Décision unilatérale portant sur la mise en place du vote électronique pour les élections CSE 2023 au sein de l'UES Orange

16 mars 2023

Préambule

La présente décision unilatérale a pour objet de déterminer le mode de scrutin des élections aux Comités Sociaux Economiques (CSE) au sein de l'UES Orange.

Le cahier des charges relatif à la mise en œuvre du vote électronique figure en annexe 1.

Les modalités d'organisation et le déroulement des opérations électorales dont font partie les modalités de mise en œuvre du vote électronique seront déterminées ultérieurement dans le Protocole d'Accord Préélectoral et à défaut, par décision unilatérale de l'employeur.

Article 1 - Champ d'application

La présente décision unilatérale s'applique aux sociétés et établissements composant l'UES Orange telles que définies dans l'accord du 12 décembre 2022, portant sur le périmètre de l'UES Orange.

Article 2 – Principe de recours au vote électronique

La négociation portant sur la possibilité de recourir à un vote électronique débutée avec les organisations syndicales représentatives de l'UES Orange le 24 janvier 2023 a abouti à la rédaction d'un projet d'accord, mis à la signature le 9 février 2023. Ce projet d'accord n'a pas recueilli les conditions de validité requises.

A défaut d'accord et conformément aux articles L.2314-26 et R.2314-5 du code du travail, le principe du recours au vote électronique dans le cadre des élections CSE 2023 est posé par décision unilatérale.

Le vote électronique est retenu comme modalité exclusive de vote dans le cadre des élections CSE 2023 de l'UES Orange.

Article 3 – Modalités de recours au vote électronique

L'organisation matérielle et technique du processus de vote électronique est confiée par les entreprises composant l'UES Orange à un prestataire indépendant sélectionné par la direction, sur la base d'un cahier des charges, annexé à la présente décision et mis en ligne sur l'intranet, respectant les prescriptions réglementaires fixées notamment aux articles R2314-6 et suivants du code du travail.

Le système de vote retenu pour les élections CSE s'inscrira dans le cadre des principes généraux du droit électoral dont le respect est indispensable à la régularité du scrutin, il s'agit notamment de :

- intégrité du vote : identité entre le vote émis par le/la salarié-e et le vote enregistré ;
- anonymat, sincérité du vote : impossibilité de relier un vote émis à un-e électeur-trice ;
- unicité du vote : impossibilité de voter plusieurs fois pour un même scrutin ;
- confidentialité, secret du vote : exercice du droit de vote sans pression extérieure.

Article 4 : Protection des données personnelles

Les traitements des données personnelles opérés dans le cadre des opérations électorales font l'objet d'une documentation interne d'Orange et d'une information auprès des personnes concernées conformément à la règlementation applicable en matière de protection des données personnelles.

Pour les seules nécessitées des opérations électorales (notamment l'établissement des listes électorales), l'entreprise transmet au prestataire des fichiers établis à partir d'extraction des fichiers de gestion du personnel de l'entreprise de l'entreprise ainsi que de données recueillies auprès des entreprises ayant mis à disposition du personnel remplissant les conditions fixées par l'article L2314-23 du code du travail.

Le prestataire ne traitera les données que sur instruction d'Orange et dans le respect de la règlementation applicable en matière de protection des données personnelles.

Article 5 : Durée de la décision unilatérale et entrée en vigueur

La présente décision unilatérale est prise pour une durée déterminée dans le cadre des élections professionnelles organisées pour la mandature CSE 2023-2027. Elle entre vigueur à la date de sa signature et prendra fin au plus tard aux termes de l'ensemble des mandats issus des scrutins CSE de la mandature 2023-2027.

Fait à Paris, le 16 mars 2023

La Direction pour les sociétés composant l'UES Orange

Signé le 16/03/2023 18:42 par
Eric
BOUSQUET

Eric Bousquet

Directeur des Relations Sociales Groupe

Annexe 1 : Cahier des charges du vote électronique

ELECTIONS CSE 2023

Cahier des charges

de mise en œuvre du vote électronique

Vos contacts pour tous renseignements ou informations complémentaires

Chef de projet élections

Eric BOUSQUET –
Directeur des Relations Sociales du Groupe
Tel : 06 62 92 02 30
Mail : eric.bousquet@orange.com

Equipe projet élections

Cédric CARVALHO
Tel : 06 32 00 78 37
Mail : cedric.carvalho@orange.com

Michèle DILOUYA
Tel : 06 30 51 07 46
Mail : michele.dilouya@orange.com

Marie Juliette FRITZ (Juriste)
Tel : 07 86 50 91 57
Mail : mariejuliette.fritz@orange.com

Magalie DE FLEURY (Juriste)
Tel : 06 73 44 98 57
Mail : magalie.defleury@orange.com

Equipe technique

Marc GOUSPY
Tel : 06 37 55 67 32
Mail : marc.gouspy@orange.com

SOMMAIRE

I - Contexte de mise en œuvre du vote électronique

Dans le cadre de l'organisation des élections pour les Comités Economiques et Sociaux (CSE), Orange souhaite mettre en place une solution de vote par voie électronique sur Internet.

La date des élections sera fixée par voie d'accord pour qu'elles aient lieu dans les 15 jours précédant la date de fin de la mandature 2019-2022, fixée au 3 décembre 2023 inclus**.**

Le vote électronique sera également encadré soit par un accord, soit, à défaut d'accord, par une Décision Unilatérale conformément aux articles L.2314-26 et R.2314-5 du code du travail.

Le prestataire aura en charge, sous le contrôle de la Direction des Relations Sociales du Groupe Orange :

- la conception et la mise en place du système de vote électronique conforme aux dispositions des articles R.2314-5 et suivants du code du travail et à la 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 (pour une élection avec un niveau de risque fixée à 2) ;
- la gestion de la préparation des élections par voie électronique ;
- la mise en œuvre du système de vote électronique conforme aux dispositions des articles R.2314-5 et suivants du code du travail et à la 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 (pour une élection avec un niveau de risque fixée à 2) ;
- la mise en œuvre du système de dépouillement des bulletins de vote électronique et l'élaboration des états des résultats permettant l'affectation des sièges ; conforme aux dispositions des articles R.2314-5 et suivants du code du travail et à la 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 (pour une élection avec un niveau de risque fixée à 2) ;
- la production de l'ensemble des statistiques relatives aux différentes élections.

La prestation confiée par Orange au prestataire fera l'objet d'un contrat de prestations de services entre Orange et le prestataire, conforme aux lois applicables en matière de protection des données.

Dans la mesure où le prestataire intervient en tant que sous-traitant dans la mise en œuvre d'un traitement de données personnelles, ce dernier s'engage à assurer à Orange « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » (article 28 du règlement général sur la protection des données personnelles).

La prestation devra respecter la loi pour une république numérique, conformément au Décret n°2019-768 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne.

II- Caractéristiques des scrutins

Les élections à organiser sont des élections des représentants du personnel pour les Comités Economiques et Sociaux d'Etablissement (CSEE).

Base légale	Art. L2314-4 à L2314-32 du code du travail
Scrutin	Par périmètre d'Etablissement Distinct Scrutin de liste à deux tours avec représentation proportionnelle à la plus forte moyenne (Art. L2414-29)
Périmètre	Périmètre UES Orange (Orange SA, Orange Caraïbe (*) et TOTEM France) (*) (Processus de consultation en cours du projet de fusion d'Orange Caraïbes au sein d'Orange SA)
Nombre d'électeurs	Environ 75 000
Nombre de collège	2 à 3 collèges avec une possibilité de collège unique pour certains scrutins

III - Pilotage du projet

1/ Moyens mis en œuvre

Le prestataire retenu nommera au sein de sa structure un Chef de projet dédié à ces élections qui pilotera la prestation dans sa globalité et qui sera présent du début à la fin du processus. Ce chef de projet sera le correspondant unique de l'équipe projet d'Orange et sera en charge :

- de coordonner l'ensemble des acteurs et assurer la responsabilité de l'interface avec Orange ;
- de répondre en temps réel aux sollicitations de l'équipe projet Orange ;
- d'être force de propositions sur les éventuelles actions à mener tout au long du processus de vote
- de mettre à disposition les moyens humains et matériels nécessaires ;
- d'assurer la tenue du planning et la mise en place du système de vote (adaptation du contexte de l'opération, paramétrage, intégration des données…).

2/ Pilotage en phase de construction/préparation

Le prestataire devra s'assurer du bon déroulement des opérations, notamment :

- dans le respect des délais ;
- en s'assurant de la conformité du résultat par rapport aux exigences spécifiées ;
- avec toutes les garanties de sécurité et de confidentialité ;
- via la mise en place d'un processus de planification, de validation et de contrôle tout au long du projet, assurant une visibilité totale sur l'avancement des travaux et sur la qualité des livrables.

Il sera chargé de planifier une série de points de rencontre avec l'équipe projet Orange au lancement du projet et tout au long du processus, permettant de mesurer le bon déroulement de l'opération.

3/ Bilan de la prestation (qualitatif et quantitatif)

Ce bilan devra permettre d'identifier et expliquer les éventuels écarts de réalisation par rapport au présent cahier des charges, et proposer des actions correctives ou des pistes d'amélioration pour de futures élections.

Il portera sur le déroulé du scrutin ainsi que sur les phases de préparation en amont.

IV – Le système de vote : architecture technique

1/ Sécurisation du système proposé

Le système de vote électronique proposé par le prestataire devra répondre aux exigences décrites ci-après.

a. Principes généraux

Le système doit notamment :

- assurer la confidentialité des données transmises, notamment de celles des fichiers constitués pour établir les listes électorales des collèges électoraux ;
- garantir la sécurisation du vote ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes ;
- permettre que les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement et de déchiffrement et le contenu de l'urne ne soient accessibles qu'aux personnes chargées de la gestion et de la maintenance du système ;
- garantir un chiffrement des données dès l'émission du vote sur le poste de l'électeur ;
- garantir que la liste d'émargement ne soit accessible qu'aux membres du bureau à des fins de contrôle du bon déroulement du scrutin ;
- garantir qu'aucun résultat partiel soit accessible pendant le déroulement du scrutin ;
- garantir que les données relatives aux électeurs inscrits sur les listes électorales et les données relatives au vote soient traités par des systèmes informatiques distincts, dédiés et isolés respectivement nommés fichier électeurs et contenu de l'urne électronique ;
- garantir l'enregistrement des listes d'émargement précisant la date et l'heure du vote sur un support distinct de l'urne électronique, scellée, non réinscriptible rendant son contenu inaltérable et probant ;
- être scellé à l'ouverture du scrutin afin de garantir la non altération des composants constituant la solution de vote (fichiers des électeurs, candidats, scrutins et applications) ;
- être scellé à la clôture du scrutin. 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 ;
- permettre le dépouillement que par activation d'au moins deux clefs de chiffrement différentes sur les trois qui doivent être éditées ;
- prévoir un système de secours susceptible de prendre le relais en cas de panne du système principal ;
- prévoir la conservation sous scellée des fichiers supports comprenant la copie des programmes sources et des programmes exécutables, les matériels de vote, les fichiers d'émargement les fichiers de résultats et de sauvegarde jusqu'à l'expiration du délai de recours ou en cas d'action contentieuse la décision juridictionnelle devenue définitive. Une fois cette période passée, le prestataire doit procéder à la destruction des fichiers supports ;

- mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers) ;
- définir le vote d'un électeur comme une opération atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé ;
- authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduit de manière significative ;
- assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant ;
- assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport ;
- assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement ;
- assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute la durée du traitement ;
- renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé ;
- définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin ;
- assurer l'intégrité du système, de l'urne et de la liste d'émargement ;
- s'assurer que le dépouillement de l'urne puisse être vérifié a posteriori ;
- assurer une haute disponibilité de la solution ;
- assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement ;
- permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin ;
- authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative ;
- assurer un cloisonnement logique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours ;
- utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI ;
- assurer la transparence de l'urne pour tous les électeurs ;

En tout état de cause, la solution devra être totalement conforme aux objectifs de sécurité de la recommandation CNIL pour un risque de niveau 2.

b. Respect de la règlementation sur la protection des données personnelles

Pour les seules nécessitées des opérations électorales (notamment l'établissement des listes électorales), l'entreprise sera amenée à transmettre au prestataire des fichiers établis à partir d'extractions des fichiers de gestion du personnel de l'entreprise.

