtingsval att avgöra.

5.4 Reprimand

Datainspektionen kritiserar bristen på dokumentation hos Landskapsregeringen. Datainspektionen har vid flertalet tillfällen begärt att få ut dokumentation men har trots detta inte blivit delgiven det berörda. Om detta är för att dokumentationen inte finns eller om Datainspektionen bara inte fått ta del av denna är i detta skede ointressant. Datainspektionen måste agera som att dokumentationen inte finns om denna inte presenteras för Datainspektionen.

Landskapsregeringen beslutade den 13 juni 2019 om att fortskrida med I-valsprocessen baserat på att ett system gjorts tillgängliga för dem, ett system som genomgått en utförlig bedömning av risker och riskhantering. Det kan starkt ifrågasättas om detta stämmer då Landskapsregeringen vid detta skede, så vitt Datainspektionen känner till, inte utfört en konsekvensbedömning eller någon annan egen åtgärd för att säkerställa att personuppgiftsbehandlingen skulle kunna skötas på ett säkert sätt.

Det underlag som fanns vid beslutstillfället var en rapport från Deductive Labs där ingen slutsats om säkerhetsåtgärder klart kunde fastställas och information om tester som utförts hos andra kunder hos Scytl. Scytl hade givit garantier utan specifikation om vad dessa omfattade ställda till ÅDA AB som inte hade eller har en avtalsrelation som omfattar behandlingen i I-valet,[53] och garantier med begränsad specifikation ställda i en upphandlingsprocess utförd av en ÅDA AB.[54]

Det är med andra ord inte klarlagt för Datainspektionen att systemet hade gjorts tillgängligt för Landskapsregeringen och det var, enligt Datainspektionen, heller inte klarlagt vid beslutsdatumet att systemet var säkert.

Systemet som Scytl tillhandahåller är visserligen beprövat, vilket talar för dess säkerhet, men Scytl hade vid beslutsdatumen den 13 juni 2019 inte visat att deras säkerhetsåtgärder uppnådde en adekvat nivå givet allvaret i behandlingen som de skulle biträda vid.

Datainspektionen har blivit informerad om att ÅDA AB är den upphandlande instansen för Landskapsregeringen, men inte sett någon dokumentation där denna relation regleras. Det måste därför återigen antas att någon sådan dokumentation inte finns.

Det saknas främst dokumentation som binder samman den behandling som Scytl avser utföra i samband med I-valet till Landskapsregeringens personuppgiftsansvar för densamma. Den

[53] LA0012019 – Scytl Secure Electronic Voting.pdf
[54] Tender_Aland_Scytl_16.11.2018_.pdf

dokumentation som tillhandahållits Datainspektionen om relationen mellan ÅDA AB och Landskapsregeringen är av allmän art och omfattar inte personuppgiftsbehandling i I-valet.

Slutsatsvis kan konstateras att Landskapsregeringen inte kan visa i sin dokumentation att de tillgodoser kraven i Dataskyddsförordningen. Behandlingen i fråga därmed kan uppfattas som osäker i bästa fall och olaglig i värsta fall. Det är även anmärkningsvärt att det trots upprepade påminnelser och anmodan från Datainspektionen inte vidtagits åtgärder för att läka bristerna i dokumentationen.

Centralnämnden för lagtingsval bör överväga att skjuta upp valet tills dokumentationen är i sin ordning om denna brist inte hinner läkas innan I-valets startdatum den 9 oktober 2019. Risken finns annars att genomförandet av val inte kan göras på ett lagenligt sätt.

Granskning utförd och beslut fattat av Datainspektionens myndighetschef.

Joakim Söderberg
den 19 september 2019

6 Bilagor

Dessa bilagor ligger till grund för beslutet i fråga och kan begäras ut av Datainspektionen genom en begäran om allmänna handlingar.

Rapport-Åland-Scytl-190916.pdf publiceras på Datainspektionens digitala anslagstavla i samband med beslutet.

1. DNR T1-2019
2. LA0012019 – Scytl Secure Electronic Voting.pdf
3. Sv_DI_s tillsynsbeslut.msg
4. Teknisk specifikation Scytl.msgs
5. Rapport-Åland-Scytl-190916.pdf
6. Yttrande gällande e-valet 12.9.2019.pdf
7. nr9-plenum-rk1a.docx
8. Registerbeskrivning version 3 sept 2019.docx
9. Konsekvensbedömning – E-röstning.xlsx
10. 4655_001.pdf
11. Utlåtande Deductive Labs juni 2019I.pdf
12. Aktuellt om systemsäkerhet april 2019.docx

7 Besvärsförfarande

Ändring i Datainspektionens beslut får sökas hos Ålands förvaltningsdomstol genom besvär på det sätt som föreskrivs i förvaltningsprocesslagen (FFS 586/1996). Besvärstiden är 30 dagar. Besvärstiden beräknas från dagen efter delgivning.

Av besvärsskriften ska framgå:
- ändringssökandens namn, hemkommun, postadress och telefonnummer,
- vilket beslut besväret gäller,
- till vilka delar av beslutet ändring söks och vilka ändringar som yrkas,
- de grunder på vilka ändring yrkas.

Om det är en laglig representant eller ett ombud som för ändringssökandens talan, eller om besvärsskriften har uppgjorts av någon annan, ska också dennes namn och hemkommun uppges i besvärsskriften.

Besvärsskriften ska undertecknas av ändringssökanden eller av dennes lagliga representant eller ombud.

Till besvärsskriften ska beslutet i original eller kopia bifogas. Dessutom ska de handlingar som ändringssökanden åberopar till stöd för sina yrkanden bifogas. Ombud ska bifoga en fullmakt till besvärsskriften om inte huvudmannen har befullmäktigat honom muntligen hos besvärsmyndigheten.

Besvärsskriften ska lämnas till:
Mottagare: Ålands förvaltningsdomstol
Postadress: Pb 31, AX-22101 Mariehamn
Besöksadress: Torggatan 16 A, Mariehamn
E-post: aland.fd@om.fi
Telefon: 029-5650265