Deliberation 2019-053 of April 25, 2019 National Commission for Computing and Liberties Nature of the deliberation: Recommendation Legal status: In force Date of publication on Légifrance: Saturday June 22, 2019 Deliberation No. 2019-053 of April 25, 2019 adopting a recommendation relating to the security of electronic postal voting systems, in particular via the Internet The National Commission for Data Processing and Liberties; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to the automatic processing of personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , and repealing directive 95/46/EC; Having regard to the electoral code; Having regard to law n° 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms, no in particular its article 11-I-2°-a bis); Having regard to decree n° 2005-1309 of October 20, 2005 as amended, taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; After having heard Mrs Dominique CASTERA, commissioner, in her report, and Mrs Nacima BELKACEM, government commissioner, in her observations; Makes the following observations: As a preliminary point, the Commission observes that the report, made during of the adoption of its 2010 recommendation, the development and extension of electronic postal voting systems, in particular via the Internet, to a growing number of voting operations and types of voting, remains topical. Commission stresses that the use of such systems must comply with the fundamental principles which govern electoral operations: the secrecy of the ballot except for public ballots, the personal and free character of the vote, the sincerity of electoral operations, the monitor Effective monitoring of the vote and subsequent control by the election judge. These electronic postal voting systems, in particular via the Internet, must also comply with the requirements of the constitutional, legislative and regulatory texts in force. Faced with the continued extension of Internet voting to all types of elections, the Commission wishes to recall that voting by electronic correspondence, in particular via the Internet, presents increased difficulties with regard to the aforementioned principles for the persons responsible for organizing the ballot and those responsible for verifying its progress, mainly because of the opacity and high technicality of the solutions implemented, as well as the very great difficulty of ensuring the identity and freedom of choice of the person carrying out the remote voting operations. During the work that the Commission has carried out since 2003 and taking into account of the threats hanging over these devices, she was able to observe that the existing voting systems did not yet provide e all the guarantees required by the legal texts. Therefore, and in particular, taking into account the aforementioned elements, the Commission remains reserved with regard to the use of electronic voting devices, in particular

via the Internet, for political elections. The purpose of this deliberation is to review the recommendation of 2010 in the light of the electoral operations that have taken place since, the evolution of the voting solutions offered by the service providers in the sector, the feedback made by the various stakeholders, the controls carried out by the CNIL as well as the evolution of the legal framework on data protection. The scope of the new recommendation is electronic postal voting systems, in particular via the Internet. It does not concern barcode voting devices, landline or mobile telephone voting devices, or computer systems made available to voters in the form of voting boxes or voting booths (called voting machines). It is intended to lay down, in a pragmatic way, the security objectives that must be achieved by any device for voting by electronic mail, in particular via the Internet, according to the risks presented by the conduct of the vote. The responses provided by the systems to these security objectives must therefore take into account the context and the threats that weigh on the ballot. with a view to better compliance with the principles of protection of personal data, and to inform data controllers about the choice of electronic voting devices to be used. It repeals deliberation no. a recommendation relating to the security of electronic voting systems. In view of these preliminary observations, the Commission makes the following recommendation. voting, feared events and threats to processing. Thus, the Commission recommends that the solution used for the vote take into account the importance of the level of risk of the election as well as the possible benefits for the stakeholders of using an electronic postal voting system and that the solution chosen meets all the security objectives set with regard to this level of risk. The Commission identifies three levels of risk: Level 1: The sources of threat, among voters, poll organizers or outsiders, have few resources and little motivation. The administrator (or administrators) of the information system is neither an elector nor a candidate. He is considered neutral by all parties. This level applies to ballots involving few voters, taking place in a non-confrontational framework, at the end of which those elected will have few powers, such as the election of a class representative. The ballot does not present significant risks.Level 2: The sources of threat, among voters, organizers of the ballot, external persons, within the service provider or internal staff, may present average resources or average motivations. This level applies to elections involving a large number of voters and presenting a high stake for people but in a context free of any particular conflict. These include, for example, the election of staff representatives within organizations or within a professional order. The ballot presents a moderate risk. Level 3: The sources of threat, among the voters, the organizers of the ballot, external persons, within the service provider or internal staff, may present significant resources or strong motivations. This level concerns elections involving a large number of voters and presenting a very high stake, in a potentially conflicting climate.