Les traitements des données personnelles opérés dans le cadre des opérations électorales feront l'objet d'une documentation interne d'Orange, conformément à la règlementation applicable en matière de protection des données personnelles.

Il est également demandé que le système intègre les recommandations de la CNIL de niveau 2 présentées en annexe. Une analyse d'impact (PIA) visée à l'article 35 du Règlement sur la protection des données sera conduite. Dans ce cadre, le prestataire pourra être sollicité par l'équipe projet d'Orange.

c. Fourniture d'un rapport d'expertise

Avec la réponse à la présente consultation, le prestataire fournira à Orange les conclusions du rapport d'expertise de son système de vote électronique, réalisé par un expert indépendant. Cet expert indépendant 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 une formation certifiée portant sur la protection des données pour le vote électronique.

Le prestataire devra permettre la réalisation d'une expertise indépendante complémentaire réalisée nécessairement après la dernière modification substantielle de la conception du système de vote, tel qu'il sera mis en œuvre pour le scrutin Orange dans le cadre du processus de vote. L'expertise réalisée doit avoir procédé au minimum à la vérification du respect par le système de vote des articles R.2314-5 à R.2314-8 du code du travail. Cela recouvre notamment le fait qu'il existe un cahier des charges qui respecte les articles R.2314-6 et suivants, la confidentialité et la sécurité du dispositif, l'accessibilité aux données et la présence de fichiers dédiés.

En complément, dans le cas où Orange déciderait de faire réaliser sa propre expertise indépendante, le prestataire s'engage à donner accès à l'ensemble des informations nécessaires pour la réalisation d'une expertise par un expert indépendant de la solution de vote conformément à la délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique.

L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), la constitution des listes d'électeurs et leur enrôlement, 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 éléments décrits dans la délibération et notamment sur :

- le code source correspondant à la version du logiciel effectivement mise en œuvre ;
- les mécanismes de scellement utilisés aux différentes étapes du scrutin ;
- le système informatique sur lequel le vote va se dérouler ;
- les échanges réseau ;
- les mécanismes de chiffrement utilisés, notamment pour le chiffrement du bulletin de vote ;
- les mécanismes d'authentification des électeurs et la transmission des secrets à ces derniers ;

- l'évaluation du niveau de risque du scrutin ;
- la pertinence et l'effectivité des solutions apportées par la solution de vote aux objectifs de sécurité.

L'expertise doit porter sur l'ensemble des éléments constituant la solution de vote.

Le scrutin présentant un niveau de risque 2 l'expert réalise des audits sur la plateforme, afin de s'assurer de la cohérence et de l'effectivité des solutions apportées, par le biais de tests d'intrusions notamment. L'ensemble des opérations effectuées dans ce cadre est annexé au rapport d'expertise.

Le rapport d'expertise, et ses annexes seront remis au responsable de traitement et au prestataire de solution de vote par correspondance électronique via Internet.

L'expert fournira 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 seront décrits dans le rapport d'expertise.

L'expert ayant accès à des informations sensibles relatives aux solutions dont il est chargé d'évaluer la conformité, notamment le code source des applications, il sera tenu de prendre toutes dispositions et précautions utilises afin de protéger les éléments qui sont portés à sa connaissance, notamment en limitant autant que possible les reproductions de code source au sein du rapport, en conservant ses rapports au sein d'espaces sécurisés dédiés et en ne conservant pas les éléments portés à sa connaissance au-delà de la durée nécessaire.

Le prestataire s'engage à tenir à la disposition de la CNIL le cas échéant tout rapport d'expertise relatif au système de vote destinées à vérifier le respect des articles R.2314-5 à R.2314-9 du code du travail.

2/ Système de vote électronique distant

Le système de vote électronique sera hébergé (en France) chez le prestataire externe ou chez un fournisseur d'hébergement et sera rendu accessible aux électeurs de manière sécurisée.

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.

Le prestataire devra garantir que toutes les mesures physiques seront 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. En particulier, le prestataire devra répondre aux exigences liées à la sécurité des données personnelles définies : par les autorités (CNIL, ANSSI …) par Orange et par l'audit réalisé. Les données échangées entre le prestataire et Orange seront transmises par un système d'échange sécurisé.

Les algorithmes de chiffrement et de signature électronique devront être des algorithmes publics réputés « forts ». Si un système matériel permet d'héberger plusieurs scrutins, il devra être mis en œuvre une solution technique 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.

Le prestataire s'engage à répondre aux exigences de la politique de Sécurité d'Orange conformément à la fiche ISA (jointe en annexe).

En plus de l'expertise indépendante pourra être commanditée par Orange, Orange pourra par ailleurs réaliser, si nécessaire :

- une analyse de risques sécurité ;
- des tests d'intrusions web sur le service ;
- un audit système ou de configuration des serveurs qui hébergent le service.

3/ Disponibilité du système de vote électronique

Le prestataire assurera la mise en ligne du système de vote électronique durant la période des élections. Durant cette période, le système sera disponible 24h/24.

Le prestataire mettra en œuvre les moyens d'assurer un service continu, sans rupture, en prévoyant un nombre de connections simultanées suffisamment dimensionné avec un **minimum de 10 000 connections simultanées** et des dispositifs de gestion des débordements pour garantir une expérience utilisateur de qualité sur la totalité de la période de vote.

En cas d'indisponibilité du site de vote ou dysfonctionnement, le système de vote doit permettre de mettre en œuvre une mesure de suspension ou de prorogation du scrutin égale à la durée constatée. Une procédure spécifique doit alors être prévue dans la solution pour permettre la prorogation, en ne levant que les scellés liés à la date de clôture.

La décision de mettre en œuvre cette mesure étant de la prérogative du bureau de vote.

4/ Accessibilité

a. Compatibilité des terminaux

Le prestataire s'assurera que le site de vote soit bien accessible via l'ensemble des outils à disposition des salariés (PC professionnel et personnel, tablette, Smartphone…) mais également avec le respect des normes d'accessibilité, notamment pour les personnes en situation de handicap (ex. malvoyants, non-voyants, handicap moteur).

Le service devra au minimum être compatible avec les spécifications minimales

- Windows 8 et navigateur Firefox ESR 32 ;
- Android 4.3.1 et navigateur Firefox 27.

b. Respect des normes d'accessibilité numérique

Le prestataire s'assurera que le respect des normes d'accessibilité numérique, pour les personnes en situation de handicap, soit pris en compte.

Le prestataire devra se référer à l'annexe accessibilité jointe au présent document.

L'ensemble des contenus numériques fourni par le prestataire devront répondre aux exigences d'accessibilité :

- Site de communication ainsi que les vidéos
- E-mail de sollicitation : l'ensemble des e-mails envoyés aux votants, du 1er jusqu'au mail de confirmation
- Site de vote : le site de démonstration et le site de production devront être identiques et accessibles. Si un mécanisme de CAPTCHA est mis en place, ce dernier devra respecter les normes d'accessibilité citées en annexe.

Conformément à la loi, le site devra afficher une déclaration d'accessibilité qui affiche le taux de conformité à la norme. Orange impose une présentation pour ces déclarations (exemple : https://www.orange.fr/accessibilite?url=app.visualvoicemail.android.orange.fr) et propose une méthode appelée la Va11ydette (https://la-va11ydette.orange.com/?list=wcag-web&lang=fr). Cette déclaration sera de préférence réalisée par le prestataire puis vérifiée par le centre de compétences accessibilité d'Orange. Elle doit être accessible via un lien « accessibilité » dans le pied de page du site. Tout nouveau site doit être proche d'une conformité à 100%.

5/ Accès aux informations sur les matériels et dans les locaux du prestataire

Le prestataire indiquera comment sont protégés :

- les locaux d'hébergement des matériels sur lesquels sont stockés les fichiers sensibles tels que le fichier des électeurs, les urnes électroniques et les émargements ;
- de manière générale, les informations liées à la gestion des élections d'Orange.

Le système de vote est hébergé en France.

V – Préparation des élections

1/ Contribution du prestataire aux modalités d'organisation des élections

Le prestataire fournira soutien et conseil tout au long des différentes phases du processus électoral. Il devra notamment être attentif et intégrer dans la solution de vote fournie sur toutes les dispositions prévues dans le protocole d'accord préélectoral.

Le prestataire s'engage par ailleurs à fournir un accompagnement via des préconisations et argumentations sur les solutions retenues lors de l'élaboration des modalités électorales au travers notamment de :

- propositions de documents types : courriers, notices de vote… ;
- arguments sur éléments techniques liés au site de vote : taille maximum des logos, visibilité de tous les logos sur une seule et même page, navigation au sein du site de vote…. ;
- éléments liés au vote lui-même : modalités d'envoi des codes, modalités de validation des votes…… ;

- proposition d'un espace de communication sur le site de vote : son organisation, élaboration d'une vidéo, affichage des listes et conception push mail (HTML).

Le prestataire s'engage à signaler par écrit à l'équipe projet sous 48 heures à compter de la réception des différents documents communiqués par Orange les questionnements et ou les éventuelles incompatibilités avec le système de vote.

A défaut de réponse dans les 48 heures, les fonctionnalités et modalités inscrites dans les documents fournis seront réputées compatibles avec le système de vote proposé par le prestataire.

Le prestataire fera une présentation du système de vote aux Organisations Syndicales.

Le prestataire s'engage à fournir une notice d'information comportant une description détaillée du système de vote et du déroulement des opérations électorales.

Le prestataire s'engage enfin à ce que le système de vote électronique proposé soit conforme à l'ensemble des exigences légales et règlementaires en vigueur.

2/ Phase de test et de recette du système de vote électronique

Le prestataire devra proposer les moyens de tester l'ensemble des scénarios durant une période prévue dans un calendrier de préparation des élections.

Cette période de test sera déterminée d'un commun accord entre Orange et le prestataire. Elle sera prévue à l'issue de la phase de paramétrage et de préparation du système de vote électronique.

Les fichiers de données de tests fournis par Orange pour la recette seront :

- Organisation
- Electeurs CSEE

En aucun cas, Orange ne peut s'engager à fournir les fichiers de données réels, définitifs et complets pour la phase de recette. Les électeurs et les candidats du jeu de données seront constituées de données fictives. Le jeu de données pour la recette sera néanmoins représentatif en termes de volumétrie.

Les tests programmés dans cette phase permettront notamment de contrôler le déroulement et la conformité du scénario de vote pour chaque élection.

Le prestataire fournira à l'issue de chaque phase de tests un rapport détaillé du déroulement et résultats de tests précisant tous les éléments nécessaires (description des plateformes, jeux de données utilisés, description des scénarios de tests, …) et permettant de qualifier les résultats obtenus.

3/ Listes électorales

Le système retenu garantit la confidentialité des données transmises par Orange au prestataire, notamment celle des fichiers constitués pour établir les listes électorales ainsi que la sécurité de

l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes.

Les moyens d'authentifications devront être adressés aux électeurs par deux canaux distincts.

a. Constitution des fichiers

Les listes électorales sont constituées par Orange. Elles comportent les informations nominatives des électeurs ayant la possibilité de participer aux élections. Elles sont établies par collège et par Etablissement Distinct.

La description de l'organisation en Etablissement Distinct sera fournie au prestataire.

Elles seront transmises au prestataire par transfert sécurisé à partir d'un outil interne à Orange.

Une fois fiabilisées, les listes électorales doivent permettre :

- d'éditer les listes électorales à afficher par Etablissement Distinct et par collège;
- d'attribuer à chaque électeur autorisé des codes d'authentification pour accéder au système de vote électronique pour chaque électeur autorisé ;
- de contrôler les accès au système de vote électronique ;
- d'enregistrer les émargements électroniques après chaque vote et assurer l'unicité du vote pour chaque électeur ;
- d'éditer les listes d'émargement ;
- d'envoyer les différents courriers et pushmails.

