#### ACCORD SUR L’ADOPTION DU VOTE ELECTRONIQUE POUR LES ELECTIONS PROFESSIONNELLES

**ENTRE :**

La Société Toppan Photomasks France S.A.S. représentée par \*\*\*, Directeur des Ressources Humaines,

ci-après désignée « **l’Entreprise** » ou « **la Société** »,

d’une part,

**ET :**

Les Organisations Syndicales représentatives représentées par :

* \*\*\*, pour l’Organisation Syndicale représentative CFE-CGC,
* \*\*\*, pour l’Organisation Syndicale représentative CGT-FO,
* \*\*\*, pour l’Organisation Syndicale représentative CFTC,
* \*\*\*, pour l’Organisation Syndicale représentative CFDT,

Dûment mandatés à cet effet,

ci-après désignées les « **Organisations Syndicales** »,

d’autre part

Ci-après désignées « **Les Parties signataires** » ou « **les Parties** ».

**IL A ETE PREALABLEMENT EXPOSE CE QUI SUIT** **:**

L’article 54 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique autorise le recours au vote électronique pour les élections professionnelles.

Le décret n° 2007-602 du 25 avril 2007 et l’arrêté du Ministère de l’Emploi de la Cohésion Sociale et du Logement pris en application du décret précisent les conditions et les modalités de vote par voie électronique pour l’élection des délégués du personnel et des représentants du personnel au Comité d’entreprise.

La délibération n° 2010-371 du 21 octobre 2010 de la Commission nationale de l’informatique et des libertés formule des recommandations sur la mise en place du vote électronique.

Dans ce cadre, les Parties signataires ont étudié l’opportunité de recourir au vote électronique pour organiser les élections professionnelles.

Les informations et témoignages recueillis ont conforté les Parties dans l’appréciation que le vote électronique est de nature à améliorer les processus de vote au sein de l’Entreprise, en permettant notamment :

* de simplifier et sécuriser l’organisation du processus électoral,
* de faciliter le vote pour les salariés en mission, en déplacement ou en horaires postés,
* d'obtenir en fin de scrutin des résultats sécurisés et affichés en quelques minutes,
* d’augmenter le niveau de participation,
* d’inscrire le processus électoral dans une démarche de préservation de l’environnement.

En conséquence, les Parties signataires ont convenu de la mise en place du vote électronique, dans le cadre et selon les conditions et modalités décrites ci-après.

**CECI EXPOSE, LES PARTIES SONT CONVENUES DE CE QUI SUIT :**

**Principes généraux**

Les modalités d’organisation et de déroulement des opérations électorales utilisant le vote électronique seront fixées dans le respect des principes généraux du droit électoral.

Ainsi, les modalités de mise en place du scrutin électronique permettront de respecter les principes suivants :

* Vérifier l’identité des électeurs,
* S’assurer de l’intégrité du vote,
* S’assurer de l’unicité du vote,
* S’assurer de l’anonymat et de la sincérité du vote,
* S’assurer de la confidentialité et respecter le secret du vote électronique,
* Permettre la publicité du scrutin.

Le système de vote permettra également la conservation puis la destruction des données dans les conditions légales.

1. **Objet et champ d’application**

Le présent accord a pour objet de permettre le recours au vote électronique pour les prochaines élections professionnelles de la Société et s’applique à l’ensemble de ses salariés (ainsi qu’aux éventuels salariés mis à disposition de l’Entreprise) appelés à voter auxdites élections.

1. **Définition et choix du moyen de vote électronique**

Les Parties conviennent de recourir au vote électronique à travers le moyen unique du vote par Internet.

Ainsi, la notion de « vote électronique » mentionnée dans le présent accord doit s’entendre comme l’utilisation de ce moyen de communication pour procéder au vote.

1. **Modalités de mise en œuvre du vote électronique**
	1. **Recours à un prestataire extérieur**

Afin de garantir la sécurité des opérations électorales et la confidentialité du vote, les Parties conviennent de ne pas recourir à une solution développée en interne et décident que les élections seront organisées par le « fournisseur prestataire », mandaté pour ce faire par la Direction.

L’Entreprise prendra contact avec un prestataire spécialisé dans les technologies Internet et plus particulièrement dans le développement du vote par Internet (ci-après désigné le « Prestataire ») et lui confiera La conception et la mise en place du système de vote électronique sur la base d’un cahier des charges respectant les prescriptions réglementaires en application des articles R2314-8 et suivants, des articles R2324-4 et suivants du Code du travail, ainsi que de l’arrêté du 25 avril 2007.

Les Parties conviennent que, pour être retenu, le Prestataire devra recevoir l’approbation du service informatique de la Société et que le système de vote sera présenté aux Organisations syndicales représentatives de l’Entreprise.

Le prestataire retenu sera indiqué dans le protocole d’accord préélectoral.

* 1. **Etablissement des fichiers**

Les fichiers électoraux seront établis dans le respect des dispositions des articles 4 et 5 de l’arrêté du 25 avril 2007 précisant les données devant être enregistrées et les destinataires ou catégories de destinataires de celles-ci.

* 1. **Confidentialité, sincérité du vote et stockage des données**

Le système retenu permettra d'assurer la confidentialité des données transmises, s'agissant notamment des listes électorales, des collèges électoraux et des moyens d'authentification.

Les données relatives aux électeurs inscrits sur les listes électorales ainsi que celles relatives à leur vote seront traitées par des systèmes informatiques distincts, dédiés et isolés, respectivement dénommés «fichier des électeurs» et «contenu de l'urne électronique».

Le vote émis par chaque électeur sera crypté et stocké dans l'urne électronique dédiée.

Le contenu des urnes électroniques sera inaccessible jusqu’au dépouillement de celles-ci, effectué sous le contrôle des membres du bureau de vote à l’aide des clés de déchiffrement reçues et conservées par ces derniers. Les fichiers comportant les éléments d'authentification des électeurs et les clés de déchiffrement de sauvegarde (qui ne seront utilisées qu’en cas de force majeure, c’est-à-dire de la perte de plus de deux clés par les membres du bureau de vote) ne seront accessibles qu'au personnel du Prestataire chargé de la gestion et de la maintenance du système.

Le système de vote électronique sera scellé à l'ouverture et à la clôture du scrutin. Le système de vote électronique sera également bloqué après le dépouillement afin de garantir l'impossibilité de reprendre ou de modifier les résultats après la décision de clôture du dépouillement. La procédure de décompte des votes enregistrés devra pouvoir être déroulée de nouveau.

Les fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde seront conservés jusqu'à l'expiration du délai de recours ou jusqu'à la décision juridictionnelle devenue définitive. A l'expiration de ces délais, ces fichiers supports seront détruits.

* 1. **Cellule d'assistance technique et sécurité**

Une cellule d'assistance technique chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique, comprenant les représentants du Prestataire, sera mise en place pendant la durée des opérations de vote.

Elle aura notamment pour mission de :

* Procéder, avant que le vote ne soit ouvert, à un test du système de vote électronique et vérifier que l'urne électronique est vide, scellée et chiffrée par des clés délivrées à cet effet ;
* Procéder, avant que le vote ne soit ouvert, à un test spécifique du système de dépouillement, à l'issue duquel le système sera scellé ;
* Contrôler, à l'issue des opérations de vote et avant les opérations de dépouillement, le scellement de ce système.

En outre, un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et les mêmes caractéristiques, sera mis en place.

En cas de dysfonctionnement informatique résultant d'une attaque du système par un tiers, d'une infection virale, d'une défaillance technique ou d'une altération des données, le bureau de vote aura compétence, après avis des représentants du Prestataire chargé de la mise en œuvre du vote, pour prendre toute mesure d'information et de sauvegarde et notamment pour décider la suspension des opérations de vote.

* 1. **Expertise et déclaration auprès de la CNIL**

Le système de vote électronique, préalablement à sa mise en place ou à toute modification substantielle de sa conception, devra avoir été soumis à une expertise indépendante, destinée à vérifier le respect des prescriptions légales.

En outre, le recours à des fichiers nominatifs au sens de la loi du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés, fera l’objet d’une déclaration auprès de la CNIL.

Conformément aux dispositions du Code du travail, les Organisations Syndicales représentatives incluses dans le périmètre du présent accord seront tenues informées de l'accomplissement des formalités déclaratives préalables auprès de la CNIL.

* 1. **Information et formation**

Tous les moyens seront mis en œuvre pour faciliter l'appropriation de cette nouvelle technique de vote par le salarié. En particulier, chaque salarié disposera d'une notice d'information détaillée sur le déroulement des opérations électorales.

Bénéficieront d’une formation sur le système de vote retenu :

* Les représentants du personnel concernés, c’est-à-dire, les Délégués du Personnel et les membres du Comité d’Entreprise, titulaires et suppléants,
* Les Délégués Syndicaux,
* Les membres du(des) bureau(x) de vote,
* Les membres de la cellule d’assistance technique, à l’exclusion du représentant du Prestataire.
1. **Déroulement des opérations de vote**
	1. **Protocole d’accord préélectoral**

Dans le cadre de l’élection professionnelle considérée, les Parties engageront une négociation en vue de la conclusion d’un protocole d’accord préélectoral, définissant notamment le calendrier, les modalités de constitution du(des) bureau(x) de vote, la répartition des sièges.

Le protocole d’accord préélectoral mentionnera la conclusion du présent accord et le nom du Prestataire choisi pour mettre en place ce système de vote électronique au sein de l’entreprise.

* 1. **Modalités relatives à l’ouverture et à la fermeture du scrutin**

Les électeurs auront la possibilité de voter à tout moment pendant l’ouverture du(des) bureau(x) de vote, de n’importe quel ordinateur, de leur lieu de travail, de leur domicile ou de leur lieu de villégiature en se connectant sur le serveur sécurisé dédié aux élections.

Les salariés seront informés, selon des modalités définies dans le protocole d’accord préélectoral, des dates et heures relatives à l’ouverture et à la fermeture du(des) bureau(x) de vote. Celles-ci seront déterminées lors de la négociation du protocole d’accord pré-électoral

* 1. **Caractéristiques du matériel de vote**

Le Prestataire assurera la programmation des pages Web et notamment la présentation à l’écran des bulletins de vote sur le site dédié et des liens vers les professions de foi.

Les professions de foi des listes candidates seront accessibles sur le site de vote. Le format des professions de foi sera défini dans le protocole d’accord préélectoral.

Le Prestataire reproduira sur le serveur les listes de candidats, avec le cas échéant, les logos.

Pour chaque élection, les listes (ainsi que les noms des candidats associés) seront présentées sur une seule et même page (sans défilement) ; les règles relatives à leur disposition à l’écran seront définies dans le protocole d’accord préélectoral.

Par ailleurs, afin de ne pas favoriser une liste ou un vote plutôt qu’un autre, le Prestataire veillera à la neutralité de la dimension des bulletins, des tailles de caractères et de la police de caractères utilisées entre les listes ou choix proposés.

Le cas échéant, le logo des listes candidates sera visible sur chaque bulletin. Les logos devront être normés en taille de lecture pour ne favoriser visuellement aucune des listes.

Le système proposera par défaut le vote pour les listes complètes. La fonctionnalité permettant de rayer un ou plusieurs noms doit être intégrée dans le moyen de vote électronique.

* 1. **Modalités d’accès au serveur de vote**

Chaque électeur recevra de la part du Prestataire, avant le premier tour des élections :

* l'adresse du serveur de vote,
* des codes d’accès personnels au serveur de vote, constitués d’un code d’identification personnel et d’un mot de passe générés de manière aléatoire par le Prestataire,
* la date de début et de fin du vote électronique au premier et au deuxième tour.

Les modalités d’envoi des codes d’accès seront définies dans le cadre du protocole d’accord préélectoral, de manière à assurer la confidentialité de ces données dans le respect des dispositions du Code du travail et de la jurisprudence.

L’électeur accèdera au système de vote en saisissant son identifiant personnel et sa date de naissance (ou une autre donnée personnelle définie dans le cadre du protocole d’accord préélectoral).

Une fois connecté, pour l’élection tant des titulaires que des suppléants, l’électeur se verra présenter les bulletins de vote correspondant à son collège.

L’électeur validera son vote en saisissant son mot de passe.

En cas de perte ou de non réception de leurs codes d’accès personnels, les électeurs pourront obtenir de nouveaux codes au cours des opérations de vote selon une procédure sécurisée.

Les membres du bureau de vote pourront consulter en permanence les listes d’émargement et le taux de participation. Aucun résultat partiel n’est accessible pendant le déroulement du scrutin, toutefois, le protocole d’accord préélectoral pourra prévoir de dévoiler aux votants le taux de participation.

* 1. **Opérations de dépouillement**

A l’issue des opérations de vote et avant les opérations de dépouillement, les membres du(des) bureau(x) de vote contrôleront la fermeture du scrutin (article R2324-7 et R2324-14 du code du travail). Dès la clôture du scrutin, le contenu de l’urne, les listes d’émargement et les serveurs informatiques seront figés, horodatés et scellés automatiquement.

Le dépouillement se fait par l’activation conjointe d’au moins deux clés de déchiffrement différentes par les membres du(des) bureau(x) de vote (Président, Assesseurs).

Les membres du(des) bureau(x) de vote proclameront les résultats et signeront les procès-verbaux.

1. **Durée de l’accord**

Le présent accord est conclu pour une durée déterminée en vue de l’organisation des prochaines élections professionnelles. Il cessera immédiatement de produire tout effet dès l’élection desdits représentants réalisée et définitive.

1. **Révision**

Le présent accord pourra faire l’objet de révision par la Société et les Partenaires sociaux signataires ou ceux y ayant adhéré ultérieurement, conformément aux dispositions des articles L. 2261-7 et L. 2261-8 du Code du travail. Toute demande de révision, totale ou partielle, obligatoirement accompagnée d’une proposition de rédaction nouvelle, sera notifiée par lettre recommandée avec accusé de réception à chacune des autres parties signataires. La discussion de la demande de révision doit s’engager dans les trois (3) mois suivant la présentation de celle-ci. Toute modification fera l’objet d’un avenant conclu dans les conditions prévues par les dispositions législatives et règlementaires en vigueur.

1. **Dépôt**

Le présent accord sera, à la diligence de la Société, déposé en double exemplaire dont une version sur support papier signée des parties, envoyée par lettre recommandée avec demande d’avis de réception, et une version sur support électronique, à la Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l’Emploi (« DIRECCTE ») compétente (Ile de France). Il sera également remis un exemplaire au greffe du Conseil de prud’hommes d’Evry, par lettre recommandée avec demande d’avis de réception.

Fait à Corbeil-Essonnes, le 06 septembre 2017

En 07 exemplaires

\*\*\*

Directeur des Ressources Humaines

Toppan Photomasks France S.A.S.

\*\*\* \*\*\*

Délégué Syndical CFE-CGC Délégué Syndical CGT-FO

\*\*\* \*\*\*

Délégué Syndical CFTC Délégué Syndical CFDT

 ANNEXE

Prescriptions légales et règlementaires

**Code du travail – Titre Ier : Délégués du personnel**

**Article R2314-8**

Modifié par Décret n°2016-1676 du 5 décembre 2016 - art. 1

L'élection des délégués du personnel peut être réalisée par vote électronique sur le lieu de travail ou à distance.

Sans préjudice des dispositions relatives au protocole d'accord préélectoral prévues aux articles L. 2314-3 et suivants, la possibilité de recourir à un vote électronique est ouverte par un accord d'entreprise ou par un accord de groupe. A défaut d'accord, l'employeur peut décider de ce recours qui vaut aussi, le cas échéant, pour les élections partielles se déroulant en cours de mandat.

Un cahier des charges respectant les dispositions du présent paragraphe est établi dans le cadre de l'accord mentionné au deuxième alinéa ou, à défaut, par l'employeur.

Le cahier des charges est tenu à la disposition des salariés sur le lieu de travail et mis sur l'intranet, dans les entreprises lorsqu'il en existe un.

La mise en place du vote électronique n'interdit pas le vote à bulletin secret sous enveloppe si l'accord ou l'employeur n'exclut pas cette modalité.

**Article R2314-9**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

La conception et la mise en place du système de vote électronique peuvent être confiées à un prestataire choisi par l'employeur sur la base d'un cahier des charges respectant les dispositions du présent paragraphe.

Le système retenu assure la confidentialité des données transmises, notamment de celles des fichiers constitués pour établir les listes électorales des collèges électoraux, ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.

**Article R2314-10**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Lors de l'élection par vote électronique, les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne sont uniquement accessibles aux personnes chargées de la gestion et de la maintenance du système.

 Les données relatives aux électeurs inscrits sur les listes électorales ainsi que celles relatives à leur vote sont traitées par des systèmes informatiques distincts, dédiés et isolés, respectivement dénommés « fichier des électeurs » et « contenu de l'urne électronique ».

**Article R2314-11**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Le système de vote électronique est conçu de manière à pouvoir être scellé à l'ouverture et à la clôture du scrutin.

**Article R2314-12**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Préalablement à sa mise en place ou à toute modification substantielle de sa conception, le système de vote électronique est soumis à une expertise indépendante, destinée à vérifier le respect des articles R. 2314-8 à R. 2314-11. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Les dispositions de ces mêmes articles s'imposent également aux personnes chargées de la gestion et de la maintenance du système informatique.

**Article R2314-13**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

L'employeur met en place une cellule d'assistance technique chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique, comprenant, le cas échéant, les représentants du prestataire.

**Article R2314-14**

Modifié par Décret n°2016-1676 du 5 décembre 2016 - art. 1

L'employeur informe les organisations syndicales de salariés représentatives dans l'entreprise ou les établissements concernés, de l'accomplissement des formalités déclaratives préalables auprès de la Commission nationale de l'informatique et des libertés.

**Article R2314-15**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Chaque salarié dispose d'une notice d'information détaillée sur le déroulement des opérations électorales.

Les représentants du personnel, les délégués syndicaux et les membres du bureau de vote bénéficient d'une formation sur le système de vote électronique retenu.

**Article R2314-16**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Le protocole d'accord préélectoral mentionne la conclusion de l'accord d'entreprise ou de l'accord de groupe autorisant le recours au vote électronique et, s'il est déjà arrêté, le nom du prestataire choisi pour le mettre en place.

Il comporte en annexe la description détaillée du fonctionnement du système retenu et du déroulement des opérations électorales.

**Article R2314-17**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Le vote électronique se déroule, pour chaque tour de scrutin, pendant une période délimitée.

**Article R2314-18**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

En présence des représentants des listes de candidats, la cellule d'assistance technique :

 1° Procède, avant que le vote ne soit ouvert, à un test du système de vote électronique et vérifie que l'urne électronique est vide, scellée et chiffrée par des clés délivrées à cet effet ;

 2° Procède, avant que le vote ne soit ouvert, à un test spécifique du système de dépouillement, à l'issue duquel le système est scellé ;

 3° Contrôle, à l'issue des opérations de vote et avant les opérations de dépouillement, le scellement de ce système.

**Article R2314-19**

Modifié par Décret n°2016-1676 du 5 décembre 2016 - art. 1

La liste d'émargement n'est accessible qu'aux membres du bureau de vote et à des fins de contrôle du déroulement du scrutin.

Aucun résultat partiel n'est accessible pendant le déroulement du scrutin. Toutefois, le nombre de votants peut, si l'employeur ou l'accord prévu à l'article R. 2314-8 le prévoit, être révélé au cours du scrutin.

Lorsque le vote sous enveloppe n'a pas été exclu, l'ouverture du vote n'a lieu qu'après la clôture du vote électronique. Le président du bureau de vote dispose, avant cette ouverture, de la liste d'émargement des électeurs ayant voté par voie électronique.

**Article R2314-20**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

L'employeur ou le prestataire qu'il a retenu conserve sous scellés, jusqu'à l'expiration du délai de recours et, lorsqu'une action contentieuse a été engagée, jusqu'à la décision juridictionnelle devenue définitive, les fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde. La procédure de décompte des votes doit, si nécessaire, pouvoir être exécutée de nouveau.

 A l'expiration du délai de recours ou, lorsqu'une action contentieuse a été engagée, après l'intervention d'une décision juridictionnelle devenue définitive, l'employeur ou, le cas échéant, le prestataire procède à la destruction des fichiers supports.

**Article R2314-21**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Un arrêté du ministre chargé du travail, pris après avis de la Commission nationale de l'informatique et des libertés, précise les dispositions pratiques de mise en œuvre du vote électronique.

**Code du travail – Titre II : Comité d’Entreprise**

**Article R2324-4**

Modifié par Décret n°2016-1676 du 5 décembre 2016 - art. 2

L'élection des délégués du personnel au comité d'entreprise peut être réalisée par vote électronique sur le lieu de travail ou à distance.

Sans préjudice des dispositions relatives au protocole d'accord préélectoral prévues aux articles L. 2324-4 et suivants, la possibilité de recourir à un vote électronique est ouverte par un accord d'entreprise ou par un accord de groupe. A défaut d'accord, l'employeur peut décider de ce recours qui vaut aussi, le cas échéant, pour les élections partielles se déroulant en cours de mandat.

Un cahier des charges respectant les dispositions des articles R. 2324-5 et suivants est établi dans le cadre de l'accord mentionné au deuxième alinéa ou, à défaut, par l'employeur.

Le cahier des charges est tenu à la disposition des salariés sur le lieu de travail et mis sur l'intranet, dans les entreprises lorsqu'il en existe un.

La mise en place du vote électronique n'interdit pas le vote à bulletin secret sous enveloppe si l'accord ou l'employeur n'exclut pas cette modalité.

**Article R2324-5**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

La conception et la mise en place du système de vote électronique peuvent être confiées à un prestataire choisi par l'employeur sur la base d'un cahier des charges respectant les dispositions du présent paragraphe.

 Le système retenu assure la confidentialité des données transmises, notamment de celles des fichiers constitués pour établir les listes électorales des collèges électoraux, ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.

**Article R2324-6**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Lors de l'élection par vote électronique, les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne sont uniquement accessibles aux personnes chargées de la gestion et de la maintenance du système.

 Les données relatives aux électeurs inscrits sur les listes électorales ainsi que celles relatives à leur vote sont traitées par des systèmes informatiques distincts, dédiés et isolés, respectivement dénommés « fichier des électeurs » et « contenu de l'urne électronique ».

**Article R2324-7**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Le système de vote électronique doit pouvoir être scellé à l'ouverture et à la clôture du scrutin.

**Article R2324-8**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Préalablement à sa mise en place ou à toute modification substantielle de sa conception, le système de vote électronique est soumis à une expertise indépendante destinée à vérifier le respect des articles R. 2324-4 à R. 2324-7. Le rapport de l'expert est tenu à la disposition de la Commission nationale de l'informatique et des libertés.

Les prescriptions de ces mêmes articles s'imposent également aux personnes chargées de la gestion et de la maintenance du système informatique.

**Article R2324-9**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

L'employeur met en place une cellule d'assistance technique chargée de veiller au bon fonctionnement et à la surveillance du système de vote électronique, comprenant, le cas échéant, les représentants du prestataire.

**Article R2324-10**

Modifié par Décret n°2016-1676 du 5 décembre 2016 - art. 2

L'employeur informe les organisations syndicales de salariés représentatives dans l'entreprise ou le ou les établissements concernés, de l'accomplissement des formalités déclaratives préalables auprès de la Commission nationale de l'informatique et des libertés.

**Article R2324-11**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Chaque salarié dispose d'une notice d'information détaillée sur le déroulement des opérations électorales.

 Les représentants du personnel et les membres du bureau de vote bénéficient d'une formation sur le système de vote électronique retenu.

**Article R2324-12**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Le protocole d'accord préélectoral mentionne la conclusion de l'accord d'entreprise ou de l'accord de groupe autorisant le recours au vote électronique et, s'il est déjà arrêté, le nom du prestataire choisi pour le mettre en place.

 Il comporte en annexe la description détaillée du fonctionnement du système retenu et du déroulement des opérations électorales.

**Article R2324-13**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Le vote électronique se déroule, pour chaque tour de scrutin, pendant une période délimitée.

**Article R2324-14**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

En présence des représentants des listes de candidats, la cellule d'assistance technique :

 1° Procède, avant que le vote ne soit ouvert, à un test du système de vote électronique et vérifie que l'urne électronique est vide, scellée et chiffrée par des clés délivrées à cet effet ;

 2° Procède, avant que le vote ne soit ouvert, à un test spécifique du système de dépouillement à l'issue duquel le système est scellé ;

 3° Contrôle, à l'issue des opérations de vote et avant les opérations de dépouillement, le scellement de ce système.

**Article R2324-15**

Modifié par Décret n°2016-1676 du 5 décembre 2016 - art. 2

La liste d'émargement n'est accessible qu'aux membres du bureau de vote et à des fins de contrôle de déroulement du scrutin.

Aucun résultat partiel n'est accessible pendant le déroulement du scrutin. Toutefois, le nombre de votants peut, si l'employeur ou l'accord prévu à l'article R. 2324-4 le prévoit, être révélé au cours du scrutin.

Lorsque le vote sous enveloppe n'a pas été exclu, l'ouverture du vote n'a lieu qu'après la clôture du vote électronique. Le président du bureau de vote dispose, avant cette ouverture, de la liste d'émargement des électeurs ayant voté par voie électronique.

**Article R2324-16**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

L'employeur ou le prestataire qu'il a retenu conserve sous scellés, jusqu'à l'expiration du délai de recours et, lorsqu'une action contentieuse a été engagée, jusqu'à la décision juridictionnelle devenue définitive, les fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde. La procédure de décompte des votes doit, si nécessaire, pouvoir être exécutée de nouveau.

 A l'expiration du délai de recours ou, lorsqu'une action contentieuse a été engagée, après l'intervention d'une décision juridictionnelle devenue définitive, l'employeur ou, le cas échéant, le prestataire procède à la destruction des fichiers supports.

**Article R2324-17**

Créé par Décret n°2008-244 du 7 mars 2008 - art. (V)

Un arrêté du ministre chargé du travail, pris après avis de la Commission nationale de l'informatique et des libertés, précise les dispositions pratiques de mise en œuvre du vote électronique.

**Délibération n° 2010-371 du 21 octobre 2010 portant adoption d’une recommandation relative à la sécurité des systèmes de vote électronique**

La Commission nationale de l’informatique et des libertés,

Vu la convention du Conseil de l’Europe du 28 janvier 1981 pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données;

Vu le code électoral ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés, modifiée par la loi no 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel ;

Vu le décret no 2005-1309 du 20 octobre 2005 pris pour l’application de la loi no 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés, modifié par le décret no 2007-451 du 25 mars 2007 ; Après avoir entendu Mme Isabelle Falque-Pierrotin, vice-présidente, en son rapport et Mme Elisabeth Rolin, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Alors que le vote électronique commençait seulement à s’implanter en 2003, lors de l’adoption de la première recommandation de la CNIL, la commission constate aujourd’hui que les systèmes de vote électronique sur place ou à distance se sont développés et s’étendent désormais à un nombre croissant d’opérations de vote et de types de vote.

La commission souligne que le recours à de tels systèmes doit s’inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin sauf pour les scrutins publics, le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l’élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

La commission constate que si l’application principale du vote électronique réside dans les élections professionnelles (comité d’entreprise et représentants du personnel), celui-ci se développe également pour les assemblées générales, conseil de surveillance, élection des représentants de professions réglementées et, depuis 2003, pour des élections à caractère politique. De plus, en 2009, pour la première fois, la possibilité de recourir au vote électronique pour une élection nationale, au suffrage universel direct, a été introduite par l’ordonnance no 2009-936 du 29 juillet 2009 relative à l’élection de députés par les Français établis hors de France.

Devant l’extension du vote par internet à tous types d’élections, la commission souhaite rappeler que le vote électronique présente des difficultés accrues au regard des principes susmentionnés pour les personnes chargées d’organiser le scrutin et celles chargées d’en vérifier le déroulement, principalement à cause de la technicité importante des solutions mises en oeuvre. Au cours des travaux que la commission a menés depuis 2003, elle a, en effet, pu constater que les systèmes de vote existants ne fournissaient pas encore toutes les garanties exigées par les textes légaux. Dès lors et en particulier, compte tenu des éléments précités, la commission est réservée quant à l’utilisation de dispositifs de vote électronique pour des élections politiques.

La présente délibération a pour objet de revoir la recommandation de 2003 à l’aune des opérations électorales intervenues depuis cette date et de leur analyse par la CNIL, y compris par les contrôles effectués.

La nouvelle recommandation a pour champ d’application les dispositifs de vote électronique à distance, en particulier par internet. Elle ne concerne pas les dispositifs de vote par codes-barres, les dispositifs de vote par téléphone fixe ou mobile, ni les machines à voter. Elle est destinée à fixer, de façon pragmatique, les garanties minimales que doit respecter tout dispositif de vote électronique, celles-ci pouvant être, le cas échéant, complétées par des mesures supplémentaires. Elle vise également à orienter les futures évolutions des systèmes de vote électronique en vue d’un meilleur respect des principes de protection des données personnelles et à éclairer les responsables de traitement sur le choix des dispositifs de vote électronique à retenir.

Elle abroge la délibération no 2003-036 du 1er juillet 2003 portant adoption d’une recommandation relative à la sécurité des systèmes de vote électronique.

Compte tenu de ces observations préalables, la commission émet la recommandation suivante

I. – Sur les exigences préalables à la mise en oeuvre des systèmes de vote électronique

1. L’expertise du système de vote électronique

Tout système de vote électronique doit faire l’objet d’une expertise indépendante.

L’expertise doit couvrir l’intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l’utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).

L’expertise doit porter sur l’ensemble des mesures décrites dans la présente délibération, et notamment sur :

* le code source du logiciel, y compris dans le cas de l’utilisation d’un logiciel libre ;
* les mécanismes de scellement utilisés aux différentes étapes du scrutin (voir ci-après) ;
* le système informatique sur lequel le vote va se dérouler, et notamment le fait que le scrutin se déroulera sur un système isolé ;
* les échanges réseau ;
* les mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l’électeur.

L’expertise doit être réalisée par un expert indépendant, c’est-à-dire qu’il devra répondre aux critères suivants :

* être un informaticien spécialisé dans la sécurité ;
* ne pas avoir d’intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d’utiliser la solution de vote ;
* posséder une expérience dans l’analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d’au moins deux prestataires différents ;
* avoir suivi la formation délivrée par la CNIL sur le vote électronique.

Le rapport d’expertise doit être remis au responsable de traitement. Les prestataires de solutions de vote électronique doivent, par ailleurs, transmettre à la CNIL les rapports d’expertise correspondant à la première version et aux évolutions substantielles de la solution de vote mise en place.

Si l’expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d’expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l’évaluation du dispositif au regard des différents points de la recommandation.

L’expert doit fournir un moyen technique permettant de vérifier a posteriori que les différents composants logiciels sur lesquels a porté l’expertise n’ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d’effectuer cette vérification doivent être décrits dans le rapport d’expertise.

2. La séparation des données nominatives des électeurs et des votes

Le dispositif doit garantir que l’identité de l’électeur ne peut pas être mise en relation avec l’expression de son vote, et cela à tout moment du processus de vote, y compris après le dépouillement.

3. Les sécurités informatiques

Il convient que toutes les mesures physiques (contrôle d’accès, détermination précise des personnes habilitées à intervenir…) et logiques (firewall, protection d’accès aux applicatifs…) soient prises, tant au niveau des serveurs du dispositif que sur les postes accessibles au public, afin de garantir la sécurité des données personnelles et du système de vote dans son ensemble. Les algorithmes de chiffrement et de signature électronique doivent, dans tous les cas, être des algorithmes publics réputés « forts » et doivent, si les élections sont mises en place par une autorité administrative, répondre aux exigences prévues dans le référentiel général de sécurité (RGS).

Si un système matériel permet d’héberger plusieurs scrutins, il doit mettre en oeuvre une solution technique (par exemple par une « virtualisation » des systèmes) permettant d’isoler chaque scrutin sur un système informatique distinct de manière à garantir que chaque système soit indépendant et se comporte de manière autonome.

4. Le scellement du dispositif de vote électronique

Avant le début du scrutin, les systèmes de vote électronique utilisés, la liste des candidats et la liste des électeurs doivent faire l’objet d’un scellement, c’est-à-dire d’un procédé permettant de déceler toute modification du système. Avant cette procédure de scellement, il est vérifié que les modules ayant fait l’objet d’une expertise n’ont pas été modifiés. La liste d’émargement et l’urne électronique doivent faire l’objet d’un procédé garantissant leur intégrité durant le vote, c’est-à-dire assurant qu’ils ne peuvent respectivement être modifiés que par l’ajout d’un bulletin et d’un émargement, dont l’intégrité est assurée, d’un électeur authentifié de manière non frauduleuse. Ce procédé doit déceler toute autre modification du système. Après la clôture du vote, la liste d’émargement et l’urne électronique doivent être scellées.

Les procédés de scellement doivent eux-mêmes utiliser des algorithmes publics réputés forts et, le cas échéant, respecter les recommandations du référentiel général de sécurité. La vérification des scellements doit pouvoir se faire à tout moment, y compris durant le déroulement du scrutin. Le bureau de vote doit disposer d’outils dont l’utilisation ne requiert pas l’intervention du prestataire pour procéder à la vérification du scellement, par exemple par une prise d’empreinte numérique.

5. L’existence d’une solution de secours

Tout système de vote électronique doit comporter un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et les mêmes caractéristiques.

6. La surveillance effective du scrutin

La mise en oeuvre du système de vote électronique doit être opérée sous le contrôle effectif, tant au niveau des moyens informatiques centraux que de ceux, éventuellement, déployés sur place, de représentants de l’organisme mettant en place le vote ou d’experts désignés par lui. Dès lors, il importe que toutes les mesures soient prises pour leur permettre de vérifier l’effectivité des dispositifs de sécurité prévus pour assurer le secret du vote et, en particulier, les mesures prises pour :

* garantir la confidentialité du fichier des électeurs comportant les éléments d’authentification ;
* garantir le chiffrement ininterrompu des bulletins de vote et leur conservation dans un traitement distinct de celui mis en oeuvre pour assurer la tenue du fichier des électeurs ;
* assurer la conservation des différents supports d’information pendant et après le déroulement du scrutin.

Toutes les facilités doivent être accordées aux membres du bureau de vote et aux délégués des candidats, s’ils le souhaitent, pour pouvoir assurer une surveillance effective de l’ensemble des opérations électorales et, en particulier, de la préparation du scrutin, du vote, de l’émargement et du dépouillement. A ce titre et afin de garantir un contrôle effectif des opérations électorales, le prestataire technique doit mettre à disposition des représentants de l’organisme responsable du traitement, des experts, des membres du bureau de vote, des délégués des candidats et des scrutateurs tous documents utiles et assurer une formation de ces personnes au fonctionnement du dispositif de vote électronique.

7. La localisation du système informatique central

Il paraît hautement souhaitable que les serveurs et les autres moyens informatiques centraux du système de vote électronique soient localisés sur le territoire national afin de permettre un contrôle effectif de ces opérations par les membres du bureau de vote et les délégués ainsi que l’intervention, le cas échéant, des autorités nationales compétentes.

II. – Sur le scrutin

A. – Sur les opérations précédant l’ouverture du scrutin 1.

1. La confidentialité des données

Les fichiers nominatifs des électeurs constitués aux fins d’établir la liste électorale, d’adresser le matériel de vote et de réaliser les émargements ne peuvent être utilisés qu’aux fins précitées et ne peuvent être divulgués sous peine des sanctions pénales encourues au titre des articles 226-17 et 226-21 du code pénal.

La confidentialité des données est également opposable aux techniciens en charge de la gestion ou de la maintenance du système informatique.

Les fichiers comportant les éléments d’authentification des électeurs, les clés de chiffrement/déchiffrement et le contenu de l’urne ne doivent pas être accessibles, de même que la liste d’émargement, sauf aux fins de contrôle de l’effectivité de l’émargement des électeurs.

En cas de recours à un prestataire extérieur, celui-ci doit s’engager contractuellement à respecter ces dispositions par la signature d’une clause de confidentialité et de sécurité et à fournir le descriptif détaillé du dispositif technique mis en oeuvre pour assurer cette confidentialité. Le prestataire doit également s’engager à restituer les fichiers restant en sa possession à l’issue des opérations électorales et à détruire toutes les copies totales ou partielles qu’il aurait été amené à effectuer sur quelque support que ce soit.

Le prestataire peut recevoir automatiquement des informations techniques sur le fonctionnement du système de vote pendant tout le déroulement du scrutin. Le prestataire ne doit intervenir sur le système de vote qu’en cas de dysfonctionnement informatique résultant d’une attaque du système par un tiers, d’une infection virale, d’une défaillance technique ou d’une altération des données. Un dispositif technique doit garantir que le bureau de vote est informé automatiquement et immédiatement de tout accès par le prestataire à la plate-forme de vote. Le prestataire doit informer le bureau de vote de toutes les mesures prises pour remédier au dysfonctionnement constaté. Le système de vote doit comprendre un module permettant la remontée automatique de cette information au bureau de vote.

Toutes les actions effectuées sur le serveur de vote ainsi que celles concernant le déroulement du scrutin doivent faire l’objet d’une journalisation. L’intégrité de cette journalisation doit être garantie à tout moment par un procédé cryptographique.

Le bureau de vote, quant à lui, a compétence pour prendre toute mesure d’information et de sauvegarde, et notamment pour décider la suspension des opérations de vote. Le système de vote doit permettre d’informer les électeurs de cette éventuelle décision.

2. Les procédés d’authentification de l’électeur

Le système de vote doit prévoir l’authentification des personnes autorisées à accéder au système pour exprimer leur vote. Il doit garantir la confidentialité des moyens fournis à l’électeur pour cet accès et prendre toutes précautions utiles afin d’éviter qu’une personne non autorisée ne puisse se substituer frauduleusement à l’électeur.

La commission estime qu’une authentification de l’électeur sur la base d’un certificat électronique constitue la solution la plus satisfaisante en l’état de la technique. Le certificat électronique doit être choisi et utilisé conformément aux préconisations du RGS.

Dans le cas du recours à un dispositif biométrique pour l’authentification, le responsable de traitement doit respecter les formalités imposées par la loi du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés.

A défaut de recourir aux solutions précitées, dans le cas de la génération d’identifiants et de mots de passe à partir de la liste électorale, le fichier ainsi créé doit faire l’objet d’un chiffrement. Les modalités de génération et d’envoi des codes personnels doivent être conçues de façon à garantir leur confidentialité et, en particulier, que les divers prestataires éventuels ne puissent pas en prendre connaissance.

Dans le cas où le vote s’opérerait par l’enregistrement d’un identifiant permanent apposé sur une carte ou tout autre document ainsi qu’un mot de passe envoyé à chaque électeur, la génération de ces identifiants et mots de passe doit se faire dans les mêmes conditions de sécurité que celles énumérées ci-dessus. Il en va de même de l’envoi du mot de passe.

L’authentification de l’électeur peut être renforcée par un dispositif de type défi/réponse – c’est-à-dire l’envoi par le serveur d’authentification d’une question dont l’électeur est seul à connaître la réponse – ou par l’envoi d’un code par SMS sur le téléphone personnel de l’électeur.

En cas de perte ou de vol de ses moyens d’authentification, une procédure doit permettre à l’électeur d’effectuer son vote et de rendre les moyens d’authentification perdus ou volés inutilisables.

Le vote doit être accessible à tous les systèmes d’exploitation et tous les navigateurs utilisés par les électeurs. A défaut de mettre à disposition du matériel de vote accessible à tous, une procédure manuelle doit être prévue.

3. L’information des électeurs

Il convient de fournir aux électeurs en temps utile une note explicative détaillant clairement les opérations de vote ainsi que le fonctionnement général du système de vote électronique.

4. Le contrôle du système avant l’ouverture du scrutin

Un contrôle du système de vote électronique doit être organisé avant l’ouverture du scrutin et en présence des scrutateurs afin de constater la présence des différents scellements, le bon fonctionnement des machines, que la liste d’émargement est vierge et que l’urne électronique destinée à recevoir les votes est bien vide.

5. Les clés de chiffrement

La génération des clés destinées à permettre le déchiffrement des bulletins de vote doit être publique et se dérouler avant l’ouverture du scrutin. Cette procédure doit être conçue de manière à prouver de façon irréfutable que seuls le président du bureau et ses assesseurs prennent connaissance de ces clés, à l’exclusion de toute autre personne y compris les personnels techniques chargés du déploiement du système de vote. La commission estime que le nombre de clés de chiffrement doit être au minimum de trois, la combinaison d’au moins deux de ces clés étant indispensable pour permettre le dépouillement.

Le système de vote doit garantir que des résultats partiels (hormis le nombre de votants) ne seront pas accessibles durant le déroulement du scrutin.

B. – Sur le déroulement du vote

1. Le vote

Les heures d’ouverture et de fermeture du scrutin électronique doivent pouvoir être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

Pour se connecter à distance ou sur place au système de vote, l’électeur doit s’authentifier conformément à la présente recommandation. Au cours de cette procédure, le serveur de vote vérifie l’identité de l’électeur et que celui-ci est bien autorisé à voter. Dans ce cas, il accède aux listes ou aux candidats officiellement retenus et dans l’ordre officiel. Le vote blanc doit être prévu lorsque la loi l’autorise.

L’électeur doit pouvoir choisir une liste, un candidat ou un vote blanc de façon à ce que ce choix apparaisse clairement à l’écran, indépendamment de toute autre information. Il doit avoir la possibilité de revenir sur ce choix. Il valide ensuite son choix et cette opération déclenche l’envoi du bulletin de vote dématérialisé vers le serveur des votes. L’électeur doit recevoir immédiatement confirmation de son vote et avoir la possibilité de conserver une trace de cette confirmation.

2. Le chiffrement du bulletin de vote

Le bulletin de vote doit être chiffré par un algorithme public réputé « fort » dès son émission sur le poste de l’électeur et être stocké dans l’urne, en vue du dépouillement, sans avoir été déchiffré à aucun moment, même de manière transitoire. La liaison entre le terminal de vote de l’électeur et le serveur des votes doit faire l’objet d’un chiffrement distinct de celui qui s’applique au bulletin pour assurer la sécurité tant du procédé d’authentification de l’électeur que la confidentialité de son vote. La mise en place du canal de communication doit intégrer une authentification du serveur de vote.

Par ailleurs, le stockage du bulletin dans l’urne ne doit pas comporter d’horodatage, pour éviter tout rapprochement avec la liste d’émargement.

3. L’émargement

L’émargement doit se faire dès la validation du vote de façon à ce qu’un autre vote ne puisse intervenir à partir des éléments d’authentification de l’électeur déjà utilisés. L’émargement comporte un horodatage. Cette liste, aux fins de contrôle de l’émargement, ainsi que le compteur des votes ne doivent être accessibles qu’aux membres du bureau de vote et aux personnes autorisées.

4. Le dépouillement

La fermeture du scrutin doit immédiatement être suivie d’une phase de scellement de l’urne et de la liste d’émargement, phase qui précède le dépouillement. L’ensemble des informations nécessaires à un éventuel contrôle a posteriori doit également être recueilli lors de cette phase. Ces éléments sont enregistrés sur un support scellé, non réinscriptible et probant.

Le dépouillement est actionné par les clés de déchiffrement, remises aux membres du bureau dûment désignés au moment de la génération de ces clés. Les membres du bureau doivent actionner publiquement le processus de dépouillement.

Les décomptes des voix par candidat ou liste de l’élection doivent apparaître lisiblement à l’écran et faire l’objet d’une édition sécurisée, c’est-à-dire d’un mécanisme garantissant que l’affichage et l’impression des résultats correspondent au décompte de l’urne, pour être portés au procès-verbal de l’élection. Le cas échéant, l’envoi des résultats à un bureau centralisateur à distance doit s’effectuer par une liaison sécurisée empêchant toute captation ou modification des résultats.

Le système de vote électronique doit être bloqué après le dépouillement de sorte qu’il soit impossible de reprendre ou de modifier les résultats après la décision de clôture du dépouillement prise par la commission électorale.

III. – Sur le contrôle des opérations de vote a posteriori par le juge électoral

1. Les garanties minimales pour un contrôle a posteriori

Pour les besoins d’audit externe, notamment en cas de contentieux électoral, le système de vote électronique doit être capable de fournir les éléments techniques permettant au minimum de prouver de façon irréfutable que :

* le procédé de scellement est resté intègre durant le scrutin ;
* les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls titulaires ;
* le vote est anonyme ;
* la liste d’émargement ne comprend que la liste des électeurs ayant voté ;
* l’urne dépouillée est bien celle contenant les votes des électeurs et elle ne contient que ces votes ;
* aucun décompte partiel n’a pu être effectué durant le scrutin ;
* la procédure de décompte des votes enregistrés doit pouvoir être déroulée de nouveau.

2. La conservation des données portant sur l’opération électorale

Tous les fichiers supports (copies des programmes sources et exécutables, matériels de vote, fichiers d’émargement, de résultats, sauvegardes) doivent être conservés sous scellés jusqu’à l’épuisement des délais de recours contentieux. Cette conservation doit être assurée sous le contrôle de la commission électorale dans des conditions garantissant le secret du vote. Obligation doit être faite, le cas échéant, au prestataire de service de transférer l’ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation des supports. Lorsqu’aucune action contentieuse n’a été engagée avant l’épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.

IV. – La publication

La présente délibération sera publiée au Journal officiel de la République française.

Le président,

A. TÜRK

**Arrêté du 25 avril 2007 pris en application du décret n° 2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote par voie électronique pour l’élection des délégués du personnel et des représentants du personnel au comité d’entreprise et modifiant le code du travail (deuxième partie : Décrets en Conseil d’Etat)**

Le ministre de l’emploi, de la cohésion sociale et du logement,

Vu le code du travail, et notamment ses articles L. 423-13 et L. 433-9 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés ;

Vu la loi n° 2004-575 du 21 juin 2004 relative à la confiance dans l’économie numérique, notamment son article 54 ;

Vu le décret n° 2007-602 du 25 avril 2007 relatif aux conditions et aux modalités de vote par voie électronique pour l’élection des délégués du personnel et des représentants du personnel au comité d’entreprise et modifiant le code du travail (deuxième partie : Décrets en Conseil d’Etat) ;

Vu l’avis de la Commission nationale de l’informatique et des libertés en date du 14 septembre 2006,

Arrête :

Article 1

En application du décret du 25 avril 2007 susvisé, les élections des délégués du personnel et des représentants du personnel au comité d’entreprise peuvent être organisées par voie électronique sur place ou à distance selon les dispositions techniques de mise en oeuvre et les garanties fixées par le présent arrêté.

Article 2

Le traitement « fichier des électeurs » est établi à partir des listes électorales. Il a pour finalité de délivrer à chaque électeur un moyen d’authentification, d’identifier les électeurs ayant pris part au vote et d’éditer les listes d’émargement. L’émargement indique la date et l’heure du vote. Les listes sont enregistrées sur un support distinct de celui de l’urne électronique, scellé, non réinscriptible, rendant son contenu inaltérable et probant.

Les données du vote font l’objet d’un chiffrement dès l’émission du vote sur le poste de l’électeur.

Le fichier dénommé « contenu de l’urne électronique » recense les votes exprimés par voie électronique. Les données de ce fichier font l’objet d’un chiffrement et ne doivent pas comporter de lien permettant l’identification des électeurs afin de garantir la confidentialité du vote.

Article 3

Les listes électorales sont établies par l’employeur. Le contrôle de la conformité des listes importées sur le système de vote électronique aux listes électorales transmises le cas échéant au prestataire est effectué sous la responsabilité de l’employeur. L’intégration et le contrôle des candidatures sont effectués dans les mêmes conditions.

La mise en oeuvre du système de vote électronique est opérée sous le contrôle effectif, tant au niveau des moyens informatiques centraux que de ceux éventuellement déployés sur place, de représentants de l’organisme mettant en place le vote. Toutes les mesures sont prises pour leur permettre de vérifier l’effectivité des dispositifs de sécurité prévus.

Tout système de vote électronique comporte un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et les mêmes caractéristiques.

En cas de dysfonctionnement informatique résultant d’une attaque du système par un tiers, d’une infection virale, d’une défaillance technique ou d’une altération des données, le bureau de vote a compétence, après avis des représentants susmentionnés, pour prendre toute mesure d’information et de sauvegarde et notamment pour décider la suspension des opérations de vote.

Article 4

Les données devant être enregistrées sont les suivantes :

* pour les listes électorales : noms et prénoms des inscrits, date d’entrée dans l’entreprise, date de naissance, collège ;
* pour le fichier des électeurs : noms, prénoms, collège, moyen d’authentification et, le cas échéant, coordonnées ;
* pour les listes d’émargement : collège, noms et prénoms des électeurs ;
* pour les listes des candidats : collège, noms, prénoms des candidats, titulaires ou suppléants, appartenance syndicale le cas échéant ;
* pour les listes des résultats : noms et prénoms des candidats, élus, non élus, voix obtenues, appartenance syndicale le cas échéant, collège, destinataires mentionnés à l’article 5.

Article 5

Les destinataires ou catégories de destinataires de ces informations sont les suivants :

* pour les listes électorales : électeurs, syndicats représentatifs le cas échéant, agents habilités des services du personnel ;
* pour le fichier des électeurs : électeurs pour les informations les concernant ;
* pour les listes d’émargement : membres des bureaux de vote, agents habilités des services du personnel ;
* pour les listes des candidats : électeurs, syndicats, agents habilités des services du personnel ;
* pour les listes des résultats : électeurs, services du ministère chargé de l’emploi, syndicats, employeurs ou agents habilités des services du personnel.

 En cas de contestation des élections, ces pièces sont tenues à la disposition du juge.

Article 6

Les heures d’ouverture et de fermeture du scrutin électronique doivent pouvoir être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

Pour se connecter sur place ou à distance au système de vote, l’électeur doit se faire connaître par le moyen d’authentification qui lui aura été transmis, selon des modalités garantissant sa confidentialité. Ce moyen d’authentification permettra au serveur de vérifier son identité et garantira l’unicité de son vote. Il est alors impossible à quiconque de voter de nouveau avec les mêmes moyens d’authentification.

L’électeur accède aux listes de candidats et exprime son vote. Son choix doit apparaître clairement à l’écran ; il peut être modifié avant validation. La transmission du vote et l’émargement font l’objet d’un accusé de réception que l’électeur a la possibilité de conserver.

Tout électeur atteint d’une infirmité le mettant dans l’impossibilité de voter peut se faire assister par un électeur de son choix.

Le vote est anonyme et chiffré par le système, avant transmission au fichier « contenu de l’urne électronique » dans les conditions fixées à l’article 2, alinéa 3. La validation le rend définitif et empêche toute modification.

Article 7

Dès la clôture du scrutin, le contenu de l’urne, les listes d’émargement et les états courants gérés par les serveurs sont figés, horodatés et scellés automatiquement sur l’ensemble des serveurs.

Le dépouillement n’est possible que par l’activation conjointe d’au moins deux clés de chiffrement différentes sur les trois qui doivent être éditées.

La génération des clés destinées à permettre le dépouillement des votes à l’issue du scrutin est publique de manière à prouver de façon irréfutable que seuls le président du bureau de vote et deux de ses assesseurs ont connaissance de ces clés à l’exclusion de toute autre personne, y compris du personnel technique chargé du déploiement du système de vote.

Ces deux assesseurs nominativement identifiés, le plus âgé et le plus jeune parmi les assesseurs à défaut d’accord, ainsi que le président du bureau de vote reçoivent chacun une clé de dépouillement distincte, selon des modalités en garantissant la confidentialité, permettant d’accéder aux données du fichier dénommé « contenu de l’urne électronique ». La présence de deux titulaires de ces clés est indispensable pour autoriser le dépouillement. Des clés de sauvegarde sont en outre conservées sous scellés.

Le décompte des voix apparaît lisiblement à l’écran et fait l’objet d’une édition sécurisée afin d’être porté au procès-verbal.

Le système de vote électronique est scellé après le dépouillement afin de garantir l’impossibilité de reprendre ou de modifier les résultats après la décision de clôture du dépouillement. La procédure de décompte des votes enregistrés doit pouvoir être déroulée de nouveau.

Article 8

Le directeur général du travail est chargé de l’exécution du présent arrêté, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 25 avril 2007.

Jean-Louis Borloo