Scytl

Innovating Democracy

Åland's I-voting Project

Clarification on the Audit Report by the Åland Data Protection Authority

Document version 2.0

Table of contents

List of figures

List of tables

1 Introduction

In early 2019, Scytl Secure Electronic Voting S.A. (Scytl) was awarded the contract for the provision of an I-voting as EaaS (Election as a Service) to be used in the election to the Lagtinget (the Parliament) of the Åland Islands in October 2019 by voters resident outside Åland.

In August and September 2019, a personal data protection audit was carried out on the Internet Voting project. This audit involved the Internet Voting System provider (Scytl) and was led by the the Åland Data Protection Authority (DPA).

The audit was not directly conducted by the DPA, but through an external delegated auditor (TechLaw Sweden AB). A report with the audit results was made public in September 2019 by the DPA.

During the audit, Scytl was requested in two instances both (1) to provide documentation and (2) to answer to a set of questions by the external auditor (i.e. there were two rounds of requests for information). Notwithstanding, Scytl was never contacted directly by the auditor neither there was any interaction. All sorts of communication flow were limited to the DPA.

At the end of the two rounds, an audit report was issued by the auditor to the DPA. No draft or final version was shared with Scytl, who was not able to review any initial findings or statements present in the draft or final reports before they were made public[1].

As soon as Scytl detected that the report was published, Scytl contacted both ÅDA and the DPA and alerted them that some of the findings in the report were not completely accurate and could be solved if we had access to the draft of the assessment. These inaccuracies could be due to a lack of some information and because Scytl's responses could have been misunderstood. Unfortunately, the report cannot be updated once it has been approved and published.

The DPA considered the situation and agreed to receive the missing feedback from Scytl, intending to ensure that the report is as accurate as possible. It was also agreed that the clarifications and missing feedback provided by Scytl would be published together with the original audit report.

This explanatory document responds to the already identified need of providing more meaningful information to the DPA and the external auditor. It also incorporates the feedback necessary to clarify any misunderstandings in the report published in September 2019. Specifically, we provide the necessary feedback to address certain inaccuracies regarding:

- The use of personal data by the online voting system and its treatment (sections 3.2, 4.1.2, 4.12, in the original report).
- How the online voting system worked and its main features (sections 3.1, 4.1.1, 4.12, 4.13.2 in the original report).

[1] Through later exchanges, the DPA informed Scytl that they "provided [the government of the Åland Islands] with the aforementioned report and a draft copy of the decision before publishing".

- Scytl's security policies (sections 4.1.3, 4.2.1., 4.2.2., 4.3, 4.4, 4.5, 4.7, 4.8, 4.9, 4.13.1 in the original report)[2].

The structure of this document is the following one:

- The main section of the document (section 2) is devoted to clarifying those statements that are considered not accurate. The structure of this section is the following:
    - Each of the subsections is titled with the original number and name as it appears in the original audit report. In this way, we expect clarifications to be easily matched to the statements in the report.
    - To provide a clearer structure, a snapshot of the original text in the audit report to be analyzed is presented at the beginning of each subsection. This information appears in the language of the original report (Swedish) and is followed by an automatic translation into English[3]. In this way, possible interpretation issues of the translation into English can also be identified.
    - Below each translation, we provide our feedback and further clarification to explain any disagreement with the feedback received from the auditor. In this way, we can solve all the issues that have been raised.
- The final section of this document (section 3) provides a summary of the analysis in section 2.

The authors of this report would like to apologize in advance for any misunderstandings and errors derived from an inaccurate translation of the Swedish audit report.

[2] Considering that the two latter issues are not usually within the scope of a data protection audit *strictu sensu,* it is possible that we did not provide all the necessary information to the auditor and the DPA to understand how we properly address them. Had we had access to a draft version of the report before it was published, we would have gladly provided the clarification necessary beforehand.
[3] The translation into English has been done using an online tool. This tool would be the one used by most non-Swedish readers when dealing with the original audit report.

2 Clarifications about statements

2.1 Section 3.1 Voting process

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.

Figure 1 - Section 3.1 Voting process

The written conversation with Scytl shows how a voter's personal data is dealt with during the voting process. The voter goes to a website provided by Ada AB and authenticates via BankID. Upon successful authentication, the Scytl server sends encryption keys for the voter's device used to encrypt the voter's voice. The encrypted voice is sent to the Scytl server which issues a "vote receipt" to selector. During this process, Scytl also collects the voter's IP address. The selector can later log in the service to check that the vote was submitted. However, the voter cannot review how he or she voted. However, the voter may not use digital device for this which the unit the voter voted for. After the votes have been received by the Scytl server the connection is removed between the person who has voted and its vote during a so-called mixing process. After the process is completed, it is no longer possible to connect a vote with the one who has voted.

This description of the voting process is misleading since it states that it is not possible for voters to check whether their intention has been properly registered by the voting system (individual verifiability). This statement is completely inaccurate since the voting system allows voters to check whether their encrypted votes contain their choices (cast-as-intended verifiability) and whether the ballot has been stored unmodified in the voting server (recorded-as-cast verifiability).

In fact, this property was one of the main verifiability requirements stated in the tender process and is required by the Election Act for Åland:

Section 79

Reliable system

A system for electronic voting via the internet shall be considered reliable if it meets accepted standards for electronic voting via the internet and if it fulfils the following basic requirements:

Figure 2 - Åland Election Act Section 79 - Reliable system (part 1)

[…]

7) the person who has voted shall be able to verify that the vote cast is stored in the intended electronic ballot box,

Figure 3 - Åland Election Act Section 79 - Reliable system (part 2)

The verification process worked as follows:

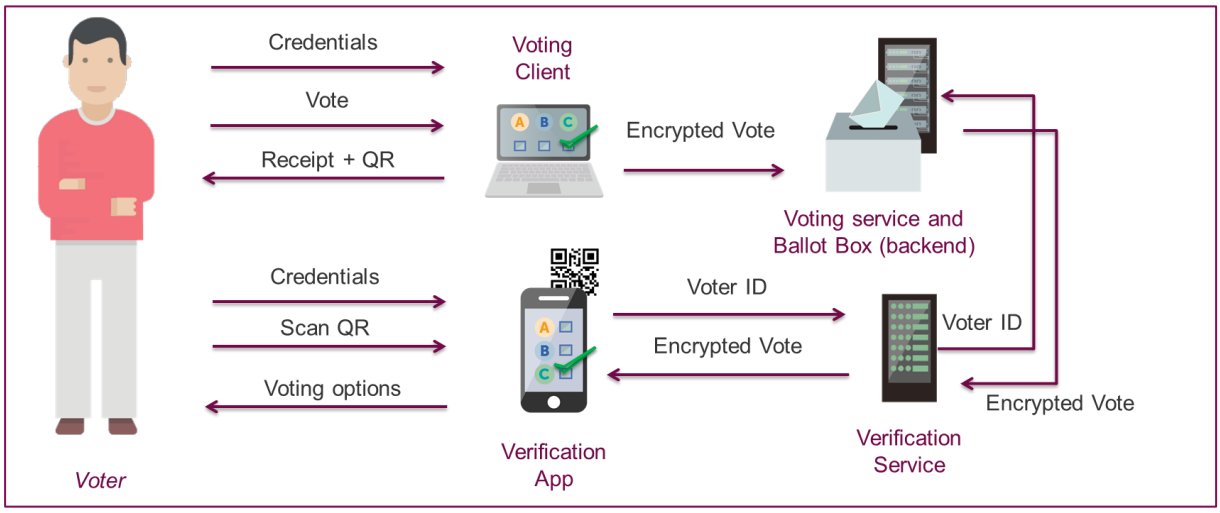

Figure 4 - Cast-as-intended verification

The voting solution shows a QR barcode to the voters, immediately after the vote has been cast, to allow them to verify whether the vote cast contains the correct selection. Voters could install a verification application on their mobile phones (available on Google Play and App Store) to verify their vote. This application allowed voters to scan the QR barcode and, after authenticating themselves, showed them the voting options retrieved from the encrypted verification data received from the voting system. If the voting process runs smoothly (i.e. if the voting device used to vote is not compromised by a malware that could change the voters' selections), the voting options displayed by the verification application are going to be the same that the voter selected.

If the choices displayed are different from those selected by the voters (meaning that their voting device has been compromised), they could have cast a new vote (either using another device or in paper) and that would cancel their previous choice.

Section 81

Execution of voting

When voting via the internet, the voter shall cast his or her vote in such a way that election secrecy is maintained.

In order to vote via the internet, the voter shall identify himself or herself and authenticate his or her identity in the manner specified.

Any person who votes in advance via the internet may vote via the internet multiple times. The last vote cast shall be counted, and previous votes shall be nullified.

Figure 5 - Åland Election Act Section 81 – Execution of voting

Section 61

Review of the advance voting documents

The central municipal election boards shall hold a meeting where they shall review the advance voting documents received by the board no later than 19.00 on the Friday before election day. A vote shall be disregarded if:

Figure 6 - Åland Election Act Section 61 – Review of advance voting documents (part 1)

[…]

6) it is to be disregarded under the order of priority set out in paragraph 3. If a voter has voted multiple times during the advance voting period, the votes shall be considered in the following order:

1) voting at an advance polling station,
2) postal voting,
3) voting via the internet.

Advance voting consignments that are received late may not be opened. If a vote is disregarded, the ballot envelope may not be opened. An open ballot envelope shall be sealed in a way that maintains election secrecy.

Figure 7 - Åland Election Act Section 61 – Review of advance voting documents (part 2)

The process for individual verification of the vote was explained to the auditor in the written responses to his questions during the first round.

2.2 Section 3.2 Types of personal data

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.

Figure 8 - Section 3.2 Types of personal data

During the voting process, information about how voters have voted, IP addresses and information, is processed via the users' digital devices. According to Article 6 (1) DSF, data on political matters opinions and thus votes cast in a political election are considered as particular categories of personal data. IP addresses and user device information are normally classified as ordinary personal data. If, on the other hand, this information is linked to a voter's vote, these data must also be classified as special categories of personal data. Special categories of personal data require a higher level of security measures than usual personal data.

First, it is important to distinguish between an encrypted[4] vote and a clear text vote. An encrypted vote cannot be considered a special category of data. Only the contents of that vote, once decrypted, can be considered as such. Encrypting a vote can be seen as sealing a vote in an envelope[5]. Therefore, during the voting phase, the categories of personal data in the system (e.g. IP addresses) can only be linked to the encrypted vote (i.e. a cyphertext) and not to its contents (e.g. the cleartext).

In remote voting, it is necessary to link the voter's identity (usually through a pseudonymous[6], such as a VoterID) to the vote that they have cast, while preserving the confidentiality of their choices. When compared to postal voting, for instance, the situation is the same when votes are sent to the electoral administration (i.e. votes are put in a second envelope that contains proof of the voter's identity, e.g. a voting card[7]). Election authorities could otherwise not be able to verify that all votes received have been cast by an eligible voter. This is also a requirement in the case of the Åland's election:

[4] GDPR refers to encryption as "the procedure that converts clear text into a hashed code using a key, where the outgoing information only becomes readable again by using the correct key."
[5] Scytl believes that encryption is more robust than putting a vote inside a paper envelope.
[6] According to GDPR, "'[p]seudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."
[7] In the case of the Åland Islands, Section 77 of the Election Act for Åland provides that, in order to cast a postal ballot, "[t]he covering letter shall be completed [by the voter] in accordance with the instructions, and the ballot envelope, containing a ballot and the covering letter, shall then be placed inside the covering envelope. Instead of a covering letter, the voter may enclose his or her voting card, which shall be signed by the voter."

Section 79

Reliable system

A system for electronic voting via the internet shall be considered reliable if it meets accepted standards for electronic voting via the internet and if it fulfils the following basic requirements:

Figure 9 - Åland Election Act Section 79 - Reliable system (part 1)

[…]

8) it shall be possible to verify, by means that are independent of the system, that
a) the votes that are counted were cast by voters who are eligible to vote and
b) that all votes that have been cast by voters who are eligible to vote are counted in the way in which they are cast, and

Figure 10 - Åland Election Act Section 79 - Reliable system (part 2)

Furthermore, linking the encrypted vote back to the identity of a voter is necessary when multiple voting is possible, especially when voters have the choice to cast multiple votes through different channels (e.g., online and by post). This was the case in the elections in Åland:

Section 85

Notification of other voting

The central municipal election board shall notify the central committee for parliamentary elections of the voters who have voted via the internet and who have also voted in any other way during the advance voting period, by the means determined by the central committee for parliamentary elections. The voter's personal identity code shall be given where necessary. The central committee for parliamentary elections shall have access to the notification no later than 12.00 on election day.

The central committee for parliamentary elections shall ensure that the votes cast via the internet by the voters referred to in paragraph 1 are nullified. The votes and information on who has voted shall be deleted from the electronic ballot box before it is opened and the votes counted.

Figure 11 - Åland Election Act Section 85 – Notification of other voting

Therefore, it is important to assess whether the process used to break any correlation between the envelopes and the voter's identity is robust and whether this process is keeping or not any link that could compromise voter's privacy. In postal voting, this is done by detaching the identity of the voter from the envelope that contains the vote before putting it in a ballot box. The ballot box is then shuffled before the envelopes are opened and the votes are retrieved. In the electronic voting system provided by Scytl, this is done through a cryptographic mixing process. The cryptographic mixing process shuffles the encrypted votes and re-encrypts them at the same time. In this way, any correlation between the original encrypted votes and the re-encrypted ones is broken.

Additionally, the private key used to decrypt the votes does not exist as such (i.e. it is not stored anywhere). The key is split into shares and can only be used once a predefined number of members of members of the Electoral Board (i.e. the threshold) joins and reconstructs it using each one's share of the key. Therefore, the decryption process is never in the hands of Scytl nor in the hands of a single individual member of the Electoral Board.

This is required by the Election Act for Åland:

Section 82

Electronic ballot box

Votes cast via the internet shall be stored in an electronic ballot box for which the central committee for parliamentary elections is responsible.

The central committee shall appoint at least five persons who shall be responsible for opening the electronic ballot box. When those persons are appointed, emphasis should be placed on their enjoying a high degree of general trust, representing different sectors of society and both genders, and having an insight into the need for security and the protection of privacy in an election. A person who is a candidate in a parliamentary or municipal election may not be appointed.

The electronic tools required in order to open the electronic ballot box shall be distributed among the persons appointed under paragraph 2. It shall not be possible to open the ballot box if at least three of those persons are not present at the same time.

Figure 12 - Åland Election Act Section 82 - Electronic ballot box

To sum up, and even though the voting system stores certain categories of personal data that are necessary to prevent a voter from casting multiple votes, these data cannot be directly or indirectly correlated to the votes in clear text (only to the encrypted ones).

2.3 Section 4.1.1 Voters

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.

Figure 13 - Section 4.1.1 Voters (part 1)

One weakness of the system is that it is not possible to ensure that the person who is using the digital evidence to cast their vote is really the voting person. It is conceivable that a voting person shares his BankID with someone another person, which may allow that person to vote in it the person entitled to vote.

Since there is no face-to-face voter identification, voter authentication in any remote voting channel is a challenge. This is the case of Internet voting but also postal voting. Therefore, the risks accepted by any electoral administrations offering their voters the choice to cast a remote electronic vote are no higher than those accepted in postal voting.

As implemented for the elections in Åland, to allow impersonation, the voter would have to share their BankID with another person. This can also be done in postal voting if the voter hands their voting card (or covering letter) to a third party. We do not see any difference in risk in these two cases.

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.

Figure 14 - Section 4.1.1 Voters (part 2)

In traditional elections, this risk is usually eliminated by implementing one face check of the voting person by means of a valid ID document containing an image. In the case of letter voting, this risk is excluded by the demands of witnesses. Also, if a possible forgery of testimony is possible, this can, depending on circumstances, is considered a higher threshold than accessing another person BankID.

This statement is not accurate. In parliament and local councils' elections in Åland, witnesses are not required by the Election Act when voters cast their votes by post. Specifically, the postal voting process goes as follows:

Section 77

Execution of voting

When voting by post, the voter shall place his or her mark on the ballot or on each of the ballots, and then enclose the folded ballot(s) in their respective ballot envelopes, which shall then be sealed. No marks may be placed on the ballot envelopes. The voter shall ensure that election secrecy is maintained. The covering letter shall be completed in accordance with the instructions, and the ballot envelope, containing a ballot and the covering letter, shall then be placed inside the covering envelope. Instead of a covering letter, the voter may enclose his or her voting card, which shall be signed by the voter. The voter shall address the covering envelope to the central municipal election board and send it by post or by other means. The voter himself or herself is responsible for ensuring that the covering envelope is received by the central municipal election board within the allotted time period.

Figure 15 - Åland Election Act Section 77 - Execution of voting

As described in the excerpt above, no witnesses are required to cast a vote by post. Therefore, even though it is not clear that adding a witness would make the authentication stronger than through a BankID, postal voting in Åland does not require witnesses to make the voter authentication more secure than through a BankID.

In the specific case of the Åland election, therefore, this argument does not apply.

2.4 Section 4.1.3 Employees

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

Figure 16 - Section 4.1.3 Employees (part 1)

Scytl's employees have access to the system's server component. In Scytl's documentation of security measures describe procedures for authenticating employees and managing them authorizations at an overall level. For example, it is described that employees rights are managed through Active Directory, which employees should only have access to tasks that they need for their work and that the number of employees who have access to (…)

This statement is misleading. Only the members of the IT department assigned to the project have access to the server components. Any other employees could not even reach the servers.

The access is done via a bastion host where every action is logged. Only the IT members assigned to the project can access these systems. This was already mentioned when answering the first round of questions. It is also highlighted here to avoid further misinterpretations.

> 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").

Figure 17 - Section 4.1.3 Employees (part 2)

> *an election project should be kept to an absolute minimum. However, it is lacking in detail descriptions of how authentication is designed, for example through policies for password or whether a smart card or similar is required to access work computers. In addition, there is no detailed and comprehensive description of how access control policy is designed.*

This is not completely accurate: Scytl does have a specific access control policy ISO document called "ISD.1.9 Access Control to Information Systems" that covers this item. This document was shared as part of the second round of requests for information. Based on the assessment in the original report, we understand that the auditor also wanted to know the measures implemented in relation to these policies. These measures are detailed in a document called "PRO.007 User Management" that explains the implementation procedures of the 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.

Figure 18 - Section 4.1.3 Employees (part 3)

Assessment: The system uses BankID for authentication of voters. BankID is for currently one of the safest methods for authenticating people on the internet. However, the method is not as secure as the authentication methods used traditional elections and letter voting. However, it is unlikely, but not excluded, that Vulnerabilities related to authentication with BankID can lead to a decisive impact on the election because it would require a large number of voters to lose control its BankID. This risk is further limited by only a fraction of the Åland Islands citizens will vote electronically. Otherwise, the methods used are authentication acceptable.

There is no access control policy. This in itself does not have to be an obstacle when Scytl meets the requirements for authentication and authorization management but should be addressed before treatment begins.

This assessment should be reviewed in light of previous remarks. Since postal voting does not require witnesses, it cannot be considered more robust than BankIDs. Furthermore, while we agree that documentation of Scytl's implementation of its access control policies was missing, that does not mean that there is no access control policy.

2.5 Section 4.2.1 Logging and logging controls

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.

Figure 19 - Section 4.2.1 Logging and logging controls

Assessment: The documentation contains logging requirements that correspond to requirements in adopted safety standards. However, it is not sufficiently detailed how these requirements are implemented. There are also no rules for handling logs and log controls.

Requests for information about log management were made and responded in the second round of questions.

Scytl has a specific document describing how to manage, process and register log information called “Parseable and good secure logs”. This document is completed with the “Secure Logger” documentation, which explains Scytl’s developed solution to protect the integrity and authenticity (immutabilisation) of the log data generated by Scytl’s solutions. Finally, there is a policy according to the ISO27001 requirements called “ISD.1.12- System Management and Operations” where logging and monitoring are explained in detail.

2.6 Section 4.2.2 Incident Management

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.

Figure 20 - Section 4.2.2 Incident Management

Assessment: The policy for handling security incidents is inadequate. Furthermore, there are no rules for reporting personal data incidents to the data controller. The person who is holding the role of data protection officer is inappropriate because of conflicts of interest.

Regarding the role of Data Protection Officer (DPO), it is shared between the members of the Data Protection Committee. The Data Protection Committee is composed of five different representatives of the main departments involved in data protection, i.e. the Legal department, the IT department, the Delivery department, the Product department, and the Security department.

The Security Director is only the point of contact of this Committee for our customers, but the responsibilities of the role are shared among the members of the Data Protection Committee and decisions are taken by the whole Committee. This information was already communicated to the DPA during the audit process.

2.7 Section 4.3 Security on computers

Bedömning: Det saknas en policy för säkerhet av datorer.

Figure 21 - Section 4.3 Security on computers

Conclusion: A computer security policy is missing.

Scytl initially shared the document "ISD.1.11 Physical safety and equipment" in the first round of questions. In the second round, we shared the document "ISD.1,1 SCYTL Group Security Regulation" (entitled "Information Security Policy 3.5" in the auditor's list). Both provide the requested policies, but neither of them is mentioned in the auditor's original report.

The link between the ISO documents and the related topics is provided in the following table (Two documents of this table were already shared during the audit):

ISO Control	Topic	Document
A.11.2.1	Equipment sitting and protection	ISD.1.11 Physical safety and equipment
A.11.2.2	Supporting utilities	ISD.1.11 Physical safety and equipment
A.11.2.3	Cabling security	ISD.1.11 Physical safety and equipment
A.11.2.4	Equipment maintenance	ISD.1.11 Physical safety and equipment
A.11.2.5	Removal of assets	ISD.1.11 Physical safety and equipment
A.11.2.6	Security of equipment and off-premises assets	ISD.1.1 SCYTL Group Security Regulation ISD.1.11 Physical safety and equipment ISD.1.12 -System Management and operations
A.11.2.7	Secure disposal or reuse of equipment	ISD.1.11 Physical safety and equipment PRO.006 Media and Data Sanitations Process
A.11.2.8	Unattended user equipment	ISD.1.1 SCYTL Group Security Regulation
A.11.2.9	Clear desk and clear screen policy	ISD.1.1 SCYTL Group Security Regulation

Table 1 – Scytl's ISO 27001 Annex 11 related documentation available

2.8 Section 4.4 Security of mobile devices and teleworking

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

Figure 22 - Section 4.4 Security of mobile devices and remote working

Assessment: Documentation about rules for use of mobile devices and remote working is substandard.

In the second round of requests for information, we shared the document "ISD.1.1 SCYTL Group Security Regulation". In this document, we explain the restrictions on using mobile devices and remote working.

2.9 Section 4.5 Security of websites, servers and internal networks

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.

Figure 23 - Section 4.5 Security of Web Sites, Servers and Internal Networks

Assessment: The safety requirements described in the documentation correspond to accepted safety standards. The implementation of the requirements is not specific enough.

The documentation applies only to customer projects and not Scytl's information management in general. It is not clear whether the documentation constitutes binding requirements or only examples of security measures that may be used.

The documentation provided by Scytl during the audit was mainly related to this project. Documentation on Scytl's policies was, however, always available upon request. Other documents and risk analyses of the data protection treatment of the company were also available. This was mentioned during the initial exchanges with the DPA.

All the documentation shared is the standard and mandatory controls that Scytl implements, and therefore are binding to its employees. They are part of the ISO 27001 compliance documentation of Scytl.

2.10 Section 4.6 Backups

Bedömning: Dokumentation av åtgärder avseende säkerhetskopior är undermålig.

Figure 24 - Section 4.6 Backups

Assessment: Backup measures documentation is poor.

In this case, we agree with the assessment by the auditor. The specific information about backups in the project was not completely ready by the time of the audit.

2.11 Section 4.7 Deletion of data

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

Figure 25 - Section 4.7 Deletion of data

Assessment: Documentation of data erasure measures is substandard.

There is a specific document that explains the deletion procedure entitled “PRO.006 Media and data sanitation process”. However, this document was not initially identified as necessary to share in any of the rounds of requests for information, until we read the assessment of the auditor.

Scytl follows a precise policy for an appropriate secure data deletion process.

2.12 Section 4.8 Secure communication with external parties

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.

Figure 26 - Section 4.8 Secure communication with external parties

Assessment: Regarding the regulation of external parties' access to Scytl's internal system, the documentation is acceptable. Regarding employees' exchange of data with the rest of the world, the documentation is deficient. It is unclear whether the existing documentation can be equated with binding policies for employees.

According to the comments provided, we assume that the auditor did not consider the relevant documentation when addressing Scytl's policies for employees. This information is in the document "ISD.1.1 SCYTL Group Security Regulation", shared with the DPA in the second round of requests for information. This documentation is part of the ISO 27001's set used in the compliance process, and it is therefore binding.

2.13 Section 4.9 Physical safety

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

Figure 27 - Section 4.9 Physical safety

Assessment: Scytl's physical safety measures are acceptable. However, it is missing rules for clean desktops and blank screen for information processing resources.

As already mentioned, policies on desktops cleaning procedures are part of the document ISD.1.1 SCYTL Group Security Regulation".

2.14 Section 4.12 Security of votes

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”.

Figure 28 - Section 4.12 Security of votes (part 1)

In conversation with Scytl, the company's representatives have only delivered few worded answers regarding this problem. Scytl claims that the vulnerabilities have been fixed, that the Government of Åland will not use the same system as Swiss Post (Swiss Post used sVote, the Government of Åland will use Invote) and that Invote was not affected by the same vulnerabilities as sVote. According to the company, sVote and Invote share "only a few libraries" and are implemented in "completely different ways".

In Switzerland, researchers detected only three vulnerabilities in a new Swiss eVoting system (sVote) that was open to public scrutiny as part of its certification process (the system was not being used in Switzerland since it was aimed at higher certification levels than those of the currently existing solutions). Only two of these three vulnerabilities were related to the cryptographic components used in the voting system in place in Åland (Invote), i.e. the mixing proofs and the decryption audit proofs.

As described[8] by the researchers, the vulnerability was on the proof system used to audit the mixing and decryption processes. It consisted in preventing any third party from being able to ensure whether the software executed was the one provided by Scytl or another one developed by an attacker (i.e., the attack cannot be made using Scytl's official software but requires that it is replaced by another one).

In any case, the vulnerabilities were easy to solve. The solution implemented was reviewed and accepted by external researchers ahead of the elections (e.g. the mixing process used in Australia in March was already implementing the correct mixing proof and the source code to check it is public[9]).

It is also important to mention that, while this personal data audit was carried out, another security audit was in process on the Åland voting system by other security experts appointed by the Government of Åland. The second audit was testing the technical security measures implemented in the system.

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.

Figure 29 - Section 4.12 Security of votes (part 2)

[8] 15. Lewis, Sarah Jamie; Pereira, Olivier and Teague, Vanessa. *How not to prove your election outcome: The use of non-adaptive zero knowledge proofs in the Scytl-Swiss Post Internet voting system, and its implications for decryption proof soundness*, 2019.

[9] https://www.scytl.com/en/AccessiVote2019/

In addition, in the document SAML Projects, GDRP compliance, Scytl states that voters' IP addresses are collected and stored for security purposes. They also claim that IP addresses cannot be used to identify voters. In the conversation, however, Scytl admits that it is possible to identify voters using the IP address. Each vote left receives a unique VoterID with a timestamp. Each IP address that is logged also receives a timestamp. By correlating the timestamp created for VoterID and IP address, it becomes possible to identify who has left which vote. Therefore, since Scytl can decrypt the votes, it is not excluded that Scytl would be able to associate decrypted votes with IP addresses belonging to individual voters and thus get to know who has voted what in the election.

It seems that Scytl's claim about the impossibility to correlate IP addressed to voters was not clear. Scytl has no information to correlate IP addresses with the real identity of a voter. The IP address could be correlated with a "pseudonymous" voter identifier (VoterID) used to ensure that a vote has been cast by an eligible voter and that no voter has voted twice (see section 2.3 above). Under no circumstances can Scytl correlate this voter identifier with the real identity of the voter.

Furthermore, and as already mentioned, these identifiers could only be linked to the encrypted vote, but not the decrypted one. This is because, as already explained, the voting system implements a mixing process that breaks any correlation between the votes cast and the pseudonymous of the voter. Only once this correlation has been broken does the Electoral Board proceed to decrypt the mixed votes.

In the statement above the auditor also makes an inaccurate statement that must be clarified: following the provisions of the Election Act for Åland (see section 2.3 above) Scytl was not in charge of the votes' decryption process, but the Electoral Board was (i.e., the persons appointed by the central committee for parliamentary elections as described in Section 82). The auditor himself mentions this in section 4.1.2 of his report. Under no circumstances can Scytl's employees be members of this board. In addition to this, to decrypt the votes it is necessary that a predefined number of members of the Electoral Board (i.e., a threshold of the members) reconstructs the election private key. Therefore, neither Scytl employees nor less than the three required members of the Electoral Board can decrypt the votes.

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.

Figure 30 - Section 4.12 Security of votes (part 3)

Verdict: Scytl has built a well-thought-out encryption solution to protect the voting integrity and confidentiality based on the state-of-the-art encryption standards. The solution is well documented. However, researchers have shown vulnerabilities in one of Scytl's products (sVote) that can be used to influence the election result. It cannot be ruled out that Invote is also affected by vulnerabilities. To ensure that Invote does not suffer from this, an independent review of Invote's source code is required.

During the audit, a possible way of identifying voters indirectly through their IP addresses was also discovered. It is not excluded that the clutch can be used to see how individual voters have voted.

As mentioned before, vulnerabilities that could affect common components in Åland were solved before the election and had been already reviewed (in some cases even in public, such as the case for the mixing in New South Wales, in Australia). Therefore, no vulnerabilities were pending to solve in the Åland voting system. However, it is fair that the auditor asks for a review of the code to ensure that vulnerabilities were not still present in the Åland voting system.

As mentioned before, IP addresses can only be correlated with a “pseudonymous” voter identifier used to ensure that a vote has been cast by an eligible voter and that no voter has voted twice (see section 2.3 above). However, this link is only maintained with the encrypted vote. The use of a mixing process and a secret-sharing scheme ensure that this link is broken before votes are decrypted and their contents are known.

2.15 Section 4.13.1 Deficiencies in documentation of security measures

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.

Figure 31 - Section 4.13.1 Deficiencies in documentation of security measures

Summary: There is no information available to assess whether Scytl has implemented effective security measures for the processing of personal data in connection with the Åland elections. The documentation of the security measures that have been submitted so far is substandard given that Scytl is handling personal data in connection with a democratic election.

Recommendation: Wait for treatment before Scytl has corrected the deficiencies in its documentation. In addition, an Åland Government should consider conducting an on-site audit at Scytl to convince itself of the implementation of the security measures.

Scytl disagrees with this conclusion. Maybe Scytl did not realize that the provided information requested in the two rounds was enough. But we did not identify this until we get access to the auditor assessment. Otherwise, Scytl had the possibility to show that it implemented effective security measures for the processing of personal data for the election by covering any missing gap.

Furthermore, the documentation provided is related to Scytl's certification process under ISO 27001. Therefore, it is not clear to us why it got assessed as substandard. All the documentation under ISO 27001 has the same structure:

- Objective.
- Scope of solution.
- Definitions.
- Responsibilities.
- Policy.
- Development of the policy.

Besides, the security framework is detailed in the document "ISD.1.5 Security Framework".

The following table shows the details for each document and its topic that could be shared with the auditor. For obvious reasons, we did not share all the set of documents under the ISO with the auditor since this is not the usual procedure under a personal data audit process for a project (not one for an ISO certification).

ISO Control	Topic	Document
A.5	Information Security Policies	
A.6	Organization of information security	
A 6.1	Internal Organization	
A.6.1.1	Information Security roles and responsibilities	ISD.1.6 Security Organization
A.6.1.2	Segregation of duties	ISD.1.6 Security Organization ISD.1.9 Access Control to Information Systems v.0.1 ISD.1.12 -System Management and operations ISD.1.14 Change management v1.1
A.6.1.3	Contact with authorities	ISD.1.6 Security Organization
A.6.1.4	Contact with special interest groups	ISD.1.6 Security Organization
A.6.1.5	information security in project management	PRO.008 SCTYL Security in Projects
A 6.2	Mobile devices and teleworking	
A.6.2.1	Mobile device policy	SCYTL Group Security Regulation ISD.1.12 -System Management and operations (Article 9) ISD.1.9 Access Control to Information
A.6.2.2	Teleworking	SCYTL Group Security Regulation ISD.1.9 Access Control to Information
A.7	Human resource security	
A.7.1	Prior to employment	
A.7.1.1	Screening	ISD1.7 HHRR Security 1.0
A.7.1.2	Terms and conditions of employment	ISD1.7 HHRR Security 1.0 ISD.0 Security Principles SCYTL Group Security Regulation
A.7.2	During employment	
A.7.2.1	Management responsibilities	ISD1.7 HHRR Security 1.0
A.7.2.2	Information security awareness, education and training	ISD1.7 HHRR Security 1.0
A.7.2.3	Disciplinary process	ISD.0 Security Policies SCYTL Group Security Regulation ISD1.7 HHRR Security 1.0

A.7.3	Termination and change of employment	
A.7.3.1	Termination or change of employment responsibilities	ISD1.7 HHRR Security 1.0
A.8	Asset management	
A 8.1	Responsibility for assets	
A.8.1.1	inventory of assets	ISD.1.8 Asset Management and Information Classification
A.8.1.2	Ownership of assets	ISD.1.8 Asset Management and Information Classification
A.8.1.3	Acceptable use of assets	ISD.1.8 Asset Management and Information Classification ISD.1.1 SCYTL Group Security Regulation
A.8.1.4	Return of assets	ISD1.7 HHRR Security 1.0
A 8.2	Information classification	
A.8.2.1	Classification of information	ISD.1.8 Asset Management and Information Classification
A.8.2.2	Labelling of information	ISD.1.8 Asset Management and Information Classification
A.8.2.3	Handling of assets	ISD.1.8 Asset Management and Information Classification ISD.1.15 Third party Security
A 8.3	Media Handling	
A.8.3.1	Management of removable media	ISD.1.8 Asset Management and Information Classification
A.8.3.2	Disposal of media	SCYTL Group Security Regulation ISD.1.8 Asset Management and Information Classification PRO.002 Media and data sanitization process
A.8.3.3	Physical media transfer	SCYTL Group Security Regulation ISD.1.8 Asset Management and Information Classification ISD.1.12 -System Management and operations ISD.1.13- Security in Communications.
A.9	Access control	
A.9.1	Business requirements of access control	
A.9.1.1	Access control policy	ISD.1.9 Access Control to Information Systems v.0.1 PRO.007 - user management PRO.008 Scytl Security in projects

A.9.1.2	Access to networks and network services	ISD.1.9 Access Control to Information Systems v.0.1 ISD.1.1 SCYTL Group Security Regulation PRO.008 Scytl Security in projects
A 9.2	User access Management	
A.9.2.1	User registration and de-registration	ISD.1.9 Access Control to Information Systems v.0.1 PRO.007.User Management PRO.008 Scytl Security in projects
A.9.2.2	User access provisioning	ISD.1.9 Access Control to Information Systems v.0.1 PRO.007.User Management PRO.008 Scytl Security in projects PRO.002 Secret Sharing procedure
A.9.2.3	Management of privileged access rights	ISD.1.9 Access Control to Information Systems v.0.1 PRO.007.User Management PRO.008 Scytl Security in projects
A.9.2.4	Management of secret authentication information of users	ISD.1.9 Access Control to Information Systems v.0.1 PRO.007.User Management PRO.008 Scytl Security in projects
A.9.2.5	Review of user access rights	ISD.1.9 Access Control to Information Systems v.0.1 PRO.007.User Management PRO.008 Scytl Security in projects
A.9.2.6	Removal or adjustment of access rights	SCYTL Group Security Regulation ISD.1.9 Access Control to Information Systems v.0.1 PRO.007.User Management PRO.008 Scytl Security in projects
A 9.3	User responsibilities	
A.9.3.1	Use of secret authentication information	SCYTL Group Security Regulation ISD.1.9 Access Control to Information Systems v.0.1 PRO.004 Password Policy and Guidelines
A 9.4	System and application access control	
A.9.4.1	Information access restriction	SCYTL Group Security Regulation ISD.1.9 Access Control to Information Systems v.0.1

A.9.4.2	Secure log-on procedures	ISD.1.9 Access Control to Information Systems v.0.1 SCYTL security in projects v1.3
A.9.4.3	Passwords management system	ISD.1.9 Access Control to Information Systems v.0.1 PRO.002 Secret Sharing procedure
A.9.4.4	Use of privileged utility programs	ISD.1.9 Access Control to Information Systems v.0.1
A.9.4.5	Access control to program source code	ISD.1.9 Access Control to Information Systems v.0.1
A.10	Cryptography	
A 10.1	Cryptographic controls	
A.10.1.1	Policy on the use of cryptographic controls	ISD.1.10 cryptography SCYTL security in projects v1.3
A10.1.2	Key management	ISD.1.10 cryptography
A.11	Physical and environmental security	
A.11.1	Secure areas	
A.11.1.1	Physical security perimeter	ISD.1.11 Physical safety and equipment
A.11.1.2	Physical entry controls	SCYTL Group Security Regulation ISD.1.11 Physical safety and equipment SCYTL Visitor Policy
A.11.1.3	Securing offices, rooms and facilities	SCYTL Group Security Regulation ISD.1.11 Physical safety and equipment
A.11.1.4	Protecting against external and environmental threats	ISD.1.11 Physical safety and equipment SCYTL security in projects v1.3
A.11.1.5	Working in secure	ISD.1.11 Physical safety and equipment SCYTL security in projects v1.3
A.11.1.6	Delivery and loading areas	ISD.1.11 Physical safety and equipment
A 11.2	Equipment	
A.11.2.1	Equipment sitting and protection	ISD.1.11 Physical safety and equipment
A.11.2.2	Supporting utilities	ISD.1.11 Physical safety and equipment
A.11.2.3	Cabling security	ISD.1.11 Physical safety and equipment
A.11.2.4	Equipment maintenance	ISD.1.11 Physical safety and equipment
A.11.2.5	Removal of assets	ISD.1.11 Physical safety and equipment
A.11.2.6	Security of equipment and assets off-premises	ISD.1,0 Group Security Regulation ISD.1.11 Physical safety and equipment ISD.1.12 -System Management and operations
A.11.2.7	Secure disposal or reuse of equipment	ISD.1.11 Physical safety and equipment PRO.006 Media and Data Sanitations Process

A.11.2.8	Unattended user equipment	ISD.1.1 SCYTL Group Security Regulation
A.11.2.9	Clear desk and clear screen policy	ISD.1.1 SCYTL Group Security Regulation
A.12	Operation security	
A.12.1	Operation procedures and responsibilities	
A.12.1.1	Documented operating procedures	PRO.005 Sharing documentation PRO.009 Windows 10 Hardening Procedure PRO.011 Secret Sharing procedure SCYTL Visitor Policy
A.12.1.2	Change management	ISD.1.12 -System Management and operations ISD.1.14 Change management v1.1
A12.1.3	Capacity management	ISD.1.12 -System Management and operations
A12.1.4	Separation of development, testing and operational environments.	ISD.1.12 -System Management and operations ISD.1.14 Change management v1.1
A. 12.2	Protection from malware	
A12.2.1	Controls against malware	ISD.1.12 -System Management and operations SCYTL Group Security Regulation
A.12.3	Backup	
A.12.3.1	Information backup	SCYTL Group Security Regulation ISD.1.12 -System Management and operations
A.12.4	Logging and monitoring	
A.12.4.1	Event logging	ISD.1.12 -System Management and operations ISD.1.14 Change management v1.1
A.12.4.2	Protection of log information	ISD.1.12 -System Management and operations
A.12.4.3	Administrator and operator logs	ISD.1.12 -System Management and operations
A.12.4.4	Clock synchronization	ISD.1.12 -System Management and operations
A.12.5	Control of operational software	
A.12.5.1	Installation of software on operational systems	ISD.1.12 -System Management and operations ISD.1.14 Change management v1.1
A. 12.6	Technical vulnerability management	
A.12.6.1	Management of technical vulnerabilities	ISD.1.14 Change management v1.1 Scytl S_SDL

A.12.6.2	Restrictions on software installation	ISD.1.12 -System Management and operations ISD.1.14 Change management v1.1
A 12. 7	Information systems audit considerations	
A.12.7.1	Information systems audit controls	ISD.1.4 Technical Audit v1 SCYTL Internal Audit v3
A.13	Communication security	
A 13.1	Network security management	
A.13.1.1	Network controls	ISD.1.1 SCYTL Group Security Regulation PRO.008 SCYTL security in projects ISD.1.9 Access Control to Information Systems v1 ISD.1.12 -System Management and operations ISD.1.19 Cloud Policy ISD.1.13 Security in communications
A.13.1.2	Security of networks services	ISD.1.15 Third party sec ISD.1.13 Security in communications
A13.1.3	Segregation in networks	ISD.1.12 System Management and operations ISD.1.13 Security in communications
A 13.2	Information transfer	
A.13.2.1	Information transfer policies and procedures	ISD.1.15 Third party security PRO.001 Personal Data Management PRO.005 Sharing documentation with SharePoint v1 ISD.1.1 SCYTL Group Security Regulation ISD.1.19 Cloud Policy
A.13.2.2	Agreements on information transfer	ISD.1.15 Third party security ISD.1.1 SCYTL Group Security Regulation ISD.1.12 -System Management and operations
A.13.2.3	Electronic messaging	ISD.1.12 -System Management and operations PRO.002 Secret Sharing procedure
A.13.2.4	Confidentiality or non-disclosure agreements	ISD.1.15 Third party security ISD.1.7 HHRR Security v.1.0
A.14	System acquisition, development and maintenance	
A 14.1	Security requirements of information system	

A.14.1.1	Information security requirements analysis and specification	ISD.1.14 Change management v1.1
A.14.1.2	Securing application services on public networks	ISD.1.20 security requirements for development. PRO.008 SCYTL Security in projects
A.14.1.3	Protecting application services transactions	ISD.1.12 -System Management and operations ISD.1.13- Security in communications.
A 14.2	Security in development and support processes	
A.14.2.1	Secure development policy	ISD.1.20 security requirements for development. SCYTL security in projects v1.3 Scytl S-SDLC Scytl's Proactive Controls
A.14.2.2	System change control procedures	ISD.1.14 Change management v1.1
A.14.2.3	Technical review of applications after operating platform changes	ISD.1.14 Change management v1.1
A.14.2.4	Restrictions on changes to software packages	ISD.1.14 Change management v1.1 ISD.1.20 security requirements for development.
A.14.2.5	Secure system engineering principles	SCYTL security in projects v1.3 ISD.1.20 security requirements for development. PRO.009 Windows 10 Hardening Procedure
A.14.2.6	Secure development environment	ISD.1.20 security requirements for development. SCYTL security in projects v1.3
A.14.2.7	Outsourced development	ISD.1.20 security requirements for development.
A.14.2.8	System security testing	ISD.1.12 -System Management and operations ISD.1.14 Change management v1.1 ISD.1.20 security requirements for development. PRO.008. SCYTL security in projects
A.14.2.9	System acceptance testing	ISD.1.12 -System Management and operations ISD.1.14 Change management v1.1 ISD.1.20 security requirements for development.

A 14.3	Test data	
A.14.3.1	Protection of test data	ISD.1.20 security requirements for development
A.15	Supplier Relationships	
A 15.1	Information security in supplier relationships	
A.15.1.1	Information security policy for supplier relationships	ISD.1.15 Third party security
A.15.1.2	Addressing security within supplier agreements	ISD.1.15 Third party security ISD.1.9 Access Control to Information Systems v.0.1
A.15.1.3	Information and communication technology supply chain	ISD.1.15 Third party security
A.15.2	Supplier service delivery management	
A.15.2.1	Monitoring and review of supplier services	ISD.1.15 Third party security
A.15.2.2	Managing changes to supplier services	ISD.1.15 Third party security
A.16	Information security incident management	
A.16.1	Management of information security incident and improvements	
A.16.1.1	Responsibilities and procedures	ISD.1.16 Security Incident Policy v.1.0 PRO.010 Security Incident Procedures v.1.0 ISD.1.7 HHRR Security v.1.0
A.16.1.2	Reporting information security events	ISD.1.16 Security Incident Policy v.1.0 PRO.010 Security Incident Procedures v.1.0
A.16.1.3	Reporting information security weaknesses	ISD.1.16 Security Incident Policy v.1.0
A.16.1.4	Assessment of and decisions on information security events	ISD.1.16 Security Incident Policy v.1.0 PRO.010 Security Incident Procedures v.1.0
A.16.1.5	Response to information security incidents	ISD.1.16 Security Incident Policy v.1.0 - Hay que
A.16.1.6	Learning from information security incidents	ISD.1.16 Security Incident Policy v.1.0 PRO.010 Security Incident Procedures v.1.0
A.16.1.7	Collection of evidence	ISD.1.16 Security Incident Policy v.1.0 PRO.010 Security Incident Procedures v.1.0
A.17	Information security aspects of business continuity management	
A 17.1	Information security continuity	
A.17.1.1	Planning information security continuity	ISD.1.17 Continuity BCP Scytl ITCP SCYTL v1
A.17.1.2	Implementing information security continuity	BCP SCTYL.V1 ITCP SCYTL v1

A.17.1.3	Verify, review and evaluate information security continuity	BCP SCTYL.V1 ITCP SCYTL v1
A 17.2	Redundancies	
A.17.2.1	Availability of information processing facilities	ISD.1.11 Physical safety and equipment
A.18	Compliance	
A 18.1	Compliance with legal and contractual requirements	
A.18.1.1	Identification of applicable legislation and contractual requirements	ISD.1.18 Conformity with legal requirements
A.18.1.2	Intellectual property rights	ISD.1.18 Conformity with legal requirements
A.18.1.3	Protection of records	ISD.1.18 Conformity with legal requirements
A.18.1.4	Privacy and protection of personally identifiable information	ISD.1.18 Conformity with legal requirements PRO.001 Personal Data Management
A.18.1.5	Regulation of cryptographic controls	ISD.1.18 Conformity with legal requirements
A 18.2	Information security reviews	
A.18.2.1	Independent review of information security	ISD.1.18 Conformity with legal requirements ISD.1.21 Cybersecurity Controls
A.18.2.2	Compliance with security policies and standards	ISD.1.18 Conformity with legal requirements
A.18.2.3	Technical compliance review	ISD.1.18 Conformity with legal requirements SD.1.21 Cybersecurity Controls

Table 2 – Scytl's ISO 27002 documentation available

2.16 Section 4.13.2 Deficiencies in the handling of votes

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.

Figure 32 - Section 4.13.2 Deficiencies in the handling of votes

Assessment: To ensure that Invote does not suffer from vulnerabilities, an independent review of Invote's source code is required. The ability for Scytl to switch voters to votes need to be further explored. A risk analysis needs to be done that assesses how it is likely that Scytl can link the contents of a voice to an individual.

Scytl has always allowed any auditor appointed by the authorities of Åland to review the source code, at any time. Scytl previously shared the protocol specification with the government of Åland, including

the details about how the proofs are implemented. Therefore, this review could have already taken place.

On the other hand, and as mentioned in several sections above, it is not possible to link the content of a vote with the voter who has cast it since the voting system is implementing a verifiable mixing to anonymize the votes and a secret-sharing scheme to protect the private key, which is managed by the Electoral Board (and Scytl is not a member of this board). The same mixing and decryption processes are used in Switzerland and no vulnerabilities that compromise privacy have ever been found (the vulnerabilities found affected only the auditability of the election but never the privacy). As explained before, this risk has always been present and properly mitigated by the cryptographic protocol and with procedural guarantees.

2.17 Section 5.2 Final assessment and recommendations

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.

Figure 33 - Section 5.2 Final assessment and recommendations

The information obtained during the second round of review from Scytl partially affects the preliminary assessment made in the first review round (section 4.13.1). However, the preliminary assessment of deficiencies in the handling of votes (section 4.13.2) remains unchanged after the second round of review and can therefore be regarded as a final assessment. In addition, there will be an assessment regarding implemented security measures as well as a general assessment of the review process.

Scytl never received any assessment or draft report related to the first round. We were approached again in the second round with a document containing a set of questions to respond and complement with related documentation, without knowing whether these questions were used to clarify issues or just because the auditor wanted to obtain more information. Had we known the initial assessment, we would have provided even further clarification to avoid any misinterpretation.

2.18 Section 5.2.1 Revision of section 4.13.1 – Deficiencies in security measures documentation

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.

Figure 34 - Section 5.2.1 Revision of section 4.13.1

Summary: There is no information available to assess whether Scytl has implemented effective security measures for the processing of personal data in connection with the Åland elections. The documentation of the security measures that have been submitted so far is partially substandard given that Scytl is handling personal data in connection with a democratic election.

Recommendation: Wait for treatment before Scytl has corrected the deficiencies in its documentation. In addition, an Åland Government should consider conducting an on-site audit at Scytl to convince itself of the implementation of the security measures.

As stated throughout this report, Scytl's policies are not substandard (see sections 2.4 to 2.13 above) nor do we deal with any special categories of personal data (see sections 2.2 and 2.14 above).

On the one hand, Scytl has implemented effective security measures for the processing of personal data for their employees and, more specifically, for the election in Åland. These include:

- Access control policies for employees.
- Logging and logging controls.
- Security on components.
- Security of mobile devices and teleworking.
- Security of websites, servers and internal networks.
- Deletion of data.
- Secure communication with external parties.
- Physical safety.
- In addition, the security framework is detailed in the ISD.1.5 Security Framework.

The documentation provided is related to Scytl's certification process under ISO 27001, and therefore it is not clear to us how it got assessed as substandard. Maybe the auditor expected additional documents that we did not identify in the requests but the DPA, but this does not mean that the quality of the documentation shared is substandard. All the documentation under ISO 27001 has the same structure: (1) Objective, (2) Scope of solution, (3) Definitions, (4) Responsibilities, (5) Policy, and (6) Development of the policy.

The table in section 2.15 above shows the details for each document and its topic. For obvious reasons, we did not share all the set of documents under the ISO with the auditor since this is not the usual procedure under a personal data audit process (not one for an ISO certification).

When it comes to the statement about "dealing with personal data", it is worth recalling that:

- The system only stores the personal data necessary (IP addresses and voter "pseudonyms") to guarantee that all votes have been cast by eligible voters and that only the appropriate number of remote electronic votes per voter gets counted (i.e. one or zero if they have canceled their electronic vote by casting a paper one).
- This data is never linked to the contents of the vote (i.e. clear text vote), but to the encrypted contents (i.e. cyphertext). Being able to link the encrypted vote to a voter identifier was necessary to prevent multiple voting and to ensure that all electronic remote votes stored in the electronic ballot box had been cast by eligible voters.
- In order to break the link between the encrypted vote and the voter identifier, both technological and procedural guarantees are in place. First, a cryptographic mixing process shuffles the encrypted votes and re-encrypts them, breaking any correlation between the original encrypted votes and the re-encrypted ones. Second, the private key used to decrypt the votes is split into shares and can only be used once a predefined number of members of the Electoral Board (i.e. the threshold) joins and reconstructed it by using their individual shares. The Electoral Board was the only stakeholder who controlled the shares of the keys, and they were, therefore, the only ones who could decrypt the votes. Scytl was not part of the Electoral Board.

2.19 Section 5.2.2 Revision of section 4.13.2 – Shortcomings in the handling of votes

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.

Figure 35 - Section 5.2.2 Revision of section 4.13.2

Assessment: To ensure that Invote does not suffer from vulnerabilities, an independent review of Invote's source code is required. The possibility of Scytl switching voters to votes also needs to be further investigated. A risk analysis needs to be done that assesses how likely it is that Scytl can link the content of a voice to an individual.

As stated before, some vulnerabilities in the system tested in Switzerland were corrected in time for the elections. Besides, not all of them were related to the system used in Åland. A public review could have verified them since the mixing source code is publicly available. The source code review was also available for the other security audit firm contracted by the government of Åland. Throughout the project duration, access to the source code was always possible.

Regarding the possibility of linking voters to votes, the cryptographic measures properly implemented and the procedural guarantees in place (see section 2.18 above) mitigate this risk. Furthermore, no findings related to this point were raised in Switzerland by the experts that participated in the experience. Findings were related to the audit mechanism.

2.20 Section 5.2.3 Assessment of the implementation of the security measures

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

Figure 36 - Section 5.2.3 Assessment of the implementation of the security measures

Assessment: Implementation of the security measures is partly unacceptable.

Recommendation: Implementation of relevant safety measures should be addressed in collaboration with Scytl before treatment is started.

As stated throughout this report, Scytl's policies are not substandard nor do we deal with special categories of personal data.

2.21 Section 5.2.4 General assessment

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.

Figure 37 - Section 5.2.4 General assessment

Assessment: Overall, there seems to be a systematic safety work at Scytl. However, many question marks remain to assess whether Scytl's technical and organizational security measures as a whole can be considered appropriate under Article 32 for the planned treatment.
Recommendation: The question marks should be removed before treatment is started.

We agree that the doubts or questions raised during the assessment should be resolved. However, sufficient information was provided during the audit process to clarify them.

3 Conclusions

In this document, we have provided the necessary clarifications to shed light on some of the inaccuracies in the audit report by the DPA.

In what follows, we provide an overview of the main inaccuracies in the audit report provided by the DPA and responses that could solve them:

- On the use of personal data by the online voting system and its treatment (sections 3.2, 4.1.2, 4.12, in the original report):
    - The system only stores the personal data necessary (IP addresses and voter "pseudonyms") to guarantee that all votes have been cast by eligible voters and that only the appropriate number of remote electronic votes per voter is counted (i.e. one or zero if they have canceled their electronic vote by casting a paper one).
    - This data is never linked to the contents of the vote (i.e. clear text vote), but to the encrypted vote (i.e. cyphertext). Being able to link the encrypted vote to a voter identifier is necessary to prevent multiple voting and to ensure that all electronic remote votes stored in the electronic ballot box had been cast by eligible voters.
    - To break the link between the encrypted vote and the voter identifier, both technological and procedural guarantees are in place. First, a cryptographic mixing process shuffles the encrypted votes and re-encryptes them, breaking any correlation between the original encrypted votes and the re-encrypted ones. Second, the private key used to decrypt the votes is split into shares and could only be used once a predefined number of members of the Electoral Board (i.e. the threshold) joined and reconstructed it by using their individual shares. The Electoral Board was the only stakeholder who controlled the shares of the keys, and they were therefore the only ones who could decrypt the votes. Scytl was not part of the Electoral Board.
- On how the online voting system worked (sections 3.1, 4.1.1, 4.12, 4.13.2 in the original report):
    - The online voting system used in Åland is end-to-end verifiable. It allowed voters to check accurately whether their encrypted vote contained their choices (cast-as-intended verifiability) and whether their ballot had been stored unmodified in the voting server (recorded-as-cast verifiability). Individual verifiability was provided by means of a cast-and-decrypt mechanisms based on a QR code that was shown to the voter after casting their vote, and that could be used (together with a verification app that should be installed in a different device) to verify their vote. Vote coercion was mitigated by allowing voters to cast multiple votes.
    - When it comes to voter identification, we have proved that the authentication mechanism used in the elections in Åland is at least as robust as the existing mechanisms for alternative remote voting channels.

- The vulnerabilities that were identified in a new Swiss remote electronic voting system (sVote) are not completely related to the cryptographic components that used in the voting system in place for the elections in Åland (Invote). Furthermore, the vulnerabilities identified were easy to solve and got implemented ahead of the elections. As a matter of fact, they had already been reviewed and accepted by external researchers ahead of the elections that took place in the State of New South Wales, in Australia. The source code to check the correct implementation is public.

- On Scytl's security policies (sections 4.1.3, 4.2.1., 4.2.2., 4.3, 4.4, 4.5, 4.7, 4.8, 4.9, 4.13.1 in the original report):
  - Scytl has a specific access control policy. This policy is detailed in the ISO 27001 document entitled "ISD 1.9 Access Control to Information Systems" and its implementation is in the document "PRO.007 User Management." Only the members of the IT department assigned to the project have access to the servers for the elections in Åland. Furthermore, access to the servers is done via a bastion host where every action gets logged.
  - Scytl has detailed documents describing how to manage, process and register log information. These documents include the documents entitled "Parsable and good secure logs", as well as the documentation for our immutable logs' solution "Secure Logger". The logging and monitoring are further detailed in a document under the ISO 27001 certification, entitled "ISD.1.12 System Management and Operations."
  - At Scytl, the responsibilities of the role of the Data Protection Officer (DPO) are shared between the members of the Data Protection Committee. The Data Protection Committee consists of one representative from the legal department, one from the IT department, one from the delivery department (projects), one from the product department and one from the security department. The Security Director is the only point of contact of this Committee for Scytl's customers.
  - Scytl has a security policy. This policy was detailed in several documents shared with the DPA, including "ISD.1.11 Physical safety and equipment" and "ISD1.1 SCYTL Groups Security Regulation."
  - Scytl has a policy for restrictions on using mobile devices and remote working (i.e. document "ISD.1.1 Scytl Group Security Regulation").
  - All the documentation shared with the DPA are the standard and mandatory controls that Scytl implements (including on security of websites, servers and internal networks, deletion of data, secure communication with external parties and physical safety). Therefore, these policies are binding for their employees.

Having due consideration to all the issues mentioned in this document, Scytl remains available for further clarification should it be required by any of the project's stakeholders.