Pour tout fichier transmis et après injection dans le système de vote, le prestataire devra s'assurer de la fiabilité et de la conformité des données injectées par lui dans le système de vote par rapport aux données transmises par Orange.

Un exemple de ces fichiers sera fourni par Orange au prestataire pour la réalisation de tests.

b. Confidentialité des fichiers

Le prestataire s'engagera à conserver de manière confidentielle toutes les informations et les données qui lui seront transmises pour les besoins de gestion du vote électronique. Il mettra en œuvre tous les moyens nécessaires afin de sécuriser l'accès aux informations de ce fichier sur ses propres systèmes et à strictement limiter leur consultation aux seuls personnels chargés de la gestion et de la maintenance du vote électronique

c. Mise à jour des listes électorales

Les listes électorales pourront subir des modifications jusqu'au scellement des urnes notamment pour la suppression ou l'ajout d'électeurs.

Pendant toute l'ouverture de la plateforme hébergeant les listes électorales et jusqu'au scellement, le prestataire devra s'assurer qu'Orange puisse :

- consulter les listes électorales et les données électeurs ;
- modifier par IHM et par import de fichier des données électeurs, y compris le collège électoral, et le positionnement de l'électeur dans l'organisation ;

- extraire les listes électorales.

Les modifications des données salariés seront traitées par la Direction des Relations Sociales Groupe.

Lorsque les modifications sont réalisées après l'affichage des listes électorales définitives, le prestataire devra s'assurer que les codes d'accès fournis à des électeurs supprimés des listes soient invalidés, et que les nouveaux électeurs inscrits sur les listes puissent disposer dans un temps utile la notice d'information sur les opérations électorales, des codes d'authentification et des accès nécessaires à leur participation effective au vote électronique.

d. Accès aux listes électorales sur le site de gestion de l'organisateur du scrutin

Le prestataire devra permettre à Orange d'accéder aux listes électorales dès leur injection dans le site de supervision jusqu'à la fin des délais de recours légaux ou, lorsqu'une action contentieuse a été engagée, après l'intervention d'une décision juridictionnelle devenue définitive.

Différents profils d'utilisateurs seront définis et communiqués par Orange, auxquels seront associés des droits différents.

Le prestataire devra notamment prévoir d'ouvrir le site de supervision avant la publication des listes électorales provisoires, afin de permettre un accès restreint aux listes électorales :

- la fiche électeur devra être masquée ;
- les utilisateurs pourront faire des recherches et des tris ;
- le téléchargement de ces listes électorales ne sera pas possible.

Le prestataire devra garantir un volume de connexions à plus de 1 000 utilisateurs (sous réserve de contrainte technique).m

4/ Liste de candidats

a. Constitution des fichiers

Les listes de candidats sont constituées par les organisations syndicales au sein de l'UES au 1er tour. La constitution de listes de candidats étant libre au 2nd tour, les listes peuvent être constituées par toute personne remplissant les conditions posées par le législateur.

b. Injection des fichiers dans le système de vote

Les listes de candidats seront transmises au prestataire par transfert sécurisé en vue de leur implémentation automatique dans le système de vote électronique afin d'éviter toute saisie manuelle.

Dès lors que les fichiers fiabilisés lui seront transmis et après injection par lui dans le système de vote, le prestataire devra s'assurer de la fiabilité et de la conformité des données injectées par rapport aux données transmises par Orange.

Orange sera responsable de la qualité des référentiels de données métier fournies en amont pour alimenter la solution de vote en ligne du prestataire.

Le prestataire sera garant et responsable de la qualité des traitements qu'il réalise sur ces données à des fins de paramétrage ou d'initialisation de sa solution de vote :

- le prestataire devra mettre en place des tests de vérification de la complétude et de l'exactitude des données injectées dans la solution sur la base du référentiel de données fournies par Orange ;
- le prestataire devra préciser les moyens et les phases du projet prévus pour réaliser ces tests.

Si une anomalie détectée est liée à la qualité des données contenues dans les fichiers fournis par Orange, alors Orange est responsable de cette anomalie. A l'inverse, si l'anomalie détectée est liée à la qualité des traitements faits sur les données par le prestataire, ce dernier est responsable de cette anomalie.

Le prestataire devra également s'assurer que les logos et professions de foi sont bien affichés dans l'ordre du tirage au sort transmis par Orange et rattachés aux listes correspondantes.

Un fichier sera fourni par Orange au prestataire pour la réalisation de tests.

Le prestataire devra prévoir un temps pour permettre aux organisations syndicales de contrôler la fiabilité, la cohérence et l'affichage des données à publier.

c. Format des fichiers

Le format des listes de candidats pour chacun des scrutins sera transmis au prestataire.

5/ Génération et envoi des informations relatives aux élections

a. Courriers et push mails

A partir des référentiels de données fournies par Orange, le prestataire assurera la réalisation et la transmission à chaque électeur des éléments suivants :

- une lettre d'annonce des élections contenant un extrait des listes électorales de chaque salarié pour contrôle et validation ;
- les modalités de connexion de vote par internet (code d'accès) accompagné de la notice de vote d'information détaillée sur le déroulement des opérations électorales ;
- un lien vers l'espace de communication des élections Orange ;
- les professions de foi ;
- l'annonce de l'ouverture du processus électoral et les relances.

La transmission de ces informations pourra se faire selon les options qui seront retenues dans les modalités électorales :

- sous format électronique ;
- sous format papier.

Pour l'envoi des courriers sous format papier, le prestataire devra respecter un délai maximum de 15 jours à compter de l'envoi des fichiers par Orange (vérification, impression et envoi des courriers).

Pour chacun de ces envois, l'électeur ne devra avoir accès qu'aux données et professions de foi qui le concerne, sauf pour les listes électorales.

b. Codes d'accès au système de vote électronique

Chaque électeur recevra de manière sécurisée :

- un identifiant unique d'accès qui permettra, outre le contrôle d'accès, la tenue des listes d'émargement électroniques garantes de l'unicité des votes ;
- un mot de passe qu'il sera seul à connaître, ce code sera unique pour valider chacun des votes sur chacun des scrutins auquel l'électeur sera amené à participer.

L'envoi de l'identifiant et du code d'accès doivent se faire impérativement par deux canaux différents.

Dans le respect de l'anonymat, le prestataire proposera des procédures de génération et de transmission des codes d'accès aux électeurs permettant de conserver le caractère confidentiel du mot de passe durant toutes les étapes.

Ainsi en cas de perte de ses codes de votes, un électeur aura la possibilité d'en demander des nouveaux en ligne via un espace sécurisé.

Les nouveaux codes seront transmis à l'électeur par mail ou SMS. En cas de problème de réception, le prestataire devra proposer une solution alternative permettant à l'électeur de pouvoir voter tout en garantissant la sincérité du vote.

Le prestataire devra proposer des solutions de contrôle.

En tout état de cause, le système retenu assurera la confidentialité des données transmises à chaque étape du processus ainsi que la sécurité de l'adressage des moyens d'authentification.

6/ Espace de communication

a. Contenu de l'espace de communication

Au sein du site de vote, se trouvera également un espace de communication paramétré par le prestataire intégrant les communications de la Direction ainsi que celles des différentes organisations syndicales, avec une visibilité de tous les logos sur une seule et même page.

Chaque électeur pourra y trouver l'ensemble des informations relatives aux différents scrutins (dates des élections et nature des scrutins) mais également l'ensemble des professions de foi relatives aux scrutins qui le concernent.

Il aura également à sa disposition :

- une vidéo réalisée par le prestataire pour permettre à l'électeur d'appréhender le fonctionnement de la solution de vote ;
- un site de démonstration pour permettre à chaque électeur de tester le dispositif de vote dans des conditions réelles.
- les listes électorales ;
- les listes de candidats.

b. Accès aux listes électorales

Le prestataire assure un accès sécurisé aux listes électorales provisoires à tous les salariés, même s'ils ne figurent pas sur les listes électorales en créant un code d'accès générique par Etablissement Distinct par exemple.

Le prestataire assure un accès sécurisé aux listes électorales définitives et restreint aux électeurs.

En tout état de cause, les listes électorales doivent pouvoir être visionnées sans être téléchargées. Les listes visionnées doivent être publiées dans un format empêchant la reproduction (ex. protection contre le copier-coller).

7/ Formation

Le prestataire proposera et dispensera une formation sur système de vote à l'ensemble des membres des bureaux de vote tels que défini dans les modalités de vote ainsi qu'aux membres des équipes projet élections de la Direction Orange sur plusieurs sessions.

VI- Le vote

1/ Organisation des bureaux de vote

Dans le cadre des opérations électorales électronique, il devra y avoir un bureau de vote électronique (BVE) centralisateur CSE et un BVE au niveau de chaque Établissement Distinct.

Le BVE centralisateur déverrouille, donne l'autorisation de dépouiller aux BVE Établissements Distincts et supervise le dépouillement des urnes CSEE de l'ensemble de l'UES. Il centralise les résultats des urnes salariés de droit privé et signe les PV.

Les BVE au sein des Établissements Distincts les urnes CSE de l'Établissement Distinct concerné.

2/ Scellement des urnes

Le prestataire s'engage à participer à la réunion de scellement des urnes en présence des représentants des listes de candidats (délégués de listes) et de la direction afin de réaliser les actions suivantes :

- 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 clefs délivrées à cet effet ;
- procède avant que le vote doit ouvert à un test spécifique du système de dépouillement à l'issue duquel le système est scellé ;
- contrôle à l'issue des opérations de vote et avant les opérations de dépouillement le scellement de ce système.

Le système de vote électronique doit être scellé à l'ouverture et à la clôture du scrutin. Le contrôle du scellement doit pouvoir être effectué à tout moment durant la période de vote par les membres du bureau de vote centralisateur, tel que défini dans le protocole d'accord préélectoral.

Ce système pourra être scellé en présence d'huissiers. La procédure de scellement devra être clairement exposée en amont et être scrupuleusement respectée.

Lors de la procédure de scellement, il sera réalisé un scrutin à blanc, sur au minimum 3 Etablissements Distincts comportant au moins 3 salariés de chaque collège par scrutin.

Le scrutin à blanc vise à contrôler et valider les scénariis d'élections et la bonne intégration des listes de candidats et des professions de foi.

Il doit être effectué sur le système de vote électronique définitif et validé préalablement, afin de permettre aux membres du bureau de vote centralisateur de contrôler la conformité du système de vote électronique avant l'ouverture effective des élections.

Le « scrutin à blanc » vise à tester l'application en fonctionnement réel. Durant cette phase, les membres du bureau de vote centralisateur pourront tester toutes les phases de vote des élections.

Pour ce faire, les membres des bureaux de vote ouvriront les scrutins, effectueront des votes, fermeront les scrutins et dépouilleront les votes effectués.

Au terme de ce test, les membres des bureaux de vote valideront l'intégrité du dispositif.

Tout au long du scrutin, le contrôle du scellement permettra aux membres du bureau de vote centralisateur de s'assurer que l'application n'a été sujette à aucune intrusion.

Les étapes de contrôle seront les suivantes :

- création de 3 clés qui permettront le chiffrement des bulletins de vote dans le système de vote électronique du prestataire. Seules 2 de ces clés seront nécessaires au dépouillement ;
- ouverture des élections ;
- réalisation de plusieurs votes ;
- clôture des élections ;
- remise des clés aux membres du bureau de vote centralisateur permettant le déchiffrement des bulletins de vote. Ces clés pourront ensuite être remises pour conservation jusqu'au jour du dépouillement à un ou plusieurs huissiers ;
- déroulement du dépouillement des urnes électroniques et édition des résultats ;
- contrôles de la conformité des résultats obtenus ;
- scellement de l'application de vote électronique.

Un mode en distanciel sera prévu si besoin (dont les modalités de mise en œuvre devront être précisées par le prestataire).