These include, for example, elections of staff representatives in large organizations, on a large scale and in a conflictual setting. Voting presents a significant risk. The Commission advises against using an electronic voting system, in particular via the Internet, on the assumption that the sources of the threat may have both significant resources and strong motivation. controller identifies the level corresponding to his situation according to the risks raised by his vote. To this end, the Commission proposes, on an optional basis and by way of example, a simplified analysis grid, based on closed questions, the purpose of which is to guide and help data controllers wishing to do so to position themselves on this ladder. This analysis grid is placed within the practical sheet. In case of doubt between two levels, the highest level should be preferred. The data controller, mastering the scope, issues and context of his vote, is free to choose the level of risk he deems appropriate, as long as he can justify his analysis to the Commission and the expert. independent.Once its level of risk has been identified, the data controller can determine the security objectives that the voting solution must achieve.The choice of the risk level by the data controller being assessed by the mandated independent expert (see below). -after) to ensure that voting operations comply with this recommendation, the data controller should provide it with the information that was taken into account in determining this level. processing of personal data, including voting devices, which meet at least two of the following criteria must in principle be subject to an impact assessment relating to the protection of data (AIPD): automatic decision with legal or similar effect; systematic monitoring; collection of sensitive data (political opinions and trade union membership in particular); collection of personal data on a large scale; cross-referencing of data; vulnerable people (patients, elderly people, children , etc.); innovative use (use of a new technology); exclusion from the benefit of a right/contract. Therefore, with regard to the criteria relating to sensitive data and the collection of data on a large scale and taking into account the context of the vote if necessary, it may be necessary for the data controller to carry out a DPIA. The security objectives to be achieved according to the level of risk Each level of risk is associated with security objectives which make it possible to define the level of security expected. These objectives are cumulative, level 2 being composed of specific security objectives and level 1 security objectives, level 3 being composed of specific security objectives and security objectives of the two previous levels The Commission will offer on its website or any other useful medium, a practical sheet presenting examples enabling the aforementioned safety objectives to be achieved. Manufacturers may, if they wish, provide the Commission with examples of means of achieving the objectives so that this sheet can be supplemented with this information. The Commission will be the sole judge of the relevance of the means proposed. This sheet will detail what is expected behind each security objective.

Voting solutions whose voting presents a level 1 risk must achieve at least all of the following security objectives :Security objective no. 1-01: Implement a high-quality technical and organizational solution that does not present any major flaws (flaws published by the publisher and/or made public by third parties). Security objective n° 1-02: Define the vote of an elector as an atomic operation, that is to say as comprising in an indivisible way the choice, the validation, the registration of the ballot in the ballot box, the signature and issuance of a receipt. Security objective n° 1-03: Authenticate voters by ensuring that the major risks linked to identity theft are significantly reduced. Security objective n° 1- 04: Ensure the strict confidentiality of the ballot from its creation on the voter's workstation. Security objective n° 1-05: Ensure the strict confidentiality and integrity of the ballot during its transport. Security objective n° 1-06: Ensure , in an organizational and/or technical manner, the strict confidentiality and integrity of the ballot during its processing and its storage in the ballot box until the counting. Security objective n° 1-07: Ensure total sealing between the voter identity and the expression of his vote throughout the d duration of the processing. Security objective n° 1-08: Reinforce the confidentiality and the integrity of the data by distributing the secrecy allowing the counting exclusively within the electoral office and guarantee the possibility of counting from a determined threshold of secrecy .Security objective n° 1-09: Define the counting as an atomic function usable only after the close of the ballot.Security objective n° 1-10: Ensure the integrity of the system, the ballot box and the list 'marking.Security objective n° 1-11: Ensure that the counting of the ballot box can be verified a posteriori.The voting solutions whose ballot presents a level 2 risk must at least achieve all the objectives security level 1 as well as the following:Security objective n° 2-01: Ensure high availability of the solution.Security objective n° 2-02: Ensure automatic control of the integrity of the system, the ballot box and attendance list t.Security objective n° 2-03: Allow automatic control by the electoral office of the integrity of the voting platform throughout the ballot.Security objective n° 2-04: Authenticate voters by ensuring that the major and minor risks linked to identity theft are significantly reduced. this has the slightest impact on the other votes in progress. Security objective n° 2-06: Use an information system implementing the physical and logical security measures recommended by the editors and ANSSI. ° 2-07: Ensure the transparency of the ballot box for all voters. Voting solutions whose voting presents a level 3 risk must meet at least all the security objectives of levels 1 and 2, as well as the following:Objecti f security n° 3-01: Study the risks according to a proven method in order to define the most appropriate measures in the context of implementation. Security objective n° 3-02: Allow the transparency of the ballot box for all voters from third-party tools. Security objective no. 3-03: Ensure very high availability of the voting solution by taking into account the risks of major damage. Security objective no. 3-04: Allow control

automatic and manual by the electoral office of the integrity of the platform throughout the ballot. that this has the slightest impact on the other elections in progress. The data controller or its service provider are free to use any solution allowing them to achieve the stated security objectives. Whatever the level determined, it is advisable to provide the electric in due time, an explanatory note clearly detailing the voting operations as well as the general operation of the electronic postal voting system, in particular via the Internet. This explanatory notice does not replace the information obligation imposed by Articles 13 and 14 of the European Data Protection Regulation (GDPR) with regard to the processing of data. At the same time, the Commission would like to point out that, from by their nature and sensitivity, electronic postal voting platforms, in particular via the Internet, must be accessible to all people, in particular to people with disabilities and in particular visually impaired. Thus, for public sector organizations or delegates of a public service mission wishing to offer this service to their voters, it is necessary that the voting system complies with the general accessibility reference system for administrations (RGAA). For organizations not subject to this reference system, it is strongly recommended to follow its requirements in order to enable all voters to cast their vote by this means. Expertise of the electronic postal voting system, in particular via the InternetAny data controller implementing an electronic postal voting system, in particular via the Internet, must have his solution appraised by an independent expert, whether the voting solution is managed in internal or provided by a service provider. The expertise must cover the entire system installed before the ballot (software, server, etc.), the constitution of the lists of electors and their enrollment and the use of the voting system during the ballot and the steps following the vote (counting, archiving, etc.). The expertise must relate to all the elements described in this deliberation and in particular to: the source code corresponding to the version of the software actually implemented; the sealing mechanisms used at the various stages of the ballot; the computer system on which the vote will take place; the network exchanges; the encryption mechanisms used, in particular for the encryption of the ballot; the mechanisms for authenticating voters and the transmission of secrets to them; the assessment of the level of risk of the vote the relevance and effectiveness of the solutions provided by the voting solution to the security objectives. The expertise must cover all the elements constituting the voting solution. The expert carries out audits on the platform, in order to ensure the consistency and effectiveness of the solutions provided, in particular through intrusion tests. All of the operations carried out in this context are appended to the expert report. The expert must be carried out by an independent expert, i.e. he must meet the following criteria: be a computer specialist specializing in the security; have no interest in the company that created the voting solution to be appraised, nor in the organization responsible for processing that

decided to use the voting solution; if possible, have experience in the analysis of voting systems, having appraised the electronic mail voting systems, in particular via the Internet, of at least two different service providers. by electronic correspondence, in particular via the Internet. If the expertise can cover a wider field than that of this recommendation, the expert report provided to the data controller must include a specific part. that presenting the evaluation of the device with regard to the various points of the recommendation. The expert must provide a technical means making it possible to verify a posteriori that the various software components on which the expertise focused have not been modified on the system used during the ballot. The method and means for carrying out this verification must be described in the expert report. To do this, the expert can, for example, use digital fingerprints. The expertise relating to a solution implemented for an election whose risk level is evaluated at 1 can take up elements of an expert report previous one, provided that this expertise carried out on the element in question is not older than 24 months, that it is possible to prove that the element on which this previous expertise related has not been modified since and that no vulnerability on this element has been revealed in the meantime. The expertise relating to a solution implemented for a ballot whose risk level is evaluated at 2 can take up elements from a previous expert report, as soon as when this expertise carried out on the element in question is not older than 12 months, that it is possible to prove that the element on which the previous expertise related has not been modified since and that no vulnerability on this element has not been revealed in the meantime. The expertise po rtant on a solution implemented for an election whose risk level assessed at 3 must be carried out again, for each element, for each election. The expert having access to sensitive information relating to the solutions for which he is responsible for evaluating compliance, in particular the source code of the applications, he is required to take all measures and precautions used in order to protect the elements which are brought to his attention, in particular by limiting as much as possible the reproductions of source code within the report, by keeping its reports within dedicated secure spaces and by not keeping the elements brought to its attention beyond the necessary duration. vote and the persons designated or authorized to ensure the control of electoral operations. he electoral list, to send the voting material and to carry out the signatures can only be used for the aforementioned purposes and cannot be disclosed under penalty of the criminal sanctions provided for by the penal code. The confidentiality of the data is also opposable to the technicians in charge of the management or maintenance of the computer system. To connect remotely or on site to the voting system, the voter must authenticate himself in accordance with this recommendation and using a means corresponding to the security objective corresponding to the level of risk identified for the ballot. During this procedure,

the voting server verifies the identity of the voter and that the latter is indeed authorized to vote. In this case, he accesses the lists or candidates officially selected and in the official order. The voter must be able to choose a list, a candidate or a blank vote so that this choice appears clearly on the screen, independently any other information. He must be able to reconsider this choice. He then validates his choice and this operation triggers the sending of the dematerialized ballot paper to the voting server. The voter then receives the confirmation of his vote and has the possibility of keeping track of this confirmation. The electronic postal voting solution, in particular via the Internet, must offer all the options offered by the texts on which the vote is based, where applicable the null or blank vote. In the event that the ballot is mixed, consisting of a postal vote associated with paper-based postal voting, for example, electronic voting should allow voters the same possibilities as those offered by paper voting, such as the possibility of casting a null or blank vote when this is planned for a ballot, in order to not create distortion depending on the medium used. In the event that these various possibilities are offered to the voter, it is advisable to be attentive to the fact that a person cannot vote twice, in particular by using the system by paper correspondence and the system by Internet. Thus, the solution adopted must make it possible to discard the votes by paper correspondence of a person who has already voted by Internet. Minimum guarantees for a posteriori control For external audit purposes, in particular in the event of electoral disputes, the voting system by electronic correspondence, in particular via the Internet, must be able to provide the technical elements allowing at least to prove irrefutably that: the sealing process remained intact during the ballot; the encryption/decryption keys are only known to their holders; the vote is anonymous when the legislation so requires; the attendance list only includes the list of electors who have voted; the stripped ballot box is indeed the one containing the votes of the electors and that it contains only these votes; no count partial could not be carried out during the ballot; the counting of the ballot box can be verified a posteriori and that it took place correctly. tion of data relating to the electoral operation All support files (copies of source and executable codes of programs and the underlying system, voting materials, registration files, results, backups) must be kept under seal until the exhaustion of the means and deadlines for contentious appeal. This conservation must be ensured under the control 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 third party named to ensure the conservation of these media. When no contentious action has been initiated after the exhaustion of the time limits for appeal, these documents must be destroyed under the control of the electoral commission. Transitional and final provisions This deliberation is published in the Official Journal of the French Republic. It must be taken into account by data

controllers after a transitional period of twelve months from its publication. President Marie-Laure DENIS