Granskning av säkerhetsåtgärder hos Scytl

Inlämnad den 12 september 2019
Sammanställd av Sebastian Arnoldt

TechLaw Sweden AB

Saltmätargatan 3A
111 60 Stockholm
Sverige

Telefon: +46 8 559 25 200
E-post: info@techlaw.se

Innehållsförteckning

1 Bakgrund och uppdrag

Under Ålands lagtingsval och kommunalval hösten 2019 ska det vara möjligt för medborgare som är bosatta utanför Åland att rösta via internet. Systemet som ska användas för att genomföra det elektroniska valet är en montjänst som tillhandahålls av Scytl S.A. i Barcelona, Spanien.

Datainspektionen Åland har den 19 juni 2019 fattat beslut om att granska den planerade personuppgiftsbehandlingen som kommer att ske i samband med valet. Särskilt fokus kommer att ligga på tillämpningen av bestämmelserna i ÅFS 2019:45 10 kap.

Denna rapport ska, inom ramen av Datainspektionen Ålands tillsyn av valet, granska huruvida de tekniska och organisatoriska säkerhetsåtgärderna som har implementerats av Scytl uppfyller gällande krav på säkerhet enligt artikel 32 i den allmänna dataskyddsförordningen (”DSF”).

2 Metod

Granskningen måste utgå från både lagliga krav på säkerhetsåtgärder och samtidigt ta hänsyn till tillsynsmyndigheters vägledningar. Nedan följer en genomgång av lagkraven och en sammanfattning av relevanta vägledningar som har utfärdats av behöriga tillsynsmyndigheter runt om i Europa. Slutligen väljs en granskningsmetod för arbetets genomförande.

2.1 Dataskyddsförordningens säkerhetskrav

Enligt artikel 32 DSF ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. De vidtagna tekniska och organisatoriska säkerhetsåtgärderna ska beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. Som exempel på sådana åtgärder anges:

- pseudonymisering och kryptering av personuppgifter,

- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingsystemen och -tjänsterna,
- förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför. Särskilt hänsyn ska tas till risker relaterade till oavsiktlig eller olaglig förstöring, förlust eller ändring, obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Denna klassificering av risker motsvarar den metodik som används i vedertagna säkerhetsstandards, som exempelvis ISO 27001, där risker grupperas enligt risker för dataintegritet, konfidentialitet och tillgänglighet.

Vidare ska den personuppgiftsansvarige och personuppgiftsbiträdet enligt artikel 32 DSF vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets kontroll, och som får tillgång till personuppgifter, endast behandlar dessa enligt instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

2.2 Tillsynsmyndigheters vägledningar

Artikel 32 DSF är en regel som anger vilka krav tekniska och organisatoriska krav måste vara uppfyllda på en övergripande nivå. Varken artikel 32 DSF eller några andra bestämmelser i samma förordning preciserar vilka specifika tekniska och organisatoriska säkerhetsåtgärder en behandling måste uppfylla för att leva upp till regelverkets krav.

Flera europeiska tillsynsmyndigheter för dataskydd har tagit fram vägledningar som ska komplettera DSF med konkreta säkerhetskrav. Den svenska Datainspektionen har

publicerat en faktabroschyr med titeln *Säkerhet för personuppgifter.*[1] Broschyren innehåller en övergripande men inte särskilt detaljerad genomgång av säkerhetsåtgärder som ska beaktas vid behandling av personuppgifter. Broschyren reviderades senast november 2008 vilket begränsar dess användbarhet.

Den franska tillsynsmyndigheten för dataskydd, CNIL, har publicerat en omfattande och detaljerad vägledning för säker hantering av personuppgifter som bygger på en riskbaserad metodik och har titeln *Security for Personal Data*.[2] Vägledningen uppdaterades senast 2018 och kan på grund av sin riskbaserade metodik användas i majoriteten av alla sammanhang där en behandling av personuppgifter är aktuell.

Den storbritanniska tillsynsmyndigheten, ICO, har publicerat flera vägledningar avseende säkerhet för personuppgifter på sin webbsida. Bland dessa finns det generella vägledningar för säker hantering av personuppgifter och mer specifika vägledningar som till exempel *Guidance on the use of Cloud Computing* eller *Guidance on encryption*. ICO uppdaterar sina vägledningar löpande vilket säkerställer deras användbarhet.

Den så kallade Artikel 29-gruppen, numera den Europeiska dataskyddsstyrelsen, publicerade 2012 en generell vägledning för användning av molntjänster.[3] Vägledningen innehåller övergripande tekniska krav på molntjänstleverantörer och är därför tillämplig på Scytl.

Även andra europeiska tillsynsmyndigheter än de ovan anförda har utfärdat vägledningar för säkerhet av personuppgifter. Dessa vägledningar är dock mindre omfattande, aktuella eller systematiska jämfört med CNIL:s och ICO:s arbete. Därutöver hänvisar flera tillsynsmyndigheter till vedertagna säkerhetsstandarder men upplyser samtidigt om att ett säkerhetscertifikat inte per automatik innebär att DSF:s säkerhetskrav är uppfyllda.

---

[1] Datainspektionen, 2008, Säkerhet för personuppgifter, tillgänglig på: https://www.datainspektionen.se/globalassets/dokument/ovrigt/faktabroschyr-allmannarad-sakerhet.pdf.
[2] CNIL, 2018, Security of Personal Data, tillgänglig på: https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf.
[3] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 2012, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

2.3 Val av granskningsmetod och begränsningar

Denna granskning utgår från CNIL:s vägledning *Security for Personal Data*. CNIL:s metod kompletteras med element från ICO:s och Artikel 29-gruppens vägledningar, samt vedertagna säkerhetsstandards när detta är lämpligt. Granskningen tar sin utgångspunkt i de tekniska och organisatoriska säkerhetsåtgärder som ska beaktas vid behandling av personuppgifter. Även om granskningen uppmärksammar risker motsvarar den inte en konsekvensbedömning avseende dataskydd enligt artikel 35 DSF. Vidare utgår granskningen ifrån den information som har varit tillgänglig och som hänvisas till i texten.

2.4 Granskning i två omgångar

Denna granskning genomförs i två omgångar eftersom dokumentationen över Skytls tekniska och organisatoriska säkerhetsåtgärder inkommit vid två olika tillfällen. De dokument som används under den första granskningsomgången listas i bilaga 1. Dessa dokument har inkommit till Datainspektionen under perioden den 19 juni 2019 (datumet när tillsynsförfarandet inleddes) och den 6 september 2019. De dokument som används under andra granskningsomgången listas i bilaga 2. Dessa dokument har inkommit till Datainspektionen den 10 september 2019. Det saknas i dagsläget fullständig dokumentation av samtliga tekniska och organisatoriska säkerhetsåtgärder hos Skytl. Granskningsprocessens förlopp beskrivs i detalj i bilaga 3.