Une fois le scellement définitif réalisé, un PV de scellement sera généré. Ce PV sera signé par les membres du bureau de vote centralisateur.

3/ Durée du vote

La durée de vote des deux tours de scrutin sera déterminée dans l'accord portant sur la date des élections CSE 2023 au sein de l'UES Orange.

Ces élections auront lieu dans les 15 jours précédant la date de fin de la mandature 2019-2022, fixée au 3 décembre 2023 inclus.

4/ Vote électronique

a. Chiffrement des bulletins de vote dans l'urne électronique

Lors de l'élection par vote électronique, les fichiers comportant les éléments d'authentification des électeurs et le contenu de l'urne sont uniquement accessibles aux personnes chargées de la gestion et de la maintenance du système. A l'inverse, les clés de déchiffrement ne sont pas accessibles par les personnes chargées de la gestion et de la maintenance mais uniquement par les porteurs membres du bureau de vote électronique centralisateur.

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 ».

Les bulletins de vote enregistrés dans le système de vote électronique doivent être chiffrés avec algorithme « fort ». Le déchiffrement des bulletins sera assuré par une clé générée par le système de vote et dont les fragments seront confiées lors du scellement au porteurs (membres du bureaux de vote centralisateur) et supprimées des serveurs après leur génération. Ces fragments de clés ou les mots de passe qui les protègent pourront être remis à un ou deux huissier(s) de justice. Dans le cadre d'un recours éventuel au distenciel, le prestataire proposera une modalité de transmission sécurisée aux huissiers.

b. Dispositifs de secours

Le système de vote électronique sera dupliqué sur 2 plateformes distinctes hébergées en France.

En cas de panne d'un des systèmes, un dispositif de secours prendra le relais en 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 centralisateur aura compétence, pour prendre toute mesure d'information et de sauvegarde et notamment pour décider la suspension des opérations de vote.

c. Scenario de vote

Le scénario de vote électronique comportera les étapes suivantes pour chaque scrutin :

- une étape d'identification de l'électeur ;
- une étape de présentation des scrutins ;
- une étape de présentation des listes de candidatures en présence ;

- la possibilité pour l'électeur de consulter les professions de foi de toutes les listes liées au scrutin sur lequel il a entamé le processus de vote ;
- le choix par l'électeur d'une seule liste parmi celles proposées, ou bien le choix de voter « blanc » ;
- la présentation du bulletin de vote définitif comprenant les candidats ;
- en cas de rature ou de décochage d'un ou plusieurs candidats sur le bulletin de vote, l'électeur sera alerté par une fenêtre « pop up » lui permettant de confirmer son ou ses choix pour les candidats concernés ;
- la confirmation par l'électeur du choix effectué via la saisie de son mot de passe pour chaque vote ;
- la confirmation à l'électeur par le système de la prise en compte de son bulletin de vote ;
- la possibilité pour l'électeur d'imprimer un accusé de réception confirmant l'enregistrement de son vote et attestant de la prise en compte de ses suffrages par le système de vote. Cette possibilité lui sera offerte à l'issue de la séquence de vote mais aussi ultérieurement, en se reconnectant à l'application. Il mentionnera les élections concernées ainsi que la date et l'heure d'émission de chaque suffrage. Cet accusé de réception comportera une marque d'authentification interdisant une édition frauduleuse.

d. Enchaînement des élections

Le système de vote proposera automatiquement à l'électeur de poursuivre le déroulement du scénario afin de réaliser le vote suivant sur le même site. L'électeur pourra se connecter tant qu'il n'aura pas épuisé les votes qui lui sont proposés.

L'électeur ne doit voir que les scrutins (Titulaires/Suppléants de son Etablissement Distinct et de son collège) pour lesquels il est concerné.

e. Emargement électronique, unicité du vote

Par ailleurs, le système de vote électronique enregistrera un émargement après confirmation du vote par l'électeur, via la saisie de son mot de passe, et ne permettra plus à ce dernier d'effectuer un nouveau vote pour cette même élection (unicité du vote).

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.

La liste d'émargement comprendra :

- les noms et prénoms des électeurs ;
- le libellé du scrutin (1er ou 2nd tour) ;
- le collège de l'électeur ;
- l'heure.

Les listes d'émargement seront disponibles en lecture sans possibilité de téléchargement pendant le scrutin et seront mise à jour toutes les heures. Les qualités des personnes qui auront accès à celles-ci seront définies dans le protocole d'accord préélectoral.

Le prestataire s'engage à mettre en place un CAPTCHA pour déceler tout chargement de données en fort volume.

f. Taux de participation

Le prestataire fournira un taux de participation de façon dynamique à la maille de chaque Etablissement Distinct pour chaque scrutin.

5/ Assistance technique

Durant le scrutin, un interlocuteur dédié du prestataire se tiendra en permanence à la disposition des représentants de la direction et des membres du bureau de vote national et assurera également la surveillance du système de vote électronique.

6/ Assistance téléphonique salariés

Un service d'assistance téléphonique (hotline salarié) sera mis en œuvre, avant et pendant les opérations électorales, dans le but de renseigner les électeurs mais également pour traiter les réclamations.

Cette hotline devra être suffisamment dimensionnée pour gérer l'ensemble des flux d'appels sur toute la durée du vote. Elle devra pouvoir être instantanément redimensionnée en cas d'incident amenant un flux d'appels important ponctuel.

Orange fournira au prestataire un modèle de fichier pour les réclamations.

VII – Dépouillement et résultats

1/ Dépouillement des urnes électroniques et déchiffrement des bulletins de vote

Le dépouillement s'effectuera après la clôture des scrutins et ne pourra commencer qu'une fois les fragments de clés de déchiffrement entrées par 2 membres du bureau de vote centralisateur. Lors de la cérémonie de dépouillement, le président puis les assesseurs, via un poste connecté à internet, introduisent leurs clés de déchiffrement et saisissent le mot de passe associé.

Ceci aura pour but de déverrouiller les urnes et ainsi avoir accès à :

- l'édition des résultats des élections ;
- la remise par le prestataire des procès-verbaux complétés et conformes aux modèles CERFA. Chaque CERFA devra mentionner tous les numéros de SIRET des établissements rattachés à l'Etablissement Distinct.

L'ensemble des étapes décrites ci-dessus seront être réalisées en présence d'Huissiers.

2/ Remise des résultats

Les résultats seront consultables dès le dépouillement des urnes électroniques.

Seuls les membres désignés du bureau de vote ainsi que les représentants de l'employeur habilités auront accès à ces résultats.

3/ Données à fournir à l'issue de la consolidation des résultats

a. Les résultats

Les fichiers de résultats comporteront à minima :

- le décompte des voix par élection ;
- le nombre d'électeurs inscrits ;
- le nombre de votants ;
- le nombre de bulletin blancs ou nuls ;
- le nombre de suffrages valablement exprimés,
- le nombre de voix obtenu par chaque liste ;
- la représentativité de chaque organisation syndicale.

A l'issue des négociations préélectorales les données produites pourront être enrichies.

b. Procès-verbaux des élections

Les Procès-verbaux qui doivent être conformes aux prescriptions légales pourront être édités par Orange depuis la solution de vote. Les résultats y seront affichés et classés selon un ordre défini en amont par tirage au sort.

Ils seront mis à disposition d'Orange par le prestataire.

En complément, pour le premier tour des élections CSE titulaires uniquement, il sera distingué au sein d'urnes séparées les votes des salariés de droits privés et ceux des fonctionnaires pour la représentativité calculée au niveau de la branche des télécoms. Les PV des résultats du scrutin des seuls salariés de droit privés aux élections professionnelles CSE de l'UES Orange par établissement et par collège sera mis à disposition des membres du bureau de vote centralisateur pour signature.

.

c. Listes d'émargement

Les listes d'émargement définitives pourront être éditées par Orange à l'issue des élections et seront accessibles en cours de scrutin par les membres du bureau de vote et les délégués de liste à des fins exclusives de contrôle du déroulement du scrutin. Aucun téléchargement de ces listes d'émargement ne sera rendu possible.

VIII – Archivage, conservation et destruction des données

Le prestataire conservera les fichiers supports (comprenant la copie des programmes sources et des programmes exécutables, les listes électorales, les matériels de vote, les fichiers d'émargement, de résultats et de sauvegarde), jusqu'à l'expiration du délai de recours ou lorsqu'une action contentieuse est engagée après qu'une décision juridictionnelle soit devenue définitive. A l'expiration de ces délais, le prestataire s'engagera à détruire tous les fichiers et à ne conserver aucune de ses données suite à une demande explicite du représentant d'Orange.
Le prestataire fournira à Orange sans délai à l'issue de cette procédure, un certificat de suppression des données.

Le prestataire fournira également sur support numérique une copie intégrale des résultats.

- Cahier des charges de l’accessibilité numérique S3F0

Cahier des Charges de l'accessibilité numérique S3F0

Introduction

La loi pour une république numérique de 2016 et le décret 2019-768 publié en juillet 2019 imposent aux entreprises dont le chiffre d'affaires annuel est d'au moins 250 millions d'euros de proposer des services numériques accessibles, engagement décrit dans le schéma pluri-annuel d'amélioration de l'accessibilité d'Orange.

L'accessibilité numérique consiste à fournir des produits ou services pouvant être utilisés par tous, sans distinction de situation ou de handicap.
Elle concerne l'ensemble des technologies de l'information et de la communication. Elle couvre différentes technologies comme le Web, les applications mobiles, les vidéos, les documents Office et PDF, la télévision numérique et les objets connectés, et ceci quel que soit le support (ordinateur, tablette, mobile…) ou le domaine (site commercial, e-learning, Intranet d'entreprise, progiciel RH ou financier, outil collaboratif…). Ce périmètre suit les évolutions des services et des technologies numériques.
L'accessibilité numérique s'intéresse à tous les handicaps qui affectent l'accès au numérique, ce qui inclut les utilisateurs ayant une déficience visuelle, auditive, motrice, de parole, cognitive...

Objectif d'accessibilité du groupe Orange

Concernant les contenus Web, quels que soient le support (ordinateur, mobile, tablette, TV…) et la technologie, l'objectif d'accessibilité du groupe est le respect du **niveau AA des Web Content Accessibility Guidelines* (WCAG) version 2.1**. Ces contenus doivent en outre ne montrer aucun point bloquant du point de vue d'un utilisateur en situation de handicap.

(*) Le World Wide Web Consortium (W3C) a lancé en 1996 l'initiative pour l'accessibilité du Web (Web Accessibility Initiative - WAI) pour améliorer l'accessibilité des contenus Web. La WAI a émis des recommandations nommées « règles d'accessibilité pour les contenus Web » ou WCAG (pour l'anglais Web Content Accessibility Guidelines), actuellement en version 2.1, qui constituent le standard international.

Référentiel

Le standard WCAG 2.1 est disponible en ligne sur le site du W3C.

Orange a créé un site de recommandations dans l'objectif de faciliter l'accès aux standards ou aux bonnes pratiques. Le site des recommandations accessibilité Orange propose des ressources pédagogiques, des exemples, une méthode de tests et une liste d'outils qui facilitent la prise en compte de l'accessibilité numérique. Ce site évolue régulièrement pour suivre l'évolution des technologies.

Exemple d'exigences fonctionnelles :

Voici un sous ensemble des exigences du référentiel WGAC 2.1 :

- Pertinence de l'information
  - Images : toujours fournir une description textuelle pertinente
    - Icônes de candidats : s'assurer qu'elles sont complètes
    - Syndicats : pas d'intitulé pour le logo
  - Titres des pages : désambiguïser les titres pour qu'on sache exactement à quel endroit du parcours on est
  - Toujours expliciter le contenu d'une iframe à l'aide de l'attribut title sur la balise iframe.
- Formulaires
  - Indiquer explicitement quels champs sont obligatoires
  - Regrouper les boutons radio
- Navigation au clavier
  - Sauf difficulté exceptionnelle, ne pas ajouter d'attribut tabindex, et si on doit en ajouter un, ne jamais utiliser une valeur supérieure à 0
  - Rendre systématiquement très visible le focus en cas de navigation clavier
- Usage conforme des technologies web
  - En cas d'ajout d'attribut ARIA, s'assurer que l'usage est conforme.
  - Ne pas utiliser de rafraîchissement automatique de la page ou fournir un moyen de prolonger ou de désactiver le compte à rebours.
- Présentation de l'information
  - Toujours permettre à l'utilisateur de zoomer l'interface (ne pas utiliser user-scalable=0 dans le meta viewport). De même s'assurer qu'en cas de zoom tous les contenus sont visibles (pas de chevauchements, pas de contenus qui disparaissent ou sont tronqués).
  - En cas de désactivation (ou de non-chargement) des feuilles de style, le contenu doit rester compréhensible. De même pour cacher un champ on préférera utiliser type=hidden plutôt que class=hidden.
  - Contrastes : s'assurer que tous les contenus ont un contraste suffisant.
  - Expliciter les contenus (Suite = suite de la liste ou étape suivante ?).
  - Doubler systématiquement, pour chaque pictogramme, l'information visuelle d'une information textuelle (ne pas s'appuyer uniquement sur le alt de l'image ou l'aria-label, ajouter systématiquement un title).

Mesure

À tout moment, l'équipe projet devra présenter des livrables (spécifications / maquettes fonctionnelles, intégrations HTML, environnement de recette et/ou de pré-production, livraison finale…) conformes aux règles d'accessibilité à appliquer au stade de développement considéré, que ce soit pour les éléments graphiques, ergonomiques, fonctionnels, techniques ou éditoriaux.

Avant la mise en production, l'équipe projet devra effectuer des tests accessibilité de validation et les remettre à Orange. Elle corrigera les éventuelles erreurs constatées pour atteindre le niveau exigé.
NB : si des erreurs résiduelles sont constatées par Orange, elles devront être corrigées.

Une vigilance particulière devra être portée sur :

- La conformité à la charte graphique d'Orange, tout particulièrement en matière de contrastes des combinaisons de couleurs entre le contenu et l'arrière-plan.
- La compatibilité avec les aides techniques (lecteurs d'écran tels que Jaws et NVDA, les systèmes de configuration d'agrandissements comme les loupes logicielles).
- L'accessibilité au clavier (touches [Tab] tabulation, [Entrée]…).

Il est demandé au candidat d'indiquer dans sa réponse :

- La méthodologie qu'il propose pour prendre en compte les règles d'accessibilité à toutes les étapes du projet.
- Les livrables qu'il s'engage à fournir pour permettre à Orange d'avoir des garanties sur le niveau d'accessibilité obtenu (tests de recette etc.).
- Les références de projets déjà réalisés et conformes aux exigences d'accessibilité.
- Les mesures prises pour s'assurer d'une compétence suffisante en accessibilité dans ses équipes et les résultats obtenus.
- Tout autre élément permettant d'évaluer l'expertise et l'engagement du candidat en matière d'accessibilité numérique.

Vérification par Orange

Le niveau de conformité au référentiel d'accessibilité est vérifié par le centre de compétence de l'accessibilité numérique du groupe Orange : conformément à la loi, cette évaluation se traduit par la relecture de la déclaration d'accessibilité informant du taux de conformité au référentiel.

- 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

DELIBERATION 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

NOR : CNIL1917529X
JORF n°0142 du 21 juin 2019
Texte n° 95

Version initiale

La Commission nationale de l'informatique et des libertés,
Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;
Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;
Vu le code électoral ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 11-I-2°-a bis) ;
Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Article

Après avoir entendu Mme Dominique CASTERA, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;
Formule les observations suivantes :

A titre liminaire, la commission observe que le constat, réalisé lors de l'adoption de sa recommandation de 2010, du développement et de l'extension des systèmes de vote par correspondance électronique, notamment via Internet, à un nombre croissant d'opérations de vote et de types de vote, reste d'actualité.

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 et libre 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 par correspondance électronique, notamment via Internet, doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.

Devant l'extension continue du vote par Internet à tous types d'élections, la commission souhaite rappeler que le vote par correspondance électronique, notamment via Internet, 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 l'opacité et de la technicité importante des solutions mises en oeuvre, ainsi que de la très grande difficulté de s'assurer de l'identité et de la liberté de choix de la personne effectuant les opérations de vote à distance.

Au cours des travaux que la commission a menés depuis 2003 et compte tenu des menaces qui pèsent sur ces dispositifs, 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 reste réservée quant à l'utilisation de dispositifs de vote par correspondance électronique, notamment via Internet, pour des élections politiques.

La présente délibération a pour objet de revoir la recommandation de 2010 à l'aune des opérations électorales intervenues depuis, de l'évolution des solutions de vote proposées par les prestataires du secteur, des retours effectués par les différentes parties prenantes, des contrôles réalisés par la CNIL ainsi que de l'évolution du cadre juridique relatif à la protection des données.

La nouvelle recommandation a pour champ d'application les dispositifs de vote par correspondance électronique, en particulier via Internet. Elle ne concerne pas les dispositifs de vote par codes-barres, les dispositifs de vote par téléphone fixe ou mobile, ni les systèmes informatiques mis à disposition des votants

sous forme de boîtiers de vote ou en isoloirs (dites « machines à voter »). Elle est destinée à fixer, de façon pragmatique, les objectifs de sécurité que doit atteindre tout dispositif de vote par correspondance électronique, notamment via Internet, en fonction des risques que présente le déroulement du vote. Les réponses apportées par les systèmes à ces objectifs de sécurité doivent ainsi prendre en compte le contexte et les menaces qui pèsent sur le scrutin.

Elle vise également à s'appliquer aux futures évolutions des systèmes de vote par correspondance électronique, notamment via Internet, 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 par correspondance électronique à retenir.

Elle abroge la délibération n° 2010-371 du 21 octobre 2010 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.
Le niveau de risque du scrutin

Le niveau de risque que présente le déroulement d'un vote varie en fonction du type de scrutin, des évènements redoutés et des menaces qui pèsent sur le traitement. Ainsi, la commission recommande que la solution utilisée pour le scrutin tienne compte de l'importance du niveau de risque de l'élection ainsi que des éventuels bénéfices pour les parties prenantes de recourir à un système de vote par correspondance électronique et que la solution choisie réponde à tous les objectifs de sécurité fixés au regard de ce niveau de risque.

La commission identifie trois niveaux de risque :

- Niveau 1 : Les sources de menace, parmi les votants, les organisateurs du scrutin ou les personnes extérieures, ont peu de ressources et peu de motivations. L'administrateur (ou les administrateurs) du système d'information n'est ni électeur, ni candidat. Il est considéré comme neutre par toutes les parties. Ce niveau s'applique pour les scrutins impliquant peu d'électeurs, se déroulant dans un cadre non conflictuel, à l'issue duquel les personnes élues auront peu de pouvoirs, comme par exemple l'élection d'un représentant de classe. Le scrutin ne présente pas de risques importants.

- Niveau 2 : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources moyennes ou des motivations moyennes. Ce niveau s'applique à des scrutins impliquant un nombre important d'électeurs et présentant un enjeu élevé pour les personnes mais dans un contexte dépourvu de conflictualité particulière. Il s'agit par exemple des élections de représentants du personnel au sein d'organismes ou encore au sein d'un ordre professionnel. Le scrutin présente un risque modéré.

- Niveau 3 : Les sources de menace, parmi les votants, les organisateurs du scrutin, les personnes extérieures, au sein du prestataire ou du personnel interne, peuvent présenter des ressources importantes ou de fortes motivations. Ce niveau concerne les scrutins impliquant un nombre important d'électeurs et présentant un enjeu très élevé, dans un climat potentiellement conflictuel. Il s'agit par exemple d'élections de représentants du personnel au sein d'organisations importantes, à grande échelle et dans un cadre conflictuel. Le scrutin présente un risque important.

La commission déconseille d'utiliser un dispositif de vote par correspondance électronique, notamment via Internet, dans l'hypothèse où les sources de menace peuvent disposer à la fois de ressources importantes et d'une motivation forte.
Le responsable du traitement identifie le niveau correspondant à sa situation en fonction des risques soulevés par son scrutin. A cette fin la commission propose, de manière facultative et à titre d'exemple, une grille d'analyse simplifiée, basée sur des questions fermées, ayant pour objet de guider et d'aider les responsables de traitement le désirant à se positionner sur cette échelle. Cette grille d'analyse est placée au sein de la fiche pratique.

En cas de doute entre deux niveaux, le niveau le plus élevé devrait être privilégié. Le responsable de traitement, maitrisant le périmètre, les enjeux et le contexte de son scrutin, est libre de choisir le niveau de risque qu'il juge approprié, dès lors qu'il peut justifier son analyse auprès de la commission et de l'expert indépendant.

Une fois son niveau de risque identifié, le responsable de traitement peut déterminer les objectifs de sécurité que la solution de vote doit atteindre.

Le choix du niveau de risque par le responsable de traitement étant évalué par l'expert indépendant mandaté (voir ci-après) pour garantir la conformité des opérations de vote à la présente recommandation, il convient que le responsable de traitement lui fournisse les éléments ayant été pris en compte dans la détermination de ce niveau.

D'une manière générale, la commission rappelle que les traitements de données personnelles, dont les dispositifs de vote, qui remplissent au moins deux des critères suivants doivent en principe faire l'objet d'une analyse d'impact relative à la protection des données (AIPD) :
- évaluation/« scoring » (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles (opinions politiques et appartenances syndicales notamment) ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une technologie nouvelle) ;
- exclusion du bénéfice d'un droit/contrat.

Dès lors, au regard des critères relatifs aux données sensibles et à la collecte de données à large échelle et compte tenu du contexte du scrutin le cas échéant, il peut être nécessaire que le responsable de traitement réalise une AIPD.
Les objectifs de sécurité à atteindre en fonction du niveau de risque
Chaque niveau de risque se voit associer des objectifs de sécurité qui permettent de définir le niveau de sécurité attendu.
Ces objectifs sont cumulables, le niveau 2 étant composé d'objectifs de sécurité spécifiques et des objectifs de sécurité du niveau 1, le niveau 3 étant, quant à lui, composé d'objectifs de sécurité spécifiques et des objectifs de sécurité des deux niveaux précédents.

La commission proposera sur son site web ou tout autre support utile, une fiche pratique présentant des exemples permettant d'atteindre les objectifs de sécurité précités. Les industriels peuvent, s'ils le souhaitent, proposer à la commission des exemples de moyens permettant d'atteindre les objectifs afin que cette fiche puisse être agrémentée de ces informations. La commission sera seule juge de la pertinence des moyens proposés.

Cette fiche détaillera ce qui est attendu derrière chaque objectif de sécurité.
Les solutions de vote dont le scrutin présente un risque de niveau 1 doivent atteindre a minima l'ensemble des objectifs de

- Objectif de sécurité n° 1-01 : Mettre en œuvre une solution technique et organisationnelle de qualité ne présentant pas de faille majeure (faille publiée par l'éditeur et/ou rendue publique par des tiers).
- Objectif de sécurité n° 1-02 : Définir le vote d'un électeur comme une opération atomique, c'est-à-dire comme comportant de manière indivisible le choix, la validation, l'enregistrement du bulletin dans l'urne, l'émargement et la délivrance d'un récépissé.
- Objectif de sécurité n° 1-03 : Authentifier les électeurs en s'assurant que les risques majeurs liés à une usurpation d'identité sont réduit de manière significative.
- Objectif de sécurité n° 1-04 : Assurer la stricte confidentialité du bulletin dès sa création sur le poste du votant.
- Objectif de sécurité n° 1-05 : Assurer la stricte confidentialité et l'intégrité du bulletin pendant son transport.
- Objectif de sécurité n° 1-06 : Assurer, de manière organisationnelle et/ou technique, la stricte confidentialité et l'intégrité du bulletin pendant son traitement et son stockage dans l'urne jusqu'au dépouillement.
- Objectif de sécurité n° 1-07 : Assurer l'étanchéité totale entre l'identité de votant et l'expression de son vote pendant toute
la durée du traitement.
- Objectif de sécurité n° 1-08 : Renforcer la confidentialité et l'intégrité des données en répartissant le secret permettant le dépouillement exclusivement au sein du bureau électoral et garantir la possibilité de dépouillement à partir d'un seuil de secret déterminé.
- Objectif de sécurité n° 1-09 : Définir le dépouillement comme une fonction atomique utilisable seulement après la fermeture du scrutin.
- Objectif de sécurité n° 1-10 : Assurer l'intégrité du système, de l'urne et de la liste d'émargement.
- Objectif de sécurité n° 1-11 : S'assurer que le dépouillement de l'urne puisse être vérifié a posteriori.

Les solutions de vote dont le scrutin présente un risque de niveau 2 doivent atteindre a minima l'ensemble des objectifs de sécurité du niveau 1 ainsi que les suivants :
- Objectif de sécurité n° 2-01 : Assurer une haute disponibilité de la solution.

- Objectif de sécurité n° 2-02 : Assurer un contrôle automatique de l'intégrité du système, de l'urne et de la liste d'émargement.
- Objectif de sécurité n° 2-03 : Permettre le contrôle automatique par le bureau électoral de l'intégrité de la plateforme de vote pendant tout le scrutin.
- Objectif de sécurité n° 2-04 : Authentifier les électeurs en s'assurant que les risques majeurs et mineurs liés à une usurpation d'identité sont réduits de manière significative.
- Objectif de sécurité n° 2-05 : Assurer un cloisonnement logique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.
- Objectif de sécurité n° 2-06 : Utiliser un système d'information mettant en œuvre les mesures de sécurité physique et logique recommandées par les éditeurs et l'ANSSI.
- Objectif de sécurité n° 2-07 : Assurer la transparence de l'urne pour tous les électeurs.
Les solutions de vote dont le scrutin présente un risque de niveau 3 doivent atteindre a minima l'ensemble des objectifs de sécurité des niveaux 1 et 2, ainsi que les suivants :
- Objectif de sécurité n° 3-01 : Etudier les risques selon une méthode éprouvée afin de définir les mesures les plus adéquates au contexte de mise en œuvre.
- Objectif de sécurité n° 3-02 : Permettre la transparence de l'urne pour tous les électeurs à partir d'outils tiers.
- Objectif de sécurité n° 3-03 : Assurer une très haute disponibilité de la solution de vote en prenant en compte les risques d'avarie majeure.
- Objectif de sécurité n° 3-04 : Permettre le contrôle automatique et manuel par le bureau électoral de l'intégrité de la plateforme pendant tout le scrutin.
- Objectif de sécurité n° 3-05 : Assurer un cloisonnement physique entre chaque prestation de vote de sorte qu'il soit possible de stopper totalement un scrutin sans que cela ait le moindre impact sur les autres scrutins en cours.
Le responsable de traitement ou son prestataire sont libres d'utiliser toute solution leur permettant d'atteindre les objectifs de sécurité énoncés.
Quel que soit le niveau déterminé, 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 par correspondance électronique, notamment via Internet. Cette notice explicative ne se substitue pas à l'obligation d'information imposée par les articles 13
et 14 du règlement européen sur la protection des données (RGPD) s'agissant du traitement des données.
Parallèlement, la commission tient à souligner que, de par leur nature et sensibilité, les plateformes de vote par correspondance électronique, notamment via Internet, se doivent d'être accessibles à toutes personnes, notamment aux personnes en situation de handicap et en particulier visuel. Ainsi, pour les organismes du secteur public ou délégataires d'une mission de service public désirant proposer ce service à ses électeurs, il est nécessaire que le système de vote respecte le référentiel général d'accessibilité pour les administrations (RGAA). Pour les organismes non soumis à ce référentiel, il est fortement recommandé d'en suivre les prescriptions afin de mettre l'ensemble des votants en capacité d'exprimer leur suffrage par ce moyen.

L'expertise du système de vote par correspondance électronique, notamment via Internet
Tout responsable de traitement mettant en oeuvre un système de vote par correspondance électronique, notamment via
Internet, doit faire expertiser sa solution par un expert indépendant, que la solution de vote soit gérée en interne ou fournie par un prestataire.
L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), la constitution des listes
d'électeurs et leur enrôlement et 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 éléments décrits dans la présente délibération et notamment sur :
- le code source correspondant à la version du logiciel effectivement mise en oeuvre ;
- les mécanismes de scellement utilisés aux différentes étapes du scrutin ;
- le système informatique sur lequel le vote va se dérouler ;
- les échanges réseau ;
- les mécanismes de chiffrement utilisés, notamment pour le chiffrement du bulletin de vote ;
- les mécanismes d'authentification des électeurs et la transmission des secrets à ces derniers ;
- l'évaluation du niveau de risque du scrutin ;
- la pertinence et l'effectivité des solutions apportées par la solution de vote aux objectifs de sécurité.
L'expertise doit porter sur l'ensemble des éléments constituant la solution de vote.
Lors de scrutins présentant un niveau de risque 2 ou 3, l'expert réalise des audits sur la plateforme, afin de s'assurer de la cohérence et de l'effectivité des solutions apportées, par le biais de tests d'intrusions notamment. L'ensemble des opérations effectuées dans ce cadre est annexé au rapport d'expertise.

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 dans la société qui a créé la solution de vote à expertiser, ni dans l'organisme responsable de traitement qui a décidé d'utiliser la solution de vote ;
- posséder si possible une expérience dans l'analyse des systèmes de vote, en ayant expertisé les systèmes de vote par correspondance électronique, notamment via Internet, d'au moins deux prestataires différents.

Le rapport d'expertise, et ses annexes doivent être remis au responsable de traitement et aux prestataires de solution de vote par correspondance électronique, notamment via Internet.
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. Pour ce faire, l'expert peut, par exemple, utiliser des empreintes numériques.
L'expertise portant sur une solution mise en œuvre pour un scrutin dont le niveau de risque est évalué à 1 peut reprendre des éléments d'un rapport d'expertise précédent, dès lors que cette expertise effectuée sur l'élément en question n'est pas antérieure à 24 mois, qu'il est possible de prouver que l'élément sur lequel a porté cette expertise précédente n'a pas été modifié depuis et qu'aucune vulnérabilité sur cet élément n'a été révélée entre temps.

L'expertise portant sur une solution mise en œuvre pour un scrutin dont le niveau de risque est évalué à 2 peut reprendre des éléments d'un rapport d'expertise précédent, dès lors que cette expertise effectuée sur l'élément en question n'est pas antérieure à mois, qu'il est possible de prouver que l'élément sur lequel a porté l'expertise précédente n'a pas été modifié depuis et qu'aucune vulnérabilité sur cet élément n'a été révélée entre temps.
L'expertise portant sur une solution mise en œuvre pour un scrutin dont niveau de risque évalué à 3 doit être réalisée de nouveau, pour chaque élément, pour chaque élection.
L'expert ayant accès à des informations sensibles relatives aux solutions dont il est chargé d'évaluer la conformité, notamment le code source des applications, il est tenu de prendre toutes dispositions et précautions utilises afin de protéger les éléments qui sont portés à sa connaissance, notamment en limitant autant que possible les reproductions de code source au sein du rapport, en conservant ses rapports au sein d'espaces sécurisés dédiés et en ne conservant pas les éléments portés à sa connaissance au-delà de la durée nécessaire.

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.

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

Pour se connecter à distance ou sur place au système de vote, l'électeur doit s'authentifier conformément à la présente recommandation et à l'aide d'un moyen répondant à l'objectif de sécurité correspondant au niveau de risque identifié pour le scrutin. 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.
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 reçoit alors la confirmation de son vote et dispose de la possibilité de conserver trace de cette confirmation. La solution de vote par correspondance électronique, notamment via Internet, doit proposer toutes les options offertes par les textes fondant le vote, le cas échéant le vote nul ou blanc.

Dans le cas où le scrutin est mixte, composé d'un vote par correspondance électronique associé à un vote par correspondance papier par exemple, il convient que le vote électronique permette aux électeurs les mêmes possibilités que celles offertes par le vote papier, telle que la possibilité de voter nul ou blanc lorsque cela est prévu pour un scrutin, afin de ne pas créer de distorsion en fonction du moyen utilisé. Dans le cas où ces différentes possibilités sont offertes à l'électeur, il convient d'être attentif au fait qu'une personne ne puisse pas voter deux fois, notamment en utilisant le système par correspondance papier et le système par Internet. Ainsi la solution retenue doit permettre d'écarter les votes par correspondance papier d'une personne ayant déjà voté par Internet.

Les garanties minimales pour un contrôle a posteriori
Pour des besoins d'audit externe, notamment en cas de contentieux électoral, le système de vote par correspondance électronique, notamment via Internet, doit pouvoir 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 détenteurs ;
- le vote est anonyme lorsque la législation l'impose ;
- la liste d'émargement ne comprend que la liste des électeurs ayant voté ;
- l'urne dépouillée est bien celle contenant les suffrages des électeurs et qu'elle ne contient que ces suffrages ;
- aucun décompte partiel n'a pu être effectué durant le scrutin ;
- le dépouillement de l'urne peut être vérifié a posteriori et qu'il s'est déroulé de façon correcte.

La conservation des données portant sur l'opération électorale
Tous les fichiers supports (copies des codes sources et exécutables des programmes et du système sous-jacent, matériels de vote, fichiers d'émargement, de résultats, sauvegardes) doivent être conservés sous scellés jusqu'à l'épuisement des voies et 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 au prestataire de service, le cas échéant, de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation de ces supports.
Lorsqu'aucune action contentieuse n'a été engagée à l'épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.
Dispositions transitoires et finales
La présente délibération est publiée au Journal officiel de la République française. Elle devra être prise en compte par les responsables de traitement après un délai transitoire de douze mois à compter de sa publication.

La présidente,
M.-L. Denis
Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une reco...
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239
5 sur 5 09/03/2021 à 10:43

- Fiche ISA

Annexe relative à la Sécurité des Informations

- Ci-après désignée « l'ISA » -

CETTE PAGE DOIT ÊTRE SUPPRIMEE SI CE DOCUMENT EST INTÉGRÉ À UN CONTRAT

Version: 3.1
Version française

Date: 01 septembre 2020

Pages: 14

Contacts:

BuyIn	Marc WESSEL (marc.wessel@buyin.pro) +49 228 433 21221
DTAG	Gero Krüger (gero.kruger@telekom.de) +49 228 18133485
Orange	Valérie Mercier (valerie.mercier@orange.com) +33 6 78 59 21 35

PRINCIPES GÉNÉRAUX

La présente Annexe relative à la Sécurité des Informations (ISA) établit les exigences de sécurité IT de Deutsche Telekom AG (DTAG) et/ou Orange SA (Orange). Si l'ISA s'applique aux Livrables du contrat, le Fournisseur doit considérer ces exigences comme un standard de sécurité minimum qui doit être appliqué pendant toute la durée du Contrat, que les Livrables soient fournis par ce contrat ou un distributeur tiers.

Ces exigences couvrent différents aspects de la sécurité de l'information et certaines d'entre elles dépendent de la nature des Livrables fournis dans le cadre du Contrat.

Par ailleurs, ces exigences pourront être renforcées par des exigences complémentaires qui seront fournies par l'Acquéreur et agréées par les Parties dans un document annexé au Contrat, au NPA et/ou à la Commande.

ORDRE DE PRIORITÉ DES DOCUMENTS

La présente ISA est un document standard qui s'applique à tout Contrat conclu avec le Fournisseur qui y fait référence.

1. Le Contrat prévaut sur l'ISA sauf si un ordre de priorité différent a été établi dans le Contrat.
2. Nonobstant ce qui précède, tous les termes commençant par une majuscule ou écrits en lettres capitales seront interprétés conformément aux définitions figurant à la fin de la présente ISA, et à défaut d'une telle définition, tels qu'ils sont définis dans le Contrat contenant la référence à la présente ISA.

Les Parties conviennent que l'ISA prévaut sur les documents du Fournisseur définissant les exigences de sécurité attachés ou référencés dans le Contrat, NPA et/ou Commande.

APPLICABILITÉ GÉNÉRALE

Le Fournisseur se conformera aux exigences de l'ISA relatives aux Livrables suivants :

- **Logiciel** fait référence à un package logiciel standard du Fournisseur et/ou à un logiciel développé spécifiquement à partir d'un cahier des charges convenu par les Parties (ex. Production Logicielle);
- **Matériel** inclus tout logiciel /firmware (ex. terminaux, systèmes, équipements, etc.) ;
- **XaaS/Cloud Services** (ex. Software As A Service)
- **Services Professionnels** prestations d'installation, formation, intégration, maintenance et/ou consulting.

APPLICABILITÉ GÉNÉRALE DES SECTIONS EN FONCTION DES LIVRABLES

Les sections suivantes s'appliquent à tous les Livrables du Fournisseur :

- **Section A: "**Respect du Contrat et des standards"
- **Section B: "**Sécurité Organisationnelle"
- **Section C: "**Gestion des incidents**"**

Les sections ci-dessous s'appliquent en fonction de la nature des Livrables tels que définis dans la table A:

- **Section D:** "Chiffrement et authentification"
- **Section E:** "Security by design"
- **Section F:** "Gestion des correctifs de sécurité"
- **Section G:** "Données de l'Acquéreur en XaaS/Cloud Services"
- **Section H:** "Contrôle d'accès au XaaS/Cloud Services"
- **Section I:** "Opérations XaaS/Cloud Services"
- **Section J:** "Accès et utilisation des systèmes et ressources de l'Acquéreur "
- **Section K:** "Intervenants et sécurité"

Livrable	Sections concernées

Table A: Application des sections de l'ISA

Logiciel	**A, B, C, D, E, F**
Matériel	**A,B, C, D, E, F**
XaaS/Cloud Services	**A, B,C, D, E, F, G, H, I**
Services Professionels	**A, B, C, J, K**

RESPECT DU CONTRAT ET DES STANDARDS

Évaluation de la Sécurité des Livrables

Sur demande de l'Acquéreur, le Fournisseur doit fournir sous 10 jours ouvrables toute information/documentation nécessaire pour évaluer la sécurité des Livrables : rapports de test/audit, scans de vulnérabilité et analyses de la robustesse du code source.

Politique de Sécurité

Le Fournisseur doit appliquer une politique de sécurité de l'information d'entreprise en tant qu'approche standard conformément à la norme ISO/IEC 27001 ou à toute autre norme.

Si le Fournisseur est certifié, il doit présenter sa certification de sécurité et tenir l'Acquéreur informé des renouvellements ou annulations de ses certifications.

Si le Fournisseur est sélectionné sur la base d'une certification (ex ISO/IEC 27001), le Fournisseur doit maintenir cette certification pendant toute la durée contractuelle.

Audit

L'Acquéreur et Orange SA et/ou Deutsche Telekom AG peuvent procéder à des audits afin de vérifier si le Fournisseur respecte les exigences de sécurité de l'Acquéreur et d'Orange et/ou de DTAG définies dans le Contrat

Recours à des services tiers

Dans le cas d'un recours à des services tiers dans la fourniture d'un Livrable, le Fournisseur doit s'assurer que ceux-ci sont toujours conformes aux exigences de sécurité définies dans le Contrat.

Conformité aux spécifications NESAS

NOTE: le paragraphe A.5 est seulement applicable aux équipements réseau mobile (équipement pour le cœur de réseau mobile, le RAN et l'accès).

Le Fournisseur d'équipements de réseau mobile doit évaluer le développement et le cycle de vie des équipements selon les spécifications adéquates du NESAS (Network Equipement Security Assurance Scheme), émises par la GSMA (GSMA PRD FS.13/15/16), dans la version en cours.

Le Fournisseur doit également fournir à Orange/DT les résumés des rapports d'audit associés, effectués par un organisme accrédité. L'évaluation doit être finalisée avant de fournir tout équipement réseau mobile.

Non-respect des dispositions de l'ISA

Dans le cas où le Fournisseur est informé du non-respect des exigences de sécurité dans les Livrables, le Fournisseur doit rapidement fournir à l'Acquéreur une analyse de la situation et un plan de remédiation. Si le plan de remédiation est accepté par l'Acquéreur, il est mis en œuvre par le Fournisseur sans surcoût pour l'Acquéreur et le Fournisseur doit fournir la preuve de l'efficacité du plan de remédiation.

Si le non-respect persiste ou si le plan de remédiation n'est pas accepté, cela constitue automatiquement un manquement grave au Contrat.

SÉCURITÉ ORGANISATIONELLE

Structure

Sur demande de l'Acquéreur, le Fournisseur doit fournir l'information sur son organisation de la sécurité.

Point de contact

Le Fournisseur doit nommer un point de contact responsable de la sécurité ainsi qu'un correspondant issu des instances dirigeantes ou un responsable Grands Comptes afin de traiter des problèmes faisant l'objet d'une escalade managériale et/ou signalisation. Les contacts sont identifiés pour chaque projet et toute modification doit être communiquée sans délai.

Revues de Sécurité

Une fois par an, sur demande de l'une des 2 parties, le Fournisseur et l'Acquéreur organisent une réunion visant à réaliser une revue des points de sécurité (ex. évolutions et opérations programmées qui sont susceptibles d'avoir un impact potentiel sur la sécurité).

Chaque partie peut solliciter une réunion de sécurité exceptionnelle lorsque la situation impose une analyse en commun ou une décision immédiate (par exemple : un incident majeur ou une évolution significative des menaces). Cette réunion doit être acceptée par l'autre partie.

Mesures de Sécurité pour les données de l'Acquéreur

Par données de l'acquéreur il est entendu tout bien informationnel de l'Acquéreur, c'est-à-dire les données commerciales (par exemple les contrats, les négotiations, les données financières) et/ou les données techniques et SI (par exemple schémas d'architecture fonctionnelle, réseau, plans d'adressage).

Le Fournisseur doit mettre en place les mesures suivantes pour les données de l'Acquéreur qui sont classifiées comme confidentielles par l'Acquéreur, c'est-à-dire envoyées de manière chiffrée par l'Acquéreur et/ou marquées confidentiel :

- toutes ces données doivent être chiffrées lors du stockage ou du transfert de celles-ci ;
- un système d'authentification forte doit être mis en place (ex. authentification à 2 facteurs).

Les Parties doivent convenir par avance des moyens appropriés permettant, en cas de besoin, d'échanger des données chiffrées.

GESTION DES INCIDENTS

Détection

Le Fournisseur doit mettre en place les mesures pour détecter les incidents de sécurité impactant l'Acquéreur et se produisant dans l'environnement du Fournisseur. Les incidents de sécurité sont, de manière non exhaustive, la perte, la modification, la divulgation ou l'accès non autorisé aux données ou informations de l'Acquéreur et la divulgation non autorisée de code source propriétaire.

Notification

Le Fournisseur doit notifier sans délai l'Acquéreur dans le cas d'un tel incident de sécurité.

En cas de violation de la sécurité des données ou de divulgation non autorisée d'information de l'Acquéreur, le Fournisseur doit notifier l'Acquéreur conformément à la législation en vigueur, et au plus tard dans un délai de 24 heures après en avoir pris connaissance.

Les détails des incidents de sécurité doivent être conservés par le Fournisseur au moins jusqu'à la prochaine revue de sécurité entre les Parties.

Résolution

Le Fournisseur doit immédiatement résoudre les incidents de sécurité et informer l'Acquéreur de l'avancement et de la clôture de l'incident. Cette obligation est une obligation de résultat.

Suspension de l'accès aux systèmes de l'Acquéreur

NOTE: le paragraphe C.4 n'est pas applicable aux Livrables Logiciel, Matériel et aux Services XaaS/Cloud.

Dans le cas où un incident de sécurité concerne les Services Professionnels, l'Acquéreur peut suspendre l'accès à ces systèmes jusqu'à la résolution de l'incident.

Suspension de l'accès de l'Acquéreur aux Services Xaas/Cloud

NOTE: le paragraphe C.5 n'est pas applicable aux Livrables Logiciel, Matériel et aux Services Professionnels.

Dans le cas d'un incident de sécurité concernant les Services XaaS/Cloud (ex. intrusion dans le système, malware), l'Acquéreur est susceptible de suspendre son accès au service concerné jusqu'à la résolution de l'incident.

Dans le cas où l'Acquéreur ne peut lui-même suspendre l'accès, l'Acquéreur demandera explicitement au Fournisseur de suspendre tout accès de l'Acquéreur jusqu'à la résolution de l'incident. Le Fournisseur devra prendre en compte immédiatement cette demande.

Rapports de sécurité pour les Services XaaS/Cloud Services et les Services Professionnels

NOTE: le paragraphe C.6 n'est pas applicable aux Livrables Logiciel et Matériel.

À concurrence de deux fois par an, l'Acquéreur peut demander au Fournisseur un rapport de sécurité relatif aux Services XaaS/Cloud. Ce rapport de sécurité comprend, entre autres, les informations suivantes :

- le nombre d'incidents de sécurité détectés au cours des 12 derniers mois, en séparant les causes internes et externes le cas échéant ;
- les informations relatives aux incidents de sécurité au cours de la période : heure de détection, nature et impact, solution de remédiation, heure de rétablissement du service, heure de clôture de l'incident, temps de résolution.

CHIFFREMENT ET AUTHENTIFICATION

Modification des données d'authentification et des clés de chiffrement par l'Acquéreur

Toutes les données d'authentification et clés cryptographiques (ex. certificats, clés privées/publiques, clés symétriques, mots de passe …) dans les Livrables Logiciel et Matériel doivent être modifiables par l'Acquéreur et protégées conformément à l'état de l'art. Pour les données d'authentification et les clés de chiffrement non modifiables par l'Acquéreur, Le Fournisseur doit fournir à DTAG et /ou Orange la liste exhaustive de celles-ci ainsi que leurs finalités. Pour les Services XaaS/Cloud, cette demande concerne uniquement les données d'authentification utilisées par l'Acquéreur pour protéger ses données, y compris les comptes administrateurs.

Robustesse des algorithmes de chiffrement et des clés

Le Fournisseur doit uniquement utiliser des algorithmes de chiffrement standard recommandés par les institutions gouvernementales (ex BSI, ANSSI et NIST) à la date de signature ou de renouvellement du Contrat.

SECURITY BY DESIGN - SÉCURITÉ INTÉGRÉE À LA CONCEPTION

Hardening

Le Fournisseur doit mettre en oeuvre les bonnes pratiques de durcissement des configurations (« hardening security »). Cela inclut notamment la restriction des protocoles d'accès, la suppression ou la désactivation des logiciels, ports réseau ou services non utilisés, la suppression des fichiers ou des comptes utilisateurs inutiles, la restriction des droits d'accès aux fichiers, l'installation des correctifs de sécurité, ainsi que l'activation de la journalisation.

Le Fournisseur doit produire des Livrables configurés par défaut conformément à l'état de l'art en matière de sécurité (ex . https://www.cisecurity.org/). Ceci s'applique également aux composants et services fournis par des tiers.

Nonobstant ce qui précède, le Fournisseur doit fournir à l'Acquéreur toutes les informations nécessaires pour configurer et utiliser les Livrables de façon sécurisée et s'assurer que ces informations sont mises à jour pendant toute la durée du Contrat.

De plus, le Fournisseur doit s'assurer que les Livrables ne contiennent pas de Backdoors.

Tests du logiciel pour les failles de sécurité

Le Fournisseur doit tester les Livrables pour s'assurer qu'ils sont exempts de vulnérabilités critiques, telles que listées dans le " Top 25 CWE/SANS " (http://cwe.mitre.org) et/ou " TOP 10 OWASP " (http://www.owasp.org) à la date de livraison (ex. robustesse de la validation des entrées face aux attaques par injection, telles que les injections SQL, comportement prédictible en cas de surcharge, etc.)

Mesures complémentaires

A la demande de l'Acquéreur, DTAG et/ou Orange, les Parties peuvent mutuellement convenir de mesures complémentaires de sécurité que les Livrables devront satisfaire.

Ces mesures complémentaires peuvent être regroupées dans un document intitulé "Security Statement of Compliance" et être intégrées au Contrat et/ou au NPA.

GESTION ET CORRECTION DES VULNÉRABILITÉS LOGICIELLES

Détection

Le Fournisseur s'engage à mettre en place un système de gestion des Vulnérabilités et des alertes permettant notamment de suivre les sources d'alertes de sécurité externes (ex. alertes émises par les éditeurs/constructeus, CERTs …) et se tenir informé des Vulnérabilités pouvant impacter les Livrables (y compris celles impactant les composants tiers utilisés).

CVE standard

Lorsque cela est pertinent, chaque Vulnérabilité détectée par le Fournisseur est identifiée par une CVE unique associée à un score CVSS (v3 ou supérieure), consistant en un score de base CVSS, le score temporel et le vecteur. Toute alternative à ce dispositif doit préalablement avoir fait l'objet d'une autorisation écrite de l'Acquéreur.

Notifications

Le Fournisseur doit fournir à l'Acquéreur, sans délai, les informations sur chaque Vulnérabilité (avec un score CVSS supérieur ou égal à 7.0) incluant les Zero-Day impactant les Livrables ainsi que leurs conséquences (ex. CVE, CVSS score, composants et services affectés).

Le Fournisseur doit communiquer les avis de sécurité au format cvrf/xml ou tout autre format parsable par email au cert@orange.com et/ou cert@telekom.de

Service level agreement pour la correction des Vulnérabilités

Pour chaque Vulnérabilité impactant les Livrables, le Fournisseur s'engage :

- à faire tous les efforts nécessaires pour fournir à l'Acquéreur le correctif temporaire dans les délais fixés par le tableau ci-après; et
- à fournir à l'Acquéreur le Correctif Officiel dans les délais fixés ci-après.

note CVSS base score v2	**Délai maximum pour fournir un Correctif Temporaire**	**Délai maximum pour fournir un Correctif Officiel**
7.0-10.0	5 (cinq) jours ouvrés	30 (trente) jours ouvrés
0-6.9	non applicable	6 (six) mois

Le délai court à partir de la découverte de la Vulnérabilité sauf si la Vulnérabilité est présente dans un composant d'une Tierce Partie dans ce cas le délai court à compter de la date de disponibilité du correctif.

Maintenance sécurisée des composants de Tierce Partie

Le Fournisseur doit s'assurer que les composants provenant de tiers utilisés dans les Livrables sont maintenus sécurisés pendant la période de maintenance ou de Service sous contrat avec l'Acquéreur.

Anomalie de sécurité

Le Fournisseur accepte que l'Acquéreur puisse ouvrir un ticket de maintenance pour corriger chaque Vulnérabilité impactant le Livrable et détectée par l'Acquéreur pendant la période contractuelle de maintenance et/ou de garantie. En sus de la section **Erreur ! Source du renvoi introuvable.**, le Fournisseur doit respecter les conditions de maintenance pour corriger l'anomalie associée à la Vulnérabilité.

Exceptions

Le Fournisseur s'engage à déployer des efforts commercialement raisonnables afin d'aider l'Acquéreur à corriger les Vulnérabilités :

- dans les cas requérant une réponse plus rapide que celle prévue dans le tableau ci-dessus (par exemple la publication dans la presse d'une vulnérabilité présente dans un Livrable utilisé par l'Acquéreur) et
- dans l'environnement nécessaire à l'exploitation du Livrable (par exemple le système d'exploitation d'un Livrable Logiciel)

Dommage et intérêts/Pénalités

En complément des pénalités appliquées suite à une violation patente telle que visée à la section A.6 « Non-respect des dispositions de l'ISA », l'Acquéreur peut demander des pénalités au Fournisseur comme mentionné dans les sections « Dommages » ou « Pénalités » du Contrat.

Les pénalités suivantes s'appliquent en cas de Vulnérabilité :

En cas de défaillance du fournisseur à livrer un Correctif Officiel de sécurité concernant des Vulnérabilités dont la note CVSS est supérieure ou égale à 7 conformément au tableau défini dans la section **Erreur ! Source du renvoi introuvable.** « **Erreur ! Source du renvoi introuvable.** », les pénalités sont calculées de la façon suivante :

$$M = V \times N / 300$$

M : montant des pénalités.

V : V correspond à la valeur des Livrables.

N : nombre de jours civils après le délai du Correctif Officiel.

Sécurité relative à la maintenance

Pendant la durée de maintenance du contrat ou de la garantie, le Fournisseur doit fournir les Livrables Logiciel et Matériel ainsi que les nouvelles versions avec tous les correctifs de sécurité. Ces correctifs peuvent être appliqués ou fournis au même moment dans des composants/packages séparés.

Pendant le cycle de vie du Livrable, le Fournisseur doit fournir à l'Acquéreur les correctifs de sécurité dès la publication de ceux-ci, en respectant les délais de correction définis à la section **Erreur ! Source du renvoi introuvable.**.

Le Fournisseur doit fournir les informations (ex CVE, CVSS score) à l'Acquéreur concernant les Vulnérabilités corrigées.

DONNÉES DE L'ACQUÉREUR DANS LES SERVICES XAAS/CLOUD

Limitation de l'utilisation des données de l'Acquéreur

Le Fournisseur ne doit utiliser, traiter, transmettre ou stocker les données de l'Acquéreur dans les Services XaaS/Cloud qu'aux fins de la fourniture du Service.

Séparation des données de l'Acquéreur

Le Fournisseur s'engage à séparer les données de l'Acquéreur des données des autres clients du Fournisseur.

Confidentialité des données de l'Acquéreur

Le Fournisseur s'engage à chiffrer toutes les données classées confidentielles par l'Acquéreur lors du transfert ou du stockage de celles-ci.

Solutions de chiffrement du Fournisseur

Dans le cas où l'Acquéreur utilise une solution de chiffrement du Fournisseur pour protéger ses données, le Fournisseur s'assure :

- que toutes les données soient chiffrées lors du stockage ou du transfert, et
- qu'un système d'authentification forte soit mis en place (ex. authentification à 2 facteurs).

Gestion des informations et des accès de l'Acquéreur

Le fournisseur s'engage à :

- journaliser les accès et actions sur les données de l'Acquéreur dans le Xaas /Service Cloud, y compris ceux de ses employés ou de tiers désignés, et
- conserver ces journaux pour la durée convenue dans le NPA et/ou la Commande (y compris les documents associés tels qu'un Accord de Confidentialité ou un Contrat de Traitement des Données), ou à défaut pour une durée maximum de 6 mois.

Les extraits des journaux conservés doivent être communiqués à l'Acquéreur sur demande de ce dernier.

Réversibilité des données de l'Acquéreur

A échéance du NPA et/ou de la commande, le Fournisseur doit restituer toutes les données de l'Acquéreur dans le XaaS/Cloud Service dans un format convenu et sur une période convenus au préalable avec l'Acquéreur.

Conformément aux sections **Erreur ! Source du renvoi introuvable.** et G.4, seules des connexions chiffrées doivent être utilisées pour la réversibilité des données de l'Acquéreur , sauf exception validée par écrit par l'Acquéreur.

A la fin de la période de réversibilité des données, le Fournisseur doit détruire tous les environnements de l'Acquéreur et les données dans le Service XaaS/Cloud Service d'une façon qui permette de s'assurer qu'elles ne peuvent être ni accédées ni lues.

Le Fournisseur doit fournir à l'Acquéreur un certificat de destruction.

CONTRÔLE D'ACCÈS DES SERVICES XAAS/CLOUD

Sécurité Physique

Le Fournisseur doit fournir des locaux sécurisés pour les infrastructures de production en Cloud et pour les sites depuis lesquels sont réalisées les opérations à distance.

Les mesures de sécurité doivent inclure à minima les éléments suivants :

- L'accès physique doit nécessiter une autorisation et être contrôlé ;
- Toute personne doit porter sur le site un badge officiel de façon visible ;
- Les visiteurs doivent signer un registre des visiteurs et être accompagnés et/ou surveillés dans les locaux ; et
- La possession des clés/cartes d'accès et la capacité d'accéder sur le site doivent être contrôlées. Le personnel du Fournisseur quittant la société doit impérativement restituer les clés/cartes .

Contrôle d'accès et gestion des mots de passe

Le Fournisseur doit contrôler l'accès aux systèmes, en restreignant ces accès aux seules personnes dûment autorisées.

Le Fournisseur doit mettre en œuvre une politique de mots de passe sur les composants de l'infrastructure et les environnements Cloud utilisés. Le Fournisseur doit protéger les mots de passe en utilisant des solutions de sécurité telles que les coffres-forts numériques.

Le Fournisseur met en place un système de contrôle et de journalisation des accès conçu pour s'assurer que seuls les personnel d'exploitation et de maintenance autorisés disposent d'accès appropriés aux systèmes. Ce système de contrôle d'accès doit comporter des mécanismes d'authentification, d'autorisation et de gestion des droits d'accès (attribution, provisionnement et révocation des droits d'accès) des employés et utilisateurs désignés par le Fournisseur.

Revue des droits d'accès

Les comptes d'accès des employés du Fournisseur au réseau et au système d'exploitation doivent être revus régulièrement pour s'assurer de la légitimité des droits d'accès.

Dans le cas où un employé du Fournisseur ne fait plus partie du projet sous contrat, le Fournisseur devra prendre rapidement les mesures nécessaires pour mettre fin aux accès associés : accès réseau, moyens téléphoniques et accès physiques.

Passerelle de sécurité

Le Fournisseur doit utiliser des passerelles de sécurité (ex. firewalls, routeurs, proxies, reverse proxies) pour contrôler l'accès Internet avec les services du Fournisseur afin de ne permettre que les flux autorisés.

Les passerelles de sécurité du Fournisseur doivent être configurées avec des politiques de sécurité et de filtrage des flux appropriés basées sur les protocoles, les ports et les adresses IP sources/destinations. Ces politiques de sécurité et de filtrage doivent donc permettre d'identifier les sources, destinations et types de flux autorisés.

Contrôles Anti-malware

Le Fournisseur doit disposer de logiciel(s) anti-malware pour scanner les fichiers téléchargés. La liste des Malware doit être mise à jour au moins une fois par jour.

Chiffrement et connections distantes aux Services XaaS/Cloud

Pour les accès et l'utilisation des Services XaaS/Cloud Service par l'Acquéreur, seules des connexions chiffrées doivent être utilisées sauf exception acceptée par écrit par l'Acquéreur.

Le Fournisseur doit s'assurer que seules des connexions authentifiées et chiffrées sont utilisées par des tiers ayant un accès distant aux données de l'Acquéreur exploitées et stockées dans les Services XaaS/Cloud .

Dans tous les cas, les dernières versions de navigateurs doivent être supportées pour la connexion aux Services Xaas/Cloud.

OPERATIONS DE XAAS/CLOUD SERVICES

Tests de Pénétration

Le Fournisseur doit s'assurer de la sécurité des Services XaaS/Cloud Service en effectuant des tests de pénétration au moins une fois par an. Le résultat et le plan de correction de ces tests doivent être partagés avec DTAG et/ou Orange SA.

Nonobstant ce qui précède, le Fournisseur doit permettre à DTAG et/ou Orange SA de réaliser des tests de pénétration des Services XaaS/Cloud Service sur son environnement de production.

Données de Production et environnement

Le Fournisseur ne doit pas utiliser les données de production pour des activités de tests.

Le Fournisseur doit séparer les environnements de développement, de test et de production (ex. réseau, données, applications, etc.).

Plan de reprise d'activité (Disaster recovery plan)

Le Fournisseur doit définir et maintenir à jour un plan de reprise d'activité et s'assurer qu'il est testé à intervalles réguliers.

Les sauvegardes doivent être détruites de façon sécurisée par le Fournisseur lors du décