

Robert Krimmer · Melanie Volkamer ·
Bernhard Beckert · Ralf Küsters ·
Oksana Kulyk · David Duenas-Cid ·
Mihkel Solvak (Eds.)


LNCS 12455

Electronic Voting

5th International Joint Conference, E-Vote-ID 2020
Bregenz, Austria, October 6–9, 2020
Proceedings



My Vote, My (Personal) Data: Remote Electronic Voting and the General Data Protection Regulation

Adrià Rodríguez-Pérez^{1,2} 

¹ Scyt1 Secure Electronic Voting, S.A., 08008 Barcelona, Spain
adria.rodriguez@scyt1.com

² Universitat Rovira i Virgili, 43002 Tarragona, Spain

Abstract. On 19 September 2019, the Data Protection Authority of the Åland Islands (in Finland) published its findings on the data processing audit for the autonomous region's parliamentary election special internet voting procedure. It claimed that there were faults in the documentation provided by the processor, which in turn meant that the election's integrity could not be guaranteed without further precautions from the government of the Åland Islands. Since the European Union's General Data Protection Regulation (GDPR) entered into force in May 2018, it has set new critical requirements for remote electronic voting projects. Yet, to date, no specific guidance nor research has been conducted on the impact of GDPR on remote electronic voting. Tacking stock of two recent internet voting experiences in the Åland Islands and France, this paper aims at identifying and understanding these new requirements. More specifically, based on these two case studies it analyses four different challenges on the processing of personal data in remote electronic voting under the GDPR: the definitions and categories of personal data processed in online voting projects; the separation of duties between data controllers and data processors; the secure processing of (sensitive) personal data, including the use of anonymisation and pseudonymisation techniques; as well as post-election processing of personal data, and possible limits to (universal) verifiability and public access to personal data.

Keywords: Internet voting · Data protection law · GDPR

1 Introduction

Since the European Union (EU)'s General Data Protection Regulation (GDPR) entered into force in May 2018, it has set new critical requirements for the processing of personal data in remote electronic voting projects. In some countries where internet voting is widely used, both in public as well as in private elections, data protection authorities have adopted or updated their regulations on i-voting. This is the case, for instance, of the Recommendation on the security of e-voting systems by the French *Commission Nationale de l'Informatique et des Libertés* (CNIL). Yet, this case is rather the exception

than the rule. In turn, no specific guidance at the European level has been provided on this matter.

Tacking stock of two recent internet voting experiences in the Åland Islands (an autonomous region in Finland) and France, this paper aims at identifying the nature of these new requirements, to understand how they have been translated into practice, and to comprehend how they have impacted the implementation of i-voting. More specifically, it addresses the four following aspects: (i) the definitions and categories of personal data processed in these two experiences; (ii) the separation of duties between data controllers and data processors; (iii) the secure processing of (sensitive) personal data, including anonymisation and pseudonymisation techniques; and (iv) post-election processing of personal data, including its destruction, as well as possible limits to (universal) verifiability and public access to personal data. To the best of our knowledge, this one is the first academic paper on the topic. Thus, our goal is to identify some critical aspects in the implementation of GDPR's requirements in online voting, rather than to come up with solutions on how to guarantee compliance with its provision.

To do so, we start by providing an overview of the legal framework governing the use of personal data in elections (Sect. 2). First, we analyse the wider, overarching principle of secret suffrage (Sect. 2.1). In the framework of remote electronic voting, it helps us identify the requirement of data minimisation, as well as that of respect with provisions on data protection. We then move to study the main provisions on personal data protection at the European level (Sect. 2.2). More specifically, we study data protection by comparing it to the international right to respect for private life, and then we move to analyse the more recent provisions on European data protection law, with a specific focus on the EU's GDPR, which was adopted in May 2016 and entered into force two years later. This analysis will allow us to argue that the requirements for personal data processing are independent of and complementary to those of secret suffrage. Following (Sect. 3), the actual implementation of the GDPR's provisions in real internet voting projects is studied. We focus on the extent to which the (planned) use of internet voting in the Åland Islands (Sect. 3.1) and France (Sect. 3.2) complied with the provisions of the new EU Regulation. Drawing from these two projects, we have identified the four above-mentioned trends, which we consider specifically relevant when it comes to the processing of personal data in i-voting under the GDPR (Sect. 3.3). After this analysis, the fourth and final section provides the conclusion of the paper, attempts to draw some lessons learned, acknowledges limitations in our study, and outlines potential future research.

2 Beyond Secret Suffrage: European Data Protection Law

2.1 The Right to Vote and Secret Suffrage

Secret suffrage is one of the key principles of the right to free elections. The obligation to guarantee the secrecy of the ballot features in both Article 21(3) of the Universal Declaration on Human Rights (UDHR) as 'secret vote', as well as in Article 25(b) of the International Covenant on Civil and Political Rights (ICCPR) as elections held by 'secret ballot' (International IDEA 2014: 43). In Europe, the right to free elections is enshrined in Article 3 of the Protocol (no. 1) to the Convention for the Protection of

Human Rights and Fundamental Freedoms (ECHR). Article 3 of the Protocol explicitly recognises that democratic elections are to be held by secret vote or by equivalent free voting procedures. In this sense, “the secrecy of the vote is [considered] an aspect of free suffrage, which aims to shield voters from any pressure that might result from the knowledge of his [sic] choice by third parties and, in fine, to ensure the honesty and sincerity of the vote” (Lécuyer 2014: 76).

As part of secret suffrage, the Council of Europe’s recently updated Recommendation CM/Rec(2017)5 on standards for e-voting specifies that “[p]rovisions on data protection shall be respected” (Council of Europe, 2017a: 20). More specifically, it states that “[t]he e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election” (2017a: 20), and that “[t]he e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data” (Council of Europe 2017a: 21). The Guidelines on implementation of the Recommendation also state that “[t]he legal framework should include procedures for the process of data destruction, in particular to align processing, storing and destruction of the data (and equipment) of voting technology with the personal data protection legislation” (Council of Europe 2017c: 28.d), and that “printing of voter identification data such as polling cards should be reviewed to ensure security of sensitive data” (Council of Europe 2017c: 48.a).

These standards are related to the requirement of ‘data minimisation’, which refers to “data necessary for fulfilling legal requirements of the voting process” (Council of Europe 2017b: 65). Interestingly enough, this provision of the Recommendation’s Explanatory Memorandum states that it is “[t]he electoral management body in charge of organising e-voting [who] identifies such data and should be able to explain what are the underlying legal provisions and considerations that render them necessary” (Council of Europe 2017b: 65). The Explanatory Memorandum concludes that “data minimisation aims at ensuring data protection and is part of vote secrecy” (Council of Europe 2017b: 65). However, and as we will see now, we should consider personal data protection requirements as protecting a distinct, independent legal asset.

2.2 The Rights to Respect for Private Life and to Personal Data Protection

From the Right to Respect for Private Life to the Right to Personal Data Protection.

The right to privacy (article 12 of the UDHR and art. 17 of the ICCPR), also known as the right to respect for private life (article 8 of the ECHR), provides that “everyone has the right to respect for his or her private and family life, home and correspondence.” Interference with this right by a public authority is prohibited, except where the interference is in accordance with the law, pursues important and legitimate public interests and is necessary in a democratic society (EU Agency for Fundamental Rights and Council of Europe 2018: 18). The development of computers and the Internet presented new risks to the right to respect for private life. In response to the need for specific rules governing the collection and use of personal information, a new concept of privacy emerged, known as ‘informational privacy’ or the ‘right to informational self-determination’ (EU Agency for Fundamental Rights and Council of Europe 2018: 18).

Data protection in Europe began in the seventies at the national level, and afterwards, data protection instruments were established at the European level: first, in the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), adopted in 1981; and then in the European Union's Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data. Over the years, data protection developed into a distinctive value that is not subsumed by the right to respect for private life (EU Agency for Fundamental Rights and Council of Europe 2018: 19).

While both rights strive to protect similar values (i.e., the autonomy and human dignity of individuals) the two differ in their formulation and scope: while the right to respect for private life consists of a general prohibition on interference, the protection of personal data is viewed as a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed. The right to personal data protection thus comes into play whenever personal data are processed. Therefore, it is broader than the right to respect for private life. Any processing operation of personal data is subject to appropriate protection. Data protection concerns all kinds of personal data and data processing, irrespective of the relationship and impact on privacy. Processing of personal data may infringe on the right to private life. However, it is not necessary to demonstrate an infringement on private life for data protection rules to be triggered (EU Agency for Fundamental Rights and Council of Europe 2018: 20). In our opinion, the same could be argued for personal data protection and secret suffrage: the former cannot be subsumed by this latter principle.

Data Protection Regulations in the EU. From 1995 until May 2018, the principal EU legal instrument on data protection was the Directive 95/46/EC (EU Agency for Fundamental Rights and Council of Europe 2018: 29). In 2009, debates on the need to modernise EU data protection rules began, with the Commission launching a public consultation about the future legal framework for the fundamental right to personal data protection. The proposal for the regulation was published by the Commission in January 2012, starting a long legislative process of negotiations between the European Parliament and the Council of the EU. After adoption, the GDPR provided for a two-year transition period. It became fully applicable on 25 May 2018, when the Directive 95/46/EC was repealed (EU Agency for Fundamental Rights and Council of Europe 2018: 30).

The adoption of GDPR in 2016 modernised EU data protection legislation, making it fit for protecting fundamental rights in the context of the digital age's economic and social challenges. The GDPR preserves and develops the core principles and rights of the data subject provided for in the Directive 95/46/EC. In addition, it has introduced new obligations requiring organisations to implement data protection by design and default, to appoint a Data Protection Officer in certain circumstances, to comply with a new right to data portability, and to comply with the principle of accountability (EU Agency for Fundamental Rights and Council of Europe 2018: 30). Furthermore, under EU law regulations are directly applicable and there is no need for national implementation. Therefore, the GDPR provides for a single set of data protection rules to the whole EU. Finally, the regulation has comprehensive rules on territorial scope: it applies both to businesses established in the UE, as well as to controllers and processors not established

in the EU that offer goods or services to data subjects in the EU or monitor their behaviour (EU Agency for Fundamental Rights and Council of Europe 2018: 31).

Ahead of the elections to the European Parliament of 2019, the European Commission released a guidance document on the application of the Union’s data protection law in the electoral context. The goal of the document was to “provide clarity to the actors involved in election processes – such as national electoral authorities, political parties, data brokers and analysts [and] highlight the data protection obligations of relevance for elections” (European Commission 2018: 2). Specifically, the document addressed key obligations for the various actors, the role as data controller or data processor, principles, lawfulness of processing and special conditions for the processing sensitive data, security and accuracy of personal data, and data protection impact assessment, to name just a few examples. Yet, it is worth noticing that the guidance document does not make specific reference to the use of (remote) electronic voting technologies.

3 Remote Electronic Voting Experiences Under the GDPR

3.1 The Parliamentary Elections in the Åland Islands, Finland

In 2014, the Government of the Åland Islands started studying how to amend the Election Act for Åland. Among other issues, they wanted to know whether internet voting could be introduced for the elections to their parliament. Work on a new Election Act for Åland started in 2017. A draft law was approved by the Government in 2018, and the Parliament passed it in January 2019. The law was then signed by the President of Finland by mid-May. Thus, the Election Act for Åland, together with the Act on the Autonomy of Åland, provide the basic electoral framework for the autonomous region. The law provides that “[a]dvance voting via the internet shall be organised in parliamentary elections if a reliable system for electronic voting via the internet is available” (Election Act for Åland, section 78).

The Government of Åland started to work on the procurement of an internet voting system for the 2019 parliamentary elections in 2018. In March, they published a Request for Information. They received answers from five different providers, but they realised that only two providers would meet the requirements of their tender. The tender was published in October 2018 and two offers were received (from the two vendors that they expected that would bid). Scytl Secure Electronic Voting, S.A. (Scytl) was awarded the project. The contract with Scytl was signed in early January 2019.

On 19 June, the Åland Data Protection Authority (DPA) decided to conduct a data protection audit for the 2019 Election Special Internet Voting Procedure (2019a)¹. The goal was to “identify potential risks with the treatment before the election would take place” (DPA 2019c). The audit was conducted by TechLaw Sweden AB (TechLaw). While the object of the audit was the Government of the Åland Islands’ treatment of i-voters’ personal data, “Scytl [the processor] got the questions asked directly from the Data Inspectorate [as] a practical solution to save time” (DPA 2019c). The report was concluded on 12 September and the findings were published on the 19 of September, together with another report by the DPA. The DPA criticised, “inter alia, the lack of clarity

¹ All translations from the original reports in Swedish by the author, using an online tool.

of contracts between the Government, ÅDA² and ScytI, as well as, the issue regarding the personal data of i-voters” (Krimmer et al. 2019: 11). The report also identified faults in the documentation provided by the processor (ScytI), which in turn meant that the election’s integrity could not be guaranteed without further precautions from the government of the Åland Islands (DPA 2019b). On 13 December, the DPA also published a report with comments from ScytI. The purpose of the comment from ScytI was “to find out any misunderstandings that may have arisen regarding their security measures by the reporter employed by the Data Inspectorate” (DPA 2019b).

3.2 The Consular Elections in France

Internet voting in France dates back to 2003, with the passing of the first law allowing the use of internet voting for the elections to the Assembly of French Citizens Abroad (Sénat 2014: 38)³. Subsequently, the Ministry of Foreign and European Affairs (MEAE) carried out three pilot projects during the 2003, 2006, and 2009 elections (OSCE/ODIHR 2012b: 9). Nowadays, internet voting is foreseen as an additional voting channel for French voters abroad. They can cast an i-vote for the elections to the National Assembly (the country’s directly elected lower house, with 577 seats) and for the election of the Consular Advisers and Delegates. For the elections to the National Assembly, a constitutional amendment of 2008 introduced 11 seats to be elected by voters residing abroad (OSCE/ODIHR 2012a: 3). In 2012, voters had the possibility to vote online for these seats (Sénat 2014: 37) for the first time (OSCE 2012a: 1). However, in 2017 this possibility was halted due to “concerns of foreign cyber threats as well as over certain technical issues” (OSCE/ODIHR 2017c: 6). On their side, Consular Advisers and Delegates are based at each embassy with a consular district and at each consular post. They are elected for a six-year period during the month of May, their first elections taking place in 2014 (Sénat 2014: 37). The next elections were scheduled on May 2020. Yet, the MEAE decided to post-pone these elections due to the Covid-19 pandemic. ScytI was also the technology provider for these two elections, having signed a contract with the MEAE for a four-year period in May 2016 (Sénat 2018: 38).

In France, and since internet voting requires the set-up of data files with the citizens enrolled on consular lists (Sénat 2014: 43; 2018: 29), this technology is under the legal supervision of the CNIL. In 2010, the CNIL adopted a Recommendation on the security of e-voting systems (CNIL 2010). The Recommendation provides “general guidelines regarding minimal privacy, secrecy and security requirements for any internet voting” (OSCE/ODIHR 2012b: 12). The CNIL prescribes both ‘physical’ measures (such as access controls to the servers or rules for the clearance of authorized employees), as well as software-related ones (i.e., firewalls) (Sénat 2014: 37). The Recommendation was updated in 2019, precisely to take stock of the new requirements introduced by the GDPR after it entered into force (CNIL 2019b). The goal of the update was for it to apply to future developments in internet voting, “with a view to better respect the principles

² According to Krimmer et al. (2019: 9): “In Åland, it is not the government itself, but a particular agency, ÅDA, which is acting as the procurement agent being in charge of the procurement process with the Government as the “real” customer”.

³ All translations from the original reports in French by the author.

of personal data protection, and to inform data controllers on their choice for an online voting system” (CNIL 2019a). Furthermore, a General Security Regulatory Framework (RGS) is established by the *Agence nationale de la sécurité des systèmes d’information* (ANSSI) to regulate minimal requirements on “electronic certificates, encryption levels, and authentication mechanisms” (OSCE/ODIHR 2012b: 12).

3.3 Comparing Remote Electronic Elections Under GDPR

In what follows, we provide an overview of the most relevant issues in these two experiences concerning the application of the GDPR. More specifically, we will focus on (i) the definitions and categories of personal data processed; (ii) the separation of duties between data controllers and data processors; (iii) the secure processing of (sensitive) personal data, including the use of anonymisation and pseudonymisation techniques; and (iv) the post-election processing of personal data, including its destruction, as well as possible limits to (universal) verifiability and public access to personal data.

This list of issues is not exhaustive, since these aspects have been identified as relevant in the two experiences studied here. It is likely that additional issues could be raised in different cases, or after the implementation of these two specific projects.

Definition and Categories of Personal Data. According to EU law, data are personal if they relate to an identified or identifiable person, the ‘data subject’ (EU Agency for Fundamental Rights and Council of Europe 2018: 83). The GDPR defines personal data as information relating to an identified or identifiable natural person (GDPR, art. 4.1). Any kind of information can be personal data provided that it relates to an identified and identifiable person⁴. Personal data covers information pertaining to the private life of a person, as well as information about their public life (EU Agency for Fundamental Rights and Council of Europe 2018: 86).

The GDPR stipulates that a natural person is identifiable when he or she “can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person” (GDPR, art. 4.1). Yet, according to the Article 29 Data Protection Working Party (Article 29 Working Party), it is also “possible to categorise [a] person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual’s contact point (a computer) no longer requires the disclosure of his or her identity in the narrow sense” (2007: 15). Identification, thus, requires elements which describe a person in such a way that he or she is distinguishable from all other persons and recognisable as an individual (EU Agency for Fundamental Rights and Council of Europe 2018: 89). Establishing the identity of a person may need additional attributes to ensure that a person is not mistaken for someone else. Sometimes, direct and indirect attributes may have to be combined to identify the individual to whom the information relates. Date and place of birth are often used. In addition, personalised numbers have been introduced in some countries to

⁴ For the applicability of European data protection law there is no need for actual identification of the data subject: it is sufficient that the person concerned is identifiable.

better distinguish between citizens. Biometric data, such as fingerprints, digital photos or iris scans, location data and online attributes are increasingly used to identify persons in the technological age (EU Agency for Fundamental Rights and Council of Europe 2018: 90).

Personal Data About Candidates. Based on the above, it is clear that data about candidates is personal data and thus falls under the scope of the right to personal data protection and of the GDPR. It goes without saying that candidates are to be described in such a way that they are distinguishable from all other persons and recognisable as individuals. How was personal data about candidates processed in these two experiences? In Åland, the online voting process was similar to the paper-based one (Krimmer et al. 2019: 11), where voters do not mark or select a candidate in the ballot but write their number on a blank ballot paper. Likewise, in the Åland's voting platform, voters were not "able to select a candidate by clicking on it in the list of candidates displayed. [Instead, a] voter will need to insert the number of a candidate, exactly like it is done when a voter cast a vote on paper" (Krimmer et al. 2019: 11). On the other hand, in France, the Election Management System service used by the election managers to configure the election (GUES), includes personal data about each candidate. This data includes their name, surname, sex, birth date, phone, e-mail, etc. Similar information is also processed for candidates' substitutes.

Authentication Data. Authentication means proving that a certain person possesses a certain identity and/or is authorized to carry out certain activities (EU Agency for Fundamental Rights and Council of Europe 2018: 83). This is a procedure by which a person is able to prove that they possess a certain identity and/or is authorised to do certain things, such as enter a security area, withdraw money from a banking account or, as in this case: cast an i-vote. Authentication can be achieved by comparing biometric data, such as a photo or fingerprints in a passport, with the data of the person presenting themselves. However, this kind of authentication can only be conducted face-to-face (i.e., when voters cast a paper ballot in polling stations). An alternative for the remote setting is to ask for information which should be known only to the person with a certain identity or authorisation, such as a personal identification number (PIN) or a password. In addition to these, electronic signatures are an instrument especially capable of identifying and authenticating a person in electronic communications (EU Agency for Fundamental Rights and Council of Europe 2018: 95).

Voter authentication was similar in both the Åland Islands and in France. In Åland, the voters had to go to a website provided by ÅDA and authenticate via BankID (TechLaw 2019: 9). Upon successful authentication, the voter received a KeyStore with the election public key (to encrypt the vote) and their voter private key (to digitally sign the encrypted vote). The voter is identified internally by the voting platform using a randomly generated pseudonymous (VoterID) "that is used to ensure that a vote has been cast by an eligible voter and that no voter has voted twice" (Scytl 2019: 24). According to Scytl (2019: 24), "under no circumstances can Scytl correlate this voter identifier with the real identity of the voter".