3 Beskrivning av behandlingen

Behandlingen omfattar de personuppgifter som är nödvändiga för att kunna genomföra det elektroniska valet på Åland. Den tekniska utrustningen för att genomföra valet tillhandahålls av en extern leverantör, Scytl, med säte i Spanien. Utrustningen består av serverkomponenter som är placerade i Spanien och klientkomponenter som används av väljarna, oavsett placeringar. Serverkomponenterna omfattar en avancerad mjukvarulösning som samlar in och räknar röstar. Behandlingen innebär att en del av rösterna i valet 2019 kommer att samlas in och räknas av en extern leverantör. Antalet röster som behandlas på detta sätt är dock begränsad eftersom det endast är utlandsregistrerade väljare som ska kunna använda sig av möjligheten att rösta elektroniskt, vilket motsvarar ungefär 2 000 väljare.

3.1 Röstprocess

Av den skriftliga konversationen med Scytl framgår hur en väljares personuppgifter behandlas under röstprocessen. Väljaren går till en webbplats som tillhandahålls av Ada AB och autentiserar sig via BankID. Vid framgångsrik autentisering skickar Scytl-servern krypteringsnycklar till väljarens enhet som används för att kryptera väljarens röst. Den krypterade rösten skickas till Scytl-servern som utfärdar en bekräftelse (”vote receipt”) åt väljaren. Under denna process samlar Scytl även in väljarens IP-adress. Väljaren kan vid ett senare tillfälle logga in i tjänsten för att granska att rösten lämnades. Väljaren kan dock inte granska hur han eller hon röstade. Väljaren får dock inte använda digitala enhet för detta som enheten väljaren röstade med. Efter att rösterna har tagits emot av Scytl-servern tas kopplingen bort mellan den person som har röstat och dess röst under en så kallad mixnings-process. Efter att processen är genomförd är det inte längre möjligt att koppla ihop en röst med den som har röstat.

3.2 Typer av personuppgifter

Under röstningen behandlas uppgifter om hur väljare har röstat, IP-adresser och uppgifter om användarnas digitala enheter. Enligt artikel 6.1 DSF klassas uppgifter om politiska åsikter och därmed röster som lämnas i ett politisk val som särskilda kategorier av personuppgifter. IP-adresser och uppgifter om användares enheter klassas normalt som vanliga personuppgifter. Om dessa uppgifter däremot kopplas till en väljares röst måste även dessa uppgifter klassas som särskilda kategorier personuppgifter. Särskilda kategorier personuppgifter kräver en högre nivå av säkerhetsåtgärder än vanliga personuppgifter.

4 Första granskningen av säkerhetsåtgärder

I detta avsnitt granskas de säkerhetsåtgärder som återfinns i Scytls dokumentation och i konversationer som har förts med Scytl under den första granskningsomgången (se bilaga 1). Säkerhetsåtgärderna är indelade i områden som bland annat används av CNIL och vedertagna säkerhetsstandarder. Det görs en bedömning i slutet av varje område. En sammanlagd bedömning av samtliga områden görs i sektion 4.13 där det även lämnas en preliminär bedömning och preliminära rekommendationer avseende säkerhetsåtgärderna.

4.1 Autentisering och behörigheter

4.1.1 Väljare

Väljare loggar in i systemet genom att gå till en webbplats och autentisera sig via BankID som uppfyller kraven på kvalificerad elektronisk signatur. En väljare kan endast lämna sin egen röst och inte rösta för någon annans räkning.

En svaghet i systemet är att det saknas möjlighet att säkerställa att den personen som använder den digitala enheten för att lämna sin röst verkligen är den röstberättigade personen. Det är tänkbart att en röstberättigad personen delar sitt BankID med någon annan person, vilket kan göra det möjligt för denna personen att rösta i den röstberättigade personens ställe.

Vid traditionella val utesluts denna risk vanligtvis genom att det genomförs en ansiktskontroll av den röstberättigade personen med hjälp av en giltig ID-handling innehållandes en bild. Vid brevröstning utesluts denna risk genom krav på vittnen. Även om en möjlig förfalskning av vittnesmål är möjlig kan detta, beroende på omständigheterna, anses vara en högre tröskel än att få tillgång till en annan persons BankID.

När det gäller väljarna uppfyller systemet därmed kraven på stark autentisering för åtkomst till särskilda kategorier av personuppgifter via internet, men autentiseringen är inte lika stark som vid traditionella val eller val via brevröstning.

4.1.2 Centralnämnden

Centralnämnden loggar in i systemet med ett personligt smartkort och egenvald pinkod. Det är inte möjligt att öppna valurnan utan att minst tre av personerna är närvarande samtidigt. Denna autentiseringsmetod bedöms som godtagbar.

4.1.3 Medarbetare

Scytls medarbetare har tillgång till systemets serverkomponent. I Scytls dokumentation av säkerhetsåtgärder beskrivs rutiner för autentisering av medarbetare och styrning av deras behörigheter på en övergripande nivå. Det beskrivs exempelvis att medarbetares rättigheter hanteras via Active Directory, att medarbetare endast ska få tillgång till de uppgifter som de behöver för sitt arbete och att antalet medarbetare som har tillgång till

ett valprojekt ska begränsas till absolut minimum. Det saknas dock detaljerade beskrivningar över hur autentiseringen är utformad, genom till exempel policyer för lösenord eller huruvida det krävs ett smart-card eller liknande för att få tillgång till arbetsdatorer. Därutöver saknas en detaljerad och övergripande beskrivning över hur behörighetsstyrningen är utformad (”access control policy”).

Bedömning: Systemet använder BankID för autentisering av väljare. BankID är för nuvarande en av de säkraste metoderna för att autentisera personer på internet. Metoden är dock inte lika säker som de autentiseringsmetoder som används vid traditionella val och brevröstning. Det är dock osannolikt, men inte uteslutet, att sårbarheter relaterade till autentisering med BankID kan leda till en avgörande påverkan på valet eftersom det skulle förutsätta att ett stort antal väljare har tappat kontroll över sitt BankID. Denna risk begränsas ytterligare genom att endast en bråkdel av Ålands medborgare kommer att rösta elektroniskt. I övrigt är metoderna som används för autentisering godtagbara.

Det saknas en access control policy. Detta behöver i sig inte vara ett hinder då Scytl uppfyller kraven på autentisering och behörighetsstyrning men borde åtgärdas innan behandlingen påbörjas.

4.2 Loggning, loggkontroller och hantering av incidenter

4.2.1 Loggning och loggkontroller

Övergripande riktlinjer för loggning beskrivs i dokumentet *Security in projects* (version 1.3). Varje projekt ska använda en centraliserad server för loggning som ska logga de mest kritiska incidenterna och samtidigt slå larm vid avvikande eller (misstänkt) skadligt beteende. IT-system ska konfigureras på så sätt att det skapar spårbarhet för specifika händelser, när detta anses vara praktiskt genomförbart. Händelserna som ska loggas på användarnas sida motsvarar ISO 27001:s krav på loggning. Därutöver inkluderar Scytls riktlinjer även krav på synkroniserade klockor i samtliga IT-system, skydd av logginformation samt loggning av administratörer och operatörer, vilket gör att Scytls riktlinjer för loggning motsvarar ISO 27001 krav på loggning i sin helhet. Däremot saknas en detaljerad beskrivning över hur dessa krav är implementerade hos Scytl.

Dokumentet *Scytl's Proactive Controls – Software Development Best Practices* ger detaljerade instruktioner om hur loggning ska implementeras i mjukvaran till Scytls utvecklare. Instruktionerna omfattar anvisningar som ska motverka förfalskning av loggarna.

Det saknas dock en övergripande policy för hantering av själva loggarna som till exempel styr hur loggarna ska arkiveras, skyddas mot åtkomst av obehöriga eller manipulering. Det saknas också regler för regelbundna loggkontroller.

Bedömning: Dokumentationen innehåller krav på loggning som motsvarar krav i vedertagna säkerhetsstandarder. Det beskrivs emellertid inte tillräckligt detaljerat hur dessa krav är implementerade. Det saknas även regler för hantering av loggar och loggkontroller.

4.2.2 Incidenthantering

Enligt dokumentet *Security in Projects* ska logguppgifterna innehålla information som gör det möjligt att följa upp säkerhetsincidenter. Därutöver finns det en policy för hantering av säkerhetsincidenter (*Computer Security Incident Handling*) som fördelar ansvaret för hantering av incidenter och innehåller en övergripande beskrivning över hur incidenter bör hanteras. När det gäller detaljerade instruktioner över hur incidenter bör hanteras hänvisar policyn till befintliga rutiner utan att ange vilka rutiner som finns eller vart de kan hittas. Medans policyn ställer krav på att dokumentera incidenter finns det inga särskilda krav på hur denna dokumentation ska se ut. Policyn nämner inte huruvida all dokumentation av incidenter samlas i ett centralt register. Däremot konstateras under artikel 4 att "The cost of managing any security incident must be proportional to the possible loss as a result of the incident." Policyn nämner dock inte att vissa typer av incidenter måste anmälas till personuppgiftsansvariga. Det saknas även en klassificering av typer av säkerhetsincidenter som kan inträffa med motsvarande allvarlighetsgrad.

Scyts hantering av personuppgiftsincidenter som faller under DSF beskrivs närmare i dokumentet *GDPR in Scytl Projects.* Inte heller här finns det en beskrivning av situationer i vilka Scytl ska rapportera personuppgiftsincidenter till personuppgiftsansvariga. Däremot

beskriver Scytl i vilka situationer Scytl ska anmäla personuppgiftsincidenter till den behöriga tillsynsmyndigheten i egenskap som personuppgiftsansvarig.

I sin roll som personuppgiftsbiträde till Ålands Regering har Scytl en skyldighet att omedelbart rapportera personuppgiftsincidenter avseende personuppgifter som ägs av Ålands Regering till densamma. Det framgår inte av dokumentationen huruvida Scytl är medveten om sin rapporteringsskyldighet till personuppgiftsansvarig enligt artikel 33 DSF. Ytterligare ett problem är att Scytls dataskyddsombud (”DSO”) samtidigt är säkerhetschef. I egenskap som DSO ska en och samma person anmäla brister för vilka han bär ansvar för i egenskap som säkerhetschef, vilket i praktiken innebär att han ska granska sig själv. Detta kan leda till intressekonflikter som i sin tur kan äventyra en effektiv hantering av personuppgiftsincidenter. Att utse IT-chefen som DSO strider därutöver mot de riktlinjer som återfinns i artikel 29-gruppens vägledning för dataskyddsombud.[4]

Bedömning: Policyn för hantering av säkerhetsincidenter är bristfällig. Vidare finns inga regler för att anmäla personuppgiftsincidenter till personuppgiftsansvarig. Personen som innehar rollen som dataskyddsombud är olämplig på grund av intressekonflikter.

4.3 Säkerhet av datorer

Dokumentet *Physical security and equipment* beskriver hur den fysiska säkerheten av datorer upprätthållas genom till exempel tillträdeskontroller till lokaler där datorer finns. Dokumentet *Change Management* innehåller en kort beskrivning av hur datorers operativsystem ska uppdateras och en allmän begränsning av vilken mjukvara som får installeras på datorerna och av vem. Det saknas däremot en policy eller annan sammanhängande beskrivning av vilka säkerhetsåtgärder som har vidtagits avseende datorer som användas av Scytl medarbetare. En sådan policy bör till exempel innehålla regler om bland annat automatisk utloggning ur datorer, hur data ska lagras och säkerhetskopieras, regelbunden uppdatering av antivirusmjukvara och annan mjukvara, installering av säkerhetsuppdateringar samt begränsning av datorernas konnektivitet.

[4] Article 29 working party, 2016, Guidelines on Data Protection Officers (‘DPOs’) – WP 243 rev.01, tillgänglig på: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

Av kommunikation med Scytl framgår att medarbetare får ansluta externa lagringsmedier till sina datorer och att datorernas hårddiskar är krypterade. Medarbetare kan få tillgång till system via fjärråtkomst (Scytl VPN med två faktorer) vilket innebär att medarbetare har tillåtelse ta med sig datorer från Scytls lokaler. Medarbetare får dock inte använda egna datorer (*Bring Your Own Device*). Av kommunikationen framgår vidare att medarbetare inte få använda sig av molntjänster.

Bedömning: Det saknas en policy för säkerhet av datorer.

4.4 Säkerhet av mobila enheter och distansarbete

Av kommunikationen med Scytl framgår att medarbetare får använda mobila enheter för sitt arbete och att de får koppla upp sig till Scytls system via fjärråtkomst. Det framgår vidare att hårddiskar tillhörandes mobila datorer är krypterade. Det saknas i övrigt information om vilka regler som gäller för medarbetares användning av mobila enheter. Det saknas även särskilda regler som beskriver hur förlust av mobila enheter ska hanteras. Det saknas vidare regler för distansarbete.

Bedömning: Dokumentation av regler för användning av mobila enheter och distansarbete är undermålig.

4.5 Säkerhet av webbsidor, servrar och interna nätverk

Säkerhet webbsidor, servrar och interna nätverk beskrivs i dokumenten *Security in Projects och SAML Projects, GDPR compliance* genom att lista omfattande säkerhetskrav som bland annat begränsning av internettrafik, managering av trådlösa nätverk, krav på VPN för fjärråtkomst, begränsningar i nätverkstrafik, krav på TLS, intrusion detection systems och partitionering av nätverk. Säkerhetskraven som anges motsvarar i sig vedertagna säkerhetsstandarder men är i huvudsak allmänt formulerad.

Dokumenten gäller endast kundprojekt och det är därför oklart huruvida samma säkerhetskrav gäller även i andra sammanhang. Det kan också ifrågasättas huruvida dokumentet kan anses som en bindande policy eftersom de endast anger säkerhetsåtgärder som exempel. Det är därför inte säkert att samtliga säkerhetsåtgärder som listas kommer att användas i ett kundprojekt. Det anges exempelvis att en server kan

förseglas för att skydda den mot obehörig åtkomst på kundförfrågan. Frågan är då varför en sådan försegling inte erbjuds som standard med tanke på känsligheten av behandlingen och huruvida oförseglade servrar är skyddade mot obehöriga på ett sämre sätt.

Bedömning: Säkerhetskraven som beskrivs i dokumentationen motsvarar vedertagna säkerhetsstandarder. Kravens implementering är inte tillräckligt specifikt. Dokumentationen gäller endast kundprojekt och inte Scytls informationshantering i övrigt. Det framgår inte huruvida dokumentationen utgör bindande krav eller bara exempel över säkerhetsåtgärder som kan komma att användas.

4.6 Säkerhetskopior

Säkerhetskopior nämns endast sporadiskt i dokumenten. I dokumentet *Security in Projects* skrivs till exempel: ”Regularly backup data so that it can easily recover lost or corrupted data from an attack or system failure. To keep everything secure, encrypt backed up data that contains sensitive information, and protect it with a password if possible.” Av detta allmänna krav framgår inte hur ofta data ska säkerhetskopieras, vart säkerhetskopiorna ska lagras, hur ofta och på vilket sätt det ska genomföras försök att återskapa säkerhetskopior osv.

Bedömning: Dokumentation av åtgärder avseende säkerhetskopior är undermålig.

4.7 Radering av data

Radering av data nämns kort i olika dokument som till exempel i *GDPR in Scytl Projects*. Här konstateras följande under punkt 3.3: ”Once the project is finished, following the ‘data minimization’ idea from the law, the information must be destroyed. All the files related with the project must be deleted from the DDBB and from all the repositories.” Det saknas dock en detaljerad beskrivning av hur data ska raderas och hur effektiviteten av raderingsprocessen ska säkerställas. Tidpunkten för raderingen, ”once the project is finished”, lämnar utrymme för tolkning.

Bedömning: Dokumentation av åtgärder avseende radering av data är undermålig.

4.8 Säkert kommunikation med externa parter

Säkerhet av kommunikation med externa parter nämns på olika ställen i dokumentationen. Dokumentet *Security in services provided by third parties* innehåller en detaljerad reglering som styr hur och under vilka omständigheter externa parter kan få tillgång till Scytls interna system. Däribland finns det specifikt formulerade krav på vilka VPN-lösningar och vilken utrustning som får användas.

I dokumentet *GDPR in Scytl Projects* sägs att data som avser kundprojekt ska skickas krypterat och att man inte kommer att använda molntjänster för att överföra data. Dokumentet innehåller en rutin som beskriver hur data ska skickas krypterad via e-post. Det framgår däremot inte vilken typ av data som ska skickas på detta sätt och vems ansvar det är att kryptera data. Dokumentet *Personal Data Management* innehåller en liknande beskrivning.

Det finns däremot ingen övergripande policy som reglerar på vilket sätt Scytl medarbetare ska utbyta data med omvärlden. Det finns inga regler för andra kommunikationskanaler än e-post och molntjänster. Det kan därutöver ifrågasättas huruvida dokumenten *GDPR in Scytl Projects* och *Personal Data Management* kan anses vara bindande policyer för medarbetare.

Bedömning: Avseende reglering av externa parters tillgång till Scytl:s interna system är dokumentationen godtagbar. Avseende medarbetares utbyte av data med omvärlden i övrigt är dokumentationen bristfällig. Det är oklart huruvida den befintliga dokumentationen kan likställas med bindande policyer för medarbetare.

4.9 Fysisk säkerhet

Scytls åtgärder avseende fysisk säkerhet beskrivs i dokument *Physical security and equipment*. Dokumentet är omfattande och motsvarar nästan alla krav som finns i ISO 27001-standarden för informationssäkerhet. Det saknas dock regler för rent skrivbord

med hänsyn till papper och flyttbara lagringsmedia samt tom skärm på informationsbehandlingsresurser. I övrigt är dokumentet skrivit på ett övergripande sätt som inte preciserar kraven för fysisk säkerhet i detalj.

Bedömning: Scytls åtgärder avseende fysisk säkerhet är godtagbara. Det saknas dock regler för rent skrivbord och tom skärm på informationsbehandlingsresurser.

4.10 Övervaka mjukvaruutveckling

Dokumentet *Scytl:s Proactive Controls – Software Development Best Practises* beskriver best practices och som företagets mjukvaruutvecklare ska ta hänsyn till vid utveckling av mjukvara. Därutöver beskriver dokumentet vanliga misstag som utvecklare ska undvika. Dokumentet innehåller detaljerade riktlinjer för säkerhet och dataskydd som är inriktade på för Scytls verksamhet.

Bedömning: Riktlinjerna för mjukvaruutveckling är godtagbara och visar att Scytl prioriterar säkerhet och dataskydd i utveckling av sina tjänster.

4.11 Kryptering

Detta avsnitt gäller endast kryptering som inte är kopplad till röstsystemet. Kryptering av röstsystemet behandlas i sektion 4.13 nedan.

Av konversationer med Scytl framgår att arbetsdatorer ska krypteras och att kommunikation via webbplatser krypteras med TLS. Flera dokument nämner kryptering men det saknas övergripande dokumentation för kryptering av informationstillgångar. Det bör bland annat finnas regler för kryptering av olika typer av informationstillgångar at rest och in transit, kryptering av löstagbara lagringsmedier, kryptering av kommunikation och hantering av krypteringsnycklar. I en viss utsträckning finns delar av sådana beskrivningar i dokumentet *SAML Projects, GDPR Compliance* som är emellertid begränsad till röster och röstsystemet. Det är dock tveksamt huruvida detta dokument ska tolkas som bindande regler för medarbetare.

Bedömning: Scytls dokumentation av krypteringsåtgärder handlar nästan uteslutande om kryptering av röster och röstsystemet. Det saknas en övergripande dokumentation av krypteringsåtgärder och hur krypteringsnycklar hanteras.

4.12 Säkerhet av rösterna

Scytl använder en avancerad krypteringsalgoritm för att säkerställa rösternas konfidentialitet och integritet. Rösterna krypteras på väljarens enhet och kan endast dekrypteras av valstyrelsen efter att kopplingen mellan rösterna och väljarna har tagits bort av en server som blandar röstarna. Det krävs flera medlemmar av valstyrelsen för att dekryptera rösterna. Med denna metod säkerställer Scytl att rösterna krypteras end-to-end, att väljarna förblir anonyma, att inga röster går förlorade, att innehållet av rösterna inte kan ändras och att valresultat inte kan felrapporternas. Krypteringsmetoderna som används motsvarar den senaste tekniska utvecklingen och vedertagna krypteringsstandarder från till exempel NIST, se bland annat *Security in Projects* och *Secure Software Development Life Cycle*. Krypteringsalgoritmen har beskrivits i detalj vid konversationen med Scytl.

I början av 2019 publicerades dataskyddsforskarna Lewis, Pereira och Teague forskningsresultat om sårbarheter i Scytls krypteringsalgoritm.[5,6] Forskarna hade analyserat källkoden av ett Scytl-system som publicerades av SwissPost och upptäckt sårbarheter i mjukvaran som blandar rösterna och också kallas för ”mixer”.[7] Mjukvaran kunde manipulareas på så sätt att innehållet i röster förändrades utan att algoritmen skulle märka något. Därutöver konstaterade de att det skulle vara möjligt för en systemadministratör eller tjänsteleverantör att utnyttja sårbarheterna för att manipulera rösterna. Forskartrions resultat verifierades av andra forskare.

Forskarnas fynd förtydligar att Scytls system är en black-box. Om SwissPost inte hade publicerat Scytls källkod hade dessa sårbarheter med stor sannolikhet inte upptäckts. För

[5]Lewis, Pereira, Teague, 2019, Ceci n'est pas une prevue, tillgänglig på: https://openprivacy.ca/research/UniversalVerifiabilitySwissPost/.
[6]Lewis, Pereira, Teague, 2019, How not to prove your election outcome, tillgänglig på: https://openprivacy.ca/research/HowNotToProveYourElectionOutcome/.
[7] SwissPost, Disclosure of Source Coce, tillgänglig på: https://www.post.ch/en/business-solutions/e-voting/publications-and-source-code/e-voting-source-code?shortcut=evoting-sourcecode.

att utnyttja sårbarheterna krävs bland annat att angriparen har detaljerad kunskap om systemet, kryptografi och tillgång till systemet, vilket begränsar antalet individer som skulle kunna utnyttja sårbarheterna för ett angrepp. Samtidigt är det viktigt att poängtera ett sådant angrepp inte skulle vara omöjlig.

I konversation med Scytl har företagets företrädare endast levererat fåordiga svar avseende denna problematik. Scytl hävdar att sårbarheterna har åtgärdats, att Ålands Regering inte kommer att använda samma system som SwissPost (SwissPost använde sVote, Ålands Regering kommer att använda Invote) och att Invote inte drabbats av samma sårbarheter som sVote. Enligt företaget delar sVote och Invote ”endast några bibliotek” och är implementerade på ”helt olika sätt”.

Mot bakgrund av att sårbarheterna som upptäcktes satt i kärnan av Scytls system, nämligen blandningsservern eller ”mixern”, är det anmärkningsvärt att Scytl hävdar att sårbarheten var begränsad till SwissPosts sVote. Att forskare har upptäckt sårbarheter i Scytls mjukvara visar att det överhuvudtaget kan förekomma sårbarheter som kan påverka utgången av ett val. Utan att genomföra en granskning av Invotes källkod är det inte möjligt att veta huruvida det föreligger sårbarheter som kan utnyttjas för att påverka valet.

Därutöver anger Scytl i dokumentet *SAML Projects, GDRP compliance* att väljarnas IP-adresser samlas in och lagras för säkerhetsändamål. De hävdar också att IP-adresser inte kan användas för att identifiera väljare. I konversationen medger Scytl dock att det är möjligt att identifiera väljare med hjälp av IP-adressen. Varje röst som lämnas får en unik VoterID med en tidsstämpel. Varje IP-adress som loggas får också en tidsstämpel. Genom att korrelera tidsstämpel som skapas in för VoterID och IP-adress blir det möjligt att identifiera vem som har lämnat vilken röst. Eftersom Scytl kan dekryptera rösterna är det därför inte uteslutet att Scytl skulle kunna koppla dekrypterade röster till IP-adresser tillhörande enskilda väljare och därmed få vetskap om vem som har röstat vad i valet.

För att identifiera väljare på detta sätt krävs enligt Scytl att loggarna av samtliga system korreleras. Detta förutsätter tillgång till loggarna vilket är begränsat till säkerhetsavdelningen och IT-avdelningen. Även om detta sätt att identifiera väljare skulle kräva mycket arbete är det alltså inte uteslutet att det skulle kunna ske. Det är

anmärkningsvärt att Scytl inte har identifierat denna risk och åtgärdat problemet genom bättre loggdesign eller val av alternativa säkerhetsåtgärder.

Bedömning: Scytl har byggt en genomtänkt krypteringslösning för att skydda rösternas integritet och konfidentialitet som baseras på vedertagna krypteringsstandarder av den senaste tekniken. Lösningen är väl dokumenterad. Forskare har emellertid visat sårbarheter i en av Scytls produkter (sVote) som kan utnyttjas för att påverka valresultatet. Det kan inte uteslutas att även Invote drabbas av sårbarheter. För att säkerställa att Invote inte drabbas av detta krävs en oberoende granskning av Invotes källkod.

Under revisionen har det vidare upptäckts ett möjligt sätt att identifiera väljare indirekt via deras IP-adresser. Det är inte uteslutet att kopplingen kan användas för att se hur enskilda väljare har röstat.

4.13 Preliminär bedömning och rekommendationer

Bedömning och rekommendationer i denna sektion görs utifrån den dokumentation som har lämnats in och granskats under revisionsprocessen första omgång.

4.13.1 Brister i dokumentation av säkerhetsåtgärder

Ett av syftena med ett ledningssystem för informationssäkerhet (LIS) som följer ISO 27001 eller någon annan vedertagen standard är att skapa en uppsättning av regler som tillåter medarbetarna att bedriva ett systematiskt säkerhetsarbete. Ett annat syfte är att dokumentera implementeringen av säkerhetsåtgärderna så att dessa kan granskas av interna och externa parter. Ett mått för effektiviteten av ett LIS är om varje enskild medlem i organisationen kan använda den för att förstå vad som krävs av honom eller henne och sedan handla i enlighet med detta.

Scytls har presenterat en omfattande dokumentation av säkerhetsåtgärder och eftersträvar att uppfylla kraven enligt ISO 27001. Scytl är dock inte certifierade enligt ISO 27001. Dokumentationen som hittills har presenterats innehåller brister:

- Dokumentationen är oorganiserad och saknar en underliggande struktur genom att dokument inte innehåller korrekta hänvisningar och att liknade ämnen beskrivs i flera dokument.
- Dokumentationen är otydlig och ospecifik. En enskild medarbetare i Scytls organisationen kan omöjligt förstå vad förväntas av honom eller henne avseende säkerhet av personuppgifter genom att läsa dokumentationen.
- Det är oklart huruvida vissa av dokumenten utgör bindande regler för medarbetare eller inte.
- Säkerhetsåtgärder listas som krav men åtgärdernas implementering av beskrivs obetydligt eller inte alls.

Huruvida bristerna i dokumentationen ska tolkas som att det finns brister i Scytl:s implementering av säkerhetsåtgärder är svårbedömd. När det gäller till exempel nätverkssäkerhet visar dokumentation som har skapats i samband med riskanalyser att Scytl har en hög riskmedvetenhet och har implementerad omfattande åtgärder avseende nätverkssäkerheten. Det har däremot inte kommit fram någon sådan dokumentation avseende andra områden som behörighetsstyrning, radering, loggning, användning av mobila enheter eller säkerhetskopior.

Sammanfattning: Det saknas information för att kunna bedöma huruvida Scytl har implementerat effektiva säkerhetsåtgärder för behandling av personuppgifter i samband med Ålands val. Dokumentationen av säkerhetsåtgärderna som har lämnats in hittills är undermåliga med tanke på att Scytl ska hantera personuppgifter i samband med ett demokratisk val.
Rekommendation: Avvakta med behandlingen innan Scytl har åtgärdat bristerna i sin dokumentation. Därutöver bör en Ålands Regering överväga genomföra en revision på plats hos Scytl för att övertyga sig om säkerhetsåtgärdernas implementering.

4.13.2 Brister i hantering av röster

Forskare har visat sårbarheter i en av Scytls produkt som kan utnyttjas för att påverka ett val. Det är inte uteslutet att andra produkter från Scytl som till exempel Invote har sårbarheter. Under revisionen har ett möjligt sätt att identifiera väljare indirekt via sina IP-

adresser upptäckts. Det är inte uteslutet att kopplingen kan användas för att se hur enskilda väljare har röstat.

Bedömning: För att säkerställa att Invote inte drabbas av sårbarheter krävs en oberoende granskning av Invotes källkod. Möjligheten för Scytl att koppla väljare till röster behöver också utredas vidare. Man behöver göras en riskanalys som bedömer hur sannolikt det är att Scytl kan koppla innehållet i en röst till en enskild individ.

5 Andra granskning av säkerhetsåtgärder

I detta avsnitt granskas de säkerhetsåtgärder som återfinns i Scytls dokumentation och i konversationer som har förts med Scytl under den andra granskningsomgången (se bilaga 2). Sektionernas indelning följer rubrikerna tillhörande de dokument som lämnats in av Scytl. Om ett dokument tillför ny information som kräver en revidering av det som skrivs i första granskningsomgången (sektion 4) anges detta i texten. I sektion 5.2 lämnas en slutbedömning och rekommendationer.

5.1 Granskning av inlämnade dokument

Sammantaget gör innehållet i dokumenten ett mer strukturerat, detaljerat och sammanhängande intryck än dokumentationen som har granskats tidigare. Skrivstilen i flera av dokumenten skiljer sig dock från den dokumentation som har granskats tidigare. Detta kan bero på att flera av dokumenten (alla som har version 1) har tagits fram så sent som april 2019. Detta leder till frågan hur långt Scytl har kommit med implementeringen av de krav som ställs i dokumenten.

5.1.1 Scytl Information Security Policy

Dokumentet innehåller omfattande och detaljerade krav på vad medarbetare ska beakta när det gäller säkerhet. Policyn öppnar upp för att andra än IT-avdelningen kan inneha administratörsrättigheter vilket motsäger Scytls svar i kommunikationen (”The users have no rights on the machines”). Policyn innehåller godtagbara regler för utbyte av data via e-post, molntjänster och Sharepoint vilket innebär att ovanstående uttalande om säker kommunikation med externa parter måste revideras avseende e-post, molntjänster och Sharepoint.

I konversationen med Scytl besvarades frågan om medarbetare får använda sina egna enheter (BYOD) med ett nej. Policyn innehåller däremot en detaljerad reglering av BYOD och lägger ansvaret för säkerheten på den enskilda medarbetaren, vilket är oacceptabelt. Det finns även detaljerade regler för hur medarbetare får jobba hemifrån och använda sina egna datorer för detta. Det finns inget förbud att lagra data på sina privata enheter. Det är förståeligt att Scytl vill tillhandahålla denna möjlighet till sina medarbetare men i sammanhanget att företaget ansvarar för att organisera demokratiska val är detta inte godtagbart med tanke vilka risker som kan uppstå.

Avsnitt 4.4 ska revideras på följande sätt: Det finns godtagbar dokumentation av säkerhetsåtgärder för säkerhet av mobila enheter och distansarbete. Säkerhetsåtgärdernas implementering är däremot delvis oacceptabela. BYOD och hemarbete innebär oacceptabla risker i sammanhanget. Ålands Regering bör får bindande garantier från Scytl som begränsar möjligheter till BYOD och hemarbete. Dokumentet innehåller även regler för tomt skrivbord så att uttalandet avseende detta i avsnitt 4.9 ska revideras.

5.1.2 Scytl Security HR

Dokumentet innehåller omfattande och detaljerade beskrivningar av bland annat sekretessförbindelser som ska ingås av medarbetare och utbildning av medarbetare. Medarbetare utbildas avseende säkerhet och dataskydd. Det finns både grundutbildningar och avancerade utbildningar. Medarbetarnas deltagande i utbildningar protokollförs. Innehållet i dokumentet tyder på att Scytl jobbar aktivt för att skapa en hög medvetenhet för risker i samband med informationshantering hos sina medarbetare. Dokumentet är godtagbar.

5.1.3 Scytl Asset Management and Information Classification

Dokumentet innehåller omfattande och detaljerade regler för hantering av informationstillgångar. Det innehåller därutöver en omfattande informationsklassning med specifika exempel som relaterar till Scytls verksamhet. Policyn är allmänt skrivet och med tanke på Scytls typ av behandling finns det utrymme för preciseringar till exempel när det gäller ägandet av data. I övrigt är dokumentet godtagbar.

Policyn innehåller även allmänna och specifika regler för delningar med tredje parter. De specifika reglerna gäller endast Sharepoint. Reglerna är inte uttömmande och täcker inte alla tänkbara delningsscenarier. Avsnitt 4.8 måste revideras utifrån detta.

5.1.4 Scytl Access Control to Information Systems

Access control policy innehåller omfattande och detaljerade krav avseende medarbetares autentisering vilket inkluderar krav på lösenord. Dokumentet är godtagbar in den delen och sektion 4.1 ska revideras avseende autentisering av medarbetare och lösenord.

Med tanke på behandlingen som genomförs av Scytl kan beskrivningen av behörighetsstyrning i avsnitt 6 av dokumentet betraktas som knapphändigt. Eftersom det finns en öppning för att delegera ansvaret för tilldelning av behörigheter till vilken medarbetare som helst är det svårt att bedöma vem som egentligen tilldelar behörigheter utifrån denna skrivning. I detta sammanhang förefaller det som positiv att en tilldelning av behörigheter ska godkännas av säkerhetschefen. Det nämns inga allmänna begränsningar som till exempel att endast vissa personer eller funktioner ska ha tillgång till viss information. Det vore önskvärt att få se en matris över behörigheter som visar vilka funktioner som får tillgång till vilken information. Därutöver saknas en beskrivning av hur användning av behörigheter övervakas och hur missbruk av behörigheter, vilket är en potentiell personuppgiftsincident, följs upp. Denna beskrivning av behörighetsstyrning hade potentiellt varit godtagbar i andra sammanhang, men eftersom behörighetsstyrningen är av avgörande betydelse för att säkerställa att Scytl uppfyller kraven på lämpliga tekniska och organisatoriska säkerhetsåtgärder bedöms den inte vara tillräckligt detaljerad. Sektion 4.1 ska revideras utifrån detta. Dokumentation avseende behörighetsstyrningen är inte tillräckligt detaljerad. Scytl bör komma in med mer detaljerad dokumentation som till exempel en matris över behörigheter.

5.1.5 Scytl Cryptography

Dokumentet innehåller regler avseende kryptering. Det är inte tydligt huruvida dokumentet endast gäller medarbetare som utvecklare men det är ett rimligt antagande eftersom samtliga krav återfinns i avsnitt 6 med titeln ”Developer”. Dokumentet innehåller bara en kort beskrivning om hantering av krypteringsnycklar som inte är tillräckligt detaljerad. Bedömningen i avsnitt 4.11 revideras inte.

5.1.6 Password Policy – Procedure

Dokumentet innehåller omfattande och detaljerade krav avseende lösenord och är godtagbar. Sektion 4.1 ska revideras avseende lösenord.

5.1.7 Computer Security Incident Handling - Procedure

Dokumentet preciserar policyn *Computer Security Incident Handling*, se avsnitt 4.2.2 ovan. Dokumentet innehåller en klassificering av relevanta incidenter och omfattningen och detaljeringsgraden av klassningen tyder på att Scytl prioriterar incidenthantering högt. Dokumentet fördelar även ansvaret för incidenthantering bland medarbetarna och innehåller detaljerade beskrivningar om hur incidenten ska dokumenteras. Det saknas dock en rutin för att anmäla personuppgiftsincidenter till personuppgiftsansvariga. Avsnitt 4.2.2 revideras i enlighet med detta.

5.2 Slutbedömning och rekommendationer

De uppgifter som har kommit fram under den andra granskningsomgången av Skytl påverkar delvis den preliminära bedömning som gjorts i första granskningsomgången (sektion 4.13.1). Den preliminära bedömningen avseende brister i hantering av röster (sektion 4.13.2) kvarstår emellertid som oförändrad efter andra granskningsomgången och kan därför betraktas som en slutbedömning. Därutöver tillkommer en bedömning avseende implementerade säkerhetsåtgärder samt en allmän bedömning av granskningsprocessen.

5.2.1 Revidering av sektion 4.13.1 – Brister i dokumentation av säkerhetsåtgärder

Att vissa av dokumenten som presenterats under uppdateringen har en högre detaljeringsgrad och är mer strukturerad än de dokument som Scytl tidigare har lämnat in tidigare visar att Scytl har förmågan att producera dokumentation som innehåller tillräckligt med information så att de kan användas för att utvärdera tekniska och organisatoriska säkerhetsåtgärder. Frågan varför samtliga dokument inte är av liknande kvalitet och varför Scytl inkom med all dokumentation vid första förfrågan av Datainspektionen kvarstår.

Den preliminära bedömningen avseende brister i dokumentation av säkerhetsåtgärder (sektion 4.13.1) revideras enligt följande:

- Dokumentationen är delvis oorganiserad och saknar en underliggande struktur genom att dokument inte innehåller korrekta hänvisningar och att liknade ämnen beskrivs i flera dokument.
- Dokumentationen är delvis otydlig och ospecifik. En enskild medarbetare i Scytls organisationen kan ha svårigheter att förstå vad förväntas av honom eller henne avseende säkerhet av personuppgifter genom att läsa dokumentationen.
- Det är oklart huruvida vissa av dokumenten utgör bindande regler för medarbetare eller inte.
- Beskrivningen av åtgärdernas implementering är delvis godtagbar.

Sammanfattning: Det saknas information för att kunna bedöma huruvida Scytl har implementerat effektiva säkerhetsåtgärder för behandling av personuppgifter i samband med Ålands val. Dokumentationen av säkerhetsåtgärderna som har lämnats in hittills är delvis undermåliga med tanke på att Scytl ska hantera personuppgifter i samband med ett demokratisk val.
Rekommendation: Avvakta med behandlingen innan Scytl har åtgärdat bristerna i sin dokumentation. Därutöver bör en Ålands Regering överväga genomföra en revision på plats hos Scytl för att övertyga sig om säkerhetsåtgärdernas implementering.

5.2.2 Revidering av sektion 4.13.2 – Brister i hantering av röster

Det har inte kommit fram någon ny information som motiverar en revidering av den preliminära bedömningen avseende brister i hantering av röster (sektion 4.13.2). Den preliminära bedömningen kvarstår oförändrad och kan därför betraktas som en slutbedömning.

Bedömning: För att säkerställa att Invote inte drabbas av sårbarheter krävs en oberoende granskning av Invotes källkod. Möjligheten för Scytl att koppla väljare till röster behöver också utredas vidare. Det behöver göras en riskanalys som bedömer hur sannolikt det är att Scytl kan koppla innehållet i en röst till en enskild individ.

5.2.3 Bedömning av säkerhetsåtgärdernas implementering

Under andra granskningsomgången har det framkommit att säkerhetsåtgärdernas implementering delvis inte är godtagbara.

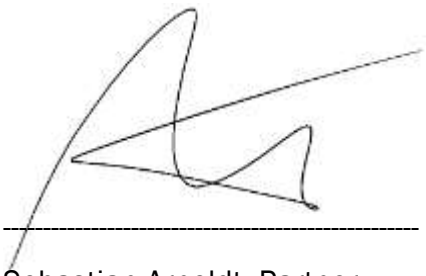
Bedömning: Säkerhetsåtgärdernas implementering är delvis inte godtagbara.
Rekommendation: Implementering av relevanta säkerhetsåtgärder bör åtgärdas i samarbete med Scytl innan behandlingen påbörjas.

5.2.4 Allmän bedömning

Kommunikationen med Scytl är fåordig. Dokumentation presenteras inte i sin helhet utan lämnas endast i omgångar. Betydande delar av dokumentationen har upprättats under våren 2019, efter att sårbarheter i en av Scytls produkter upptäcktes och publicerats. Dokumentationen är mer detaljerad när det gäller tekniska åtgärder i jämförelse med organisatoriska åtgärder vilket kan tolkas som ett tecken på att det kan finnas brister i implementeringen av organisatoriska säkerhetsåtgärder. Det som kommunicerats av Scytls medarbetare säger delvis emot det som står i dokumentationen.

Bedömning: 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.
Rekommendation: Frågetecknen bör undanröjas innan behandlingen påbörjas.

Stockholm den 12 september 2019



Sebastian Arnoldt, Partner

Bilaga 1 – Dokumentation från första granskningsomgången

Följande dokument har tillhandahållits av Scytl under den första granskningsomgången:

- Scytl's Proactive Controls – Software Development Best Practices, ingen version
- Security in projects, version 1.3
- Scytl sVote – Secure-SDLC, version 1.2
- Risk Management in OLV – Information Security Management Systems, version 1.1
- Personal Data Management – Census Management, Version 1
- Cybersecurity Controls, version 1
- Security Requirements for development, version 1.1
- Security in services provided by third parties, ingen version
- Computer Security Incident Handling – Policy, version 1
- Physical security and equipment – Information Security Management System, version 0.1
- Change Management of IS, version 1.1
- Security Organization, ingen version
- GDPR in Scytl Projects, version 1
- Annex ISO 27001 – Krav 13.5
- Annex Technical capacity – Krav 24.1
- SAML Projects, GDPR compliance, version 1.0
- RISK ANALYS VOTING PROCESS (Excelfil)
- Questions for Scytl (Wordfil)

Bilaga 2 – Dokumentation från andra granskningsomgången

Följande dokument har lämnats in av Scytl den 10 september 2019 och användes under andra den granskningsomgången:

- Scytl Information Security Policy, version 3.5
- Scytl Security HR, version 1
- Scytl Asset Management and Information Classification, version 1
- Scytl Access Control to Information Systems, version 1
- Scytl Cryptography, version 1
- Scytl Password Policy- Procedure, version 1.1
- Scytl Computer Security Incident Handling - Procedure, version 1

Bilaga 3 – Granskningsprocessens förlopp

För att illustrera granskningsprocessens förlopp presenteras en tidslinje över relevanta händelser:

- Den 19 juni 2019 inleddes tillsynsförfarandet av Datainspektionen.
- Den 24 juni 2019 fick Datainspektionen del av upphandlingsdokument och personuppgiftsbiträdesavtal mellan ÅDA AB och Scytl. Avtalet saknade tekniska och organisatoriska säkerhetsåtgärder som garanti för säkerheten.
- Den 25 juni 2019 delgav Datainspektionen Landskapsregeringen om att det förelåg ett problematik avseende ansvarsfördelningen.
- Den 26 juni 2019 redogjorde Datainspektionen för problemet för ÅDA AB. Under redogörelsen påpekades att det även saknades tekniska och organisatoriska säkerhetsåtgärder i biträdesavtalet. Frågan överlämnades åt Scytl och det konstaterades av ÅDA AB att frågan om ansvarsfördelning fick bero till augusti 2019.
- Den 11 juli 2019 skickade Datainspektionen en påminnelse till ÅDA AB gällande de tekniska och organisatoriska säkerhetsåtgärderna.
- Den 19 juli 2019 bjöds Datainspektionen in till att ta del av handlingar via en molntjänst som inte var tillämplig i sammanhanget.
- Den 15 augusti 2019 fick Datainspektionen tillgång till handlingar från Scytl via ÅDA AB.
- Den 19 augusti 2019 informerade Datainspektionen Scytl att den tillhandahållna informationen inte var tillräcklig.
- Den 30 augusti 2019 lämnade Scytl in dokumentet SAML Projects, GDPR compliance, version 1.0.
- Den 3 september 2019 lämnade Scytl in skriftliga svar på frågor som ställts en dag tidigare.
- Den 5 september 2019 lämnade Scytl in dokumentet Risk Analysis Voting Process. All dokumentation som lämnades in av Scytl till och med denna dag användes i granskningsomgång 1 (bilaga 1).
- Den 10 september 2019 lämnade Scytl in de dokument som användes i granskningsomgång 2 (bilaga 2). Dokumenten lämnades in som svar på frågor avseende specifika säkerhetsåtgärder.