In addition to the vote and the voterID, Scytl's voting system also stores the voters' IP addresses (TechLaw 2019: 8). In a 2011 ruling, the Court of Justice of the EU (CJEU)

held that users' IP addresses "are protected personal data because they allow those users to be precisely identified" (CJEU 2011: para. 51). The CJEU has also considered that a dynamic IP address, which an online media services provider registers when a person accesses a website that the provider has made accessible to the public, constitutes personal data where only a third party (i.e., the internet service provider) has the additional data necessary to identify the person (EU Agency for Fundamental Rights and Council of Europe 2018: 91). According to Scytl (2019: 24), it is not possible to link the vote or the voter with the IP because they have "no information to correlate IP addresses with the real identity of the voter".

Encrypted and Digitally Signed Electronic Ballots. There are special categories of data, so-called 'sensitive data', which require enhanced protection and, therefore, are subject to a special legal regime (EU Agency for Fundamental Rights and Council of Europe 2018: 83). These are special categories of personal data which, by their nature, may pose a risk to the data subjects when processed and need enhanced protection. Such data are subject to a prohibition principle and there are a limited number of conditions under which such processing is lawful (EU Agency for Fundamental Rights and Council of Europe 2018: 96). Within the framework of the GDPR, the following categories are considered sensitive data: personal data revealing racial or ethnic origin; political opinions, religious or other beliefs, including philosophical beliefs; trade union membership; genetic data and biometric data processed for the purpose of identifying a person; and, personal data concerning health, sexual life or sexual orientation. Since digital ballots reveal political opinions (they contain the political preferences of voters), they must be considered sensitive data. As a matter of fact, research conducted by Duenas-Cid et al. (2020) concludes that it was precisely the processing of political opinions as a special category of personal data that motivated an audit in the Åland Islands.

In both the Åland Islands (Scytl 2019: 11) and in France, votes are encrypted and sealed in encrypted envelopes (directly on the voter's computers). The encrypted vote is then digitally signed (also in the voting device). Since votes are digitally signed, only the votes cast (and signed) by eligible voters are verified and stored in the voting server (i.e., the digital ballot box) (Scytl 2019: 38). In the case of Åland, the system also provided individual verifiability (cast-as-intended and recorded-as-cast verifiability). In practice, it means that after casting their vote, voters could log into the voting service to check that their vote had reached the voting server unaltered (TechLaw 2019: 8).

Data processing: The Role of Data Controllers and Data Processors. 'Data processing' concerns any operation performed on personal data. According to the GDPR, "processing of personal data [...] shall mean any operation [...] such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (art. 4.2).

Whoever determines the means and purposes of processing the personal data of others is a controller under data protection law. If several persons take this decision together, they may be joint controllers. A 'processor' is a natural or legal person that processes the personal data on behalf of a controller. If a processor determines the means

and purposes of data processing itself, they become a controller. Any person to whom personal data are disclosed is a ‘recipient’ (EU Agency for Fundamental Rights and Council of Europe 2018: 101). Any person other than the data subject, the controller, the processor and persons who are authorised to process personal data under the direct authority of the controller or processor is considered a ‘third-party’.

The most important consequence of being a controller or a processor is a legal responsibility for complying with the respective obligations under data protection law. In the private sector, this is usually a natural or legal person. In the public sector, it is usually an authority. There is a significant distinction between a data controller and a data processor: the former is the natural or legal person who determines the purposes and the means of processing, while the latter is the natural or legal person who processes the data on behalf of the controller, following strict instructions. In principle, it is the data controller that must exercise control over the processing and who has responsibility for this, including legal liability (EU Agency for Fundamental Rights and Council of Europe 2018: 101). Yet, processors also have an obligation to comply with many of the requirements which apply to controllers⁵. Whether a person has the capacity to decide and determine the purpose and means of processing will depend on the factual elements or circumstances of the case.

As has been already seen, according to the Council of Europe’s Recommendation it is “[t]he electoral management body in charge of organising e-voting [who] identifies such data and should be able to explain what are the underlying legal provisions and considerations that render them necessary” (Council of Europe 2017b: 65) In a similar vein, the GDPR clearly states that the processor may only process personal data on instructions from the controller, unless the EU or Member State law requires the processor to do so (art. 29). According to the GDPR, if the power to determine the means of processing is delegated to a processor, the controller must nonetheless be able to exercise an appropriate degree of control over the processor’s decisions regarding the means of processing. Overall responsibility lies with the controller, who must supervise the processor to ensure that their decisions comply with data protection law and their instructions (EU Agency for Fundamental Rights and Council of Europe 2018: 108).

For the sake of clarity and transparency, the details of the relationship between a controller and a processor must be recorded in a written contract (GDPR, art. 28.3 and .9). The contract between the controller and the processor is an essential element of their relationship, and is a legal requirement (GDPR, art. 28.3). It must include, in particular, the subject matter, nature, purpose and duration of the processing, the type of personal data and the categories of data subjects. It should also stipulate the controller’s and the processor’s obligations and rights, such as requirements regarding confidentiality and security. Having no such contract is an infringement of the controller’s obligation to provide written documentation of mutual responsibilities, and could lead to sanctions (EU Agency for Fundamental Rights and Council of Europe 2018: 109). Yet, in the

⁵ Under the GDPR, “processors must maintain a record of all categories of processing activities to demonstrate compliance with their obligations under the regulation” (art. 30.2). Processors are also required to implement appropriate technical and organisational measures to ensure the security of processing (art. 32), to appoint a Data Protection Officer (DPO) in certain situations (art. 37), and to notify data breaches to the controller (art. 33.2).

case of the Åland Islands the DPA criticized, precisely, “the lack of clarity of contracts between the Government, ÅDA and Scytl” (Krimmer et al. 2019: 11). In France, the CNIL’s updated Recommendation specifically provides that “the processing of personal data, including the voting systems, must in principle be subject to a data protection impact assessment (PIA) when meet at least two of [several] criteria”. Among these, this project seems to include, indeed, at least two of these criteria, i.e.: processing of sensitive data (i.e., political opinions) and large-scale processing of personal data. Thus, such an assessment is required in internet voting in France.

Anonymisation, Pseudonymisation and (Sensitive) Personal Data. Data are anonymised if they no longer relate to an identified or identifiable individual (EU Agency for Fundamental Rights and Council of Europe 2018: 83). Pseudonymisation is a measure by which personal data cannot be attributed to the data subject without additional information, which is kept separately. The ‘key’ that enables re-identification of the data subjects must be kept separate and secure. Data that have undergone a pseudonymisation process remains personal data (EU Agency for Fundamental Rights and Council of Europe 2018: 83). The principles and rules of data protection do not apply to anonymised information. However, they do apply to pseudonymised data (EU Agency for Fundamental Rights and Council of Europe 2018: 83).

The process of anonymising data means that all identifying elements are eliminated from a set of personal data so that the data subject is no longer identifiable (GDPR, Recital 26). In its Opinion 05/2014, the Article 29 Working Party analysed the effectiveness and limits of different anonymisation techniques. It acknowledged the potential value of such techniques, but underlined that certain techniques do not necessarily work in all cases. To find the optimal solution in a given situation, the appropriate process of anonymisation should be decided on a case-by-case basis. Irrespective of the technique used, identification must be prevented, irreversibly. This means that for data to be anonymised, no element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned (GDPR, Recital 26). The risks of re-identification can be assessed by taking into account “the time, effort or resources needed in light of the nature of the data, the context of their use, the available re-identification technologies and related costs” (EU Agency for Fundamental Rights and Council of Europe 2018: 94). When data have been successfully anonymised, they are no longer personal data and data protection legislation no longer applies. On the other hand, pseudonymisation means that certain attributes (such as name, date of birth, sex, address, or other elements that could lead to identification) are replaced by pseudonym. EU law defined ‘pseudonymisation’ as ‘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’ (GDPR, art. 4.5). Contrary to anonymised data, pseudonymised data are still personal data and are therefore subject to data protection legislation. Although pseudonymisation can reduce security risks to the data subjects, it is not exempt from the scope of the GDPR (EU Agency for Fundamental Rights and Council of Europe 2018: 94). The GDPR recognises various uses of pseudonymisation as an appropriate technical measure for enhancing data protection,

and is specifically mentioned for the design and security of its data processing (GDPR, art. 25.1). It is also an appropriate safeguard that could be used to process personal data for purposes other than for which they were initially collected.

Based on these provisions, it is clear that both anonymisation and pseudonymisation techniques were used in these two projects. However, most of the time the data processed is pseudonymised, not anonymised. Since it is always possible to relate the encrypted data to a pseudonymous, which in turn can be related to the actual voter identity⁶, it is difficult to argue that no element has been left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned⁷. In Åland, and since multiple voting is supported (Election Act for Åland, Section 61), it is necessary to keep the link between the encrypted vote and the VoterID to cleanse those online votes cast by voters who have cast more than one i-vote, as well as those who have also cast a postal vote or an advanced one in polling stations. In France, it is necessary to prevent i-voters from casting a paper vote in polling stations on election day⁸. In order to prevent a voter from casting a second vote, the voter rolls need to be updated. More specifically, at the end of the internet voting period, a mark is included by the side of the name of those voters who have already voted, i.e.: a list of voters having voted (*liste d'émargement*) is generated. The main implication here is that pseudonymous data remain personal data and must be processed as such.

Yet, it is also possible to talk about anonymised data. In the two projects we can find “both technological and procedural guarantees” (Scytl 2019: 41) in place to break the link between the vote and the voter’s pseudonymous identifier (VoterID). In the case of Åland, during the counting phase a mix-net removes the connection between the identity of the voter and their vote (TechLaw 2019: 8). According to Scytl (2019: 12), this “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”. Once mixed, it is no longer possible to link a vote with the identity of the voter who has cast it. In France, on the other hand, homomorphic tallying is used. In homomorphic tallying, the different options (whether selected or not) are encrypted separately, aggregated, and then decrypted anonymously. When the voter issues their vote, the voting client generates as many cyphertexts as possible options. Therefore, the encrypted vote is represented as an array of as many individual ciphertexts as possible voting options there are within the ballot. During the counting phase, the digital ballot box is exported from the online component of the voting system and imported in the offline one. In the offline environment, all the ciphertexts from all the votes corresponding to the same voting options are aggregated (multiplied), which allows for the computation of a unique aggregated cyphertext for each option. In both cases, the private key used for decryption is protected by a cryptographic secret-sharing scheme

⁶ Which is necessary to “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” (Scytl 2019: 38).

⁷ Recital 26 of the GDPR explicitly includes a scenario where it is foreseeable that further data recipients, other than the immediate data user, may attempt to identify the individuals (EU Agency for Fundamental Rights and Council of Europe 2018: 91).

⁸ Contrary to good practice (Council of Europe 2017c: 9.b), in France once a voter has cast an i-vote, they cannot cast a second vote in person to cancel it.

(Shamir) that requires the collaboration of several members of the electoral commission to reconstruct the key before decryption. Thus, to decrypt these results, it is required that a minimum number of their members meet to reconstruct the election private key: i.e., three out of five persons in Åland (Election Act for Åland, Section 61) and four out of the eight members of the *Bureau de vote électronique* (BVE) in France (*Code électoral*, R177-5).

Post-election: The Destruction of Data, Universal Verifiability and Public Access to Personal Data. The CNIL’s Recommendation (2019a) states that all supporting files of an election (such as copies of the source and executable codes of the programs and the underlying system, voting materials, signature files, results’ files, backups) must be kept under seal until the channels and deadlines for litigation are exhausted. This conservation must be ensured under the supervision of the electoral commission under conditions guaranteeing the secrecy of the vote. Obligation must be made to the service provider, if necessary, to transfer all of these media to the person or to the third party named to ensure the conservation of these media. When no contentious action has been taken to exhaust the time limits for appeal, these documents must be destroyed under the supervision of the BVE. This requirement is not new, and already in 2012 various audits were conducted on data destruction in the context of the parliamentary elections (OSCE/ODIHR 2012bb: 13). Along these lines, the Council of Europe’s Recommendation also provides, in its Explanatory Memorandum, that “[t]he duration of processing, storing etc. [of personal data] also depends on legal requirements, namely those related to appeals”. While these measures may be necessary to ensure the preservation of data protection in the long term, they may prevent the election data from being audited or universally verified⁹. Notwithstanding, the Election Act for Åland (Section 99) requires that “after confirming the result of the election, the ballot papers and a copy of the combined list of candidates or a copy of a list of presidential candidates is placed in a container, which shall be sealed as is laid down by the Ministry of Justice. These are to be kept until the next corresponding elections have been conducted”¹⁰.

Overall, there is a growing realisation of the importance of government transparency for the functioning of a democratic society (EU Agency for Fundamental Rights and Council of Europe 2018: 62). The right to receive information, which forms part of freedom of expression, may come into conflict with the right to data protection if access to documents would reveal other’s personal data. Art. 86 of the GDPR clearly provides that personal data in official documents held by public authorities and bodies may be disclosed by the authority or body concerned in accordance with EU or Member State’s law to reconcile public access to official documents with the right to data protection (EU Agency for Fundamental Rights and Council of Europe 2018: 63). Balancing between data protection and access to documents requires a detailed, case-by-case analysis. Neither right can automatically overrule the other. The CJEU has had the chance to interpret the right to access to documents containing personal data in two cases (EU Agency for

⁹ Universal verifiability refers to “tools which allow any interested person to verify that votes are counted as recorded” (Council of Europe 2017b: 56).

¹⁰ That is so even if an “appeal shall be sent to a competent Provincial Administrative Court within 14 days from the confirmation of the election results” (Election Act for Åland, Section 102).

Fundamental Rights and Council of Europe 2018: 65). According to these judgements, interference with the right to data protection in the context of access to documents needs a specific and justified reason. Furthermore, according to the principle of storage limitation, data must be kept ‘in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed’ (GDPR, art. 5.1.e). For internet voting, it seems advisable that this information is kept at least until the next election has taken place (and not, as it is provided in the CNIL’s recommendation, until the channels and deadlines for litigation are exhausted). Consequently, data would have to be erased or anonymised if a controller wanted to store them after they were no longer needed and no longer served their initial purpose (EU Agency for Fundamental Rights and Council of Europe 2018: 63).

4 Conclusion

The entry into force of the EU’s GDPR has set new requirements for the implementation of internet voting in Europe. Yet, no general guidance has yet been provided on how it impacts this kind of projects specifically. In this context, we have aimed at identifying some critical aspects in the implementation of GDPR’s requirements in online voting, to understand how they have been translated into practice, and to comprehend how they have impacted the implementation of i-voting projects.

Two sorts of conclusions can be inferred from this research. First, the requirements for personal data processing in remote electronic voting projects are independent of secret suffrage and cannot be subsumed by this latter principle. Personal data protection is broader than the principle of secret suffrage since any processing of personal data is subject to appropriate protection. Thus, data that may not fall under the scope of secret suffrage, such as personal data about candidates, is also covered by the GDPR. Second, our account of the internet voting experiences in the Åland Islands and in France has allowed us to identify some critical aspects related to the GDPR in the implementation of internet voting projects, namely: the categories of personal data processed (both about voters and candidates), as well as the processing of special categories of personal data (i.e., the votes, which are personal data that reveal political opinions); aspects related to the role played by data controllers (normally, electoral authorities) and processors (usually, technology vendors and services’ providers); the use of pseudonymisation techniques for the processing of ‘sensitive data’; and, the post-election processing of personal data, including its destruction, as well as possible limits to (universal) verifiability and public access to personal data. As we have seen, all these aspects could benefit from more guidance, be it by the national regulator or at the wider EU-level.

Acknowledgments. This work has received funding from the European Commission under the auspices of PROMETHEUS Project, Horizon 2020 Research and Innovation action (Grant Agreement No. 780701).

References

Act on the Autonomy of Åland (2010)

- Åland Data Protection Authority: DNR T1-2019 (2019a). <https://www.di.ax/anslagstavla/dnr-t1-2019>. Accessed 03 Aug 2020
- Åland Data Protection Authority: Resultat och beslut av den beslutade Dataskyddstillsynen gällande personuppgiftsbehandling i Lagtingsvalet, särskilt fokus I-valet Dnr T1-2019 (2019b). <https://www.di.ax/anslagstavla/dnr-t5-2019>. Accessed 03 Aug 2020
- Åland Data Protection Authority: Rapport om Säkerhetsåtgärder i E-valet samt svar från Scytl (2019c). <https://www.di.ax/anslagstavla/rapport-om-sakerhetsatgarder-e-valet-samt-svar-fran-scytl>. Accessed 03 Aug 2020
- Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data (2007). <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf>. Accessed 03 Aug 2020
- Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 03 Aug 2020
- Court of Justice of the EU: Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (2011)
- CNIL: Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique (2010). <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023124205&categorieLien=id>. Accessed 03 Aug 2020
- CNIL: Sécurité des systèmes de vote par internet: la CNIL actualise sa recommandation de 2010 (2019a). <https://www.cnil.fr/fr/secure-des-systemes-de-vote-par-internet-la-cnil-actualise-sa-recommandation-de-2010>. Accessed 03 Aug 2020
- CNIL: Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet (2019b). <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038661239>. Accessed 03 Aug 2020
- Code électoral, France (2019)
- Council of Europe: Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (2017a). https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f. Accessed 03 Aug 2020
- Council of Europe: Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (2017b). https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726c0b. Accessed 03 Aug 2020
- Council of Europe: Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting (2017c). https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168071bc84. Accessed 03 Aug 2020
- Duenas-Cid, D., Krivososova, I., Serrano, R., Freire, M., Krimmer, R.: Tripped at the finish line: the Åland Islands internet voting project. In: Krimmer, R., et al. (eds.) Electronic Voting. Fifth International Joint Conference, E-Vote-ID 2020. Springer, Cham (2020)
- Election Act for Åland (2019)
- EU Agency for Fundamental Rights and Council of Europe: Handbook on European data protection law - 2018 edition (2018). https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Accessed 03 Aug 2020
- European Commission: Free and Fair elections. Guidance Document. Commission guidance on the application of Union data protection law in the electoral context (2018). https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf. Accessed 03 Aug 2020
- International Covenant on Civil and Political Rights (1966)

- International IDEA: International Obligations for Elections. Guidelines for Legal Frameworks (2014). <https://www.idea.int/sites/default/files/publications/international-obligations-for-elections.pdf>. Accessed 03 Aug 2020
- Krimmer, R., Duenas-Cid, D., Krivososova, I., Serrano, R., Freire, M., Wrede, C.: Nordic Pioneers: facing the first use of Internet Voting in the Åland Islands (Parliamentary Elections 2019) (2019). <https://doi.org/10.31235/osf.io/5zr2e>. Accessed 03 Aug 2020
- Lécuyer, Y.: Le droit a des élections libres. Council of Europe, Strasbourg (2014)
- OSCE/ODIHR: Republic of France Parliamentary Elections, 10 and 17 June 2012. Needs Assessment Mission Report (2012a). <https://www.osce.org/files/f/documents/7/5/90763.pdf>. Accessed 03 Aug 2020
- OSCE/ODIHR: Republic of France Parliamentary Elections, 10 and 17 June 2012. Election Assessment Mission Final Report (2012b). <https://www.osce.org/files/f/documents/7/7/93621.pdf>. Accessed 03 Aug 2020
- OSCE/ODIHR: France Presidential and Parliamentary Elections, 2017. Needs Assessment Mission Report (2017c). <https://www.osce.org/files/f/documents/0/8/311081.pdf>. Accessed 03 Aug 2020
- Protocol (no. 1) to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, ECHR) (1952)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) (2016)
- Sénat: Rapport d'information fait au nom de la commission de lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le vote électronique (2014). <https://www.senat.fr/rap/r13-445/r13-4451.pdf>. Accessed 03 Aug 2020
- Sénat: Rapport d'information fait au nom de la commission de lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le vote électronique (2018). <http://www.senat.fr/rap/r18-073/r18-0731.pdf>. Accessed 03 Aug 2020
- Scytl Secure Electronic Voting, S.A.: Åland's I-voting Project. Clarification of the Audit Report by the Åland Data Protection Authority (2019). https://www.di.ax/sites/default/files/attachment/pinboard-message/data_protection_audit_clarifications_v3.0.pdf. Accessed 03 Aug 2020
- TechLaw Sweden AB: Granskning av säkerhetsåtgärder hos Scytl (2019). https://www.di.ax/sites/default/files/attachment/pinboard-message/rapport-aland-scytl-190916_0.pdf. Accessed 03 Aug 2020
- Universal Declaration on Human Rights (1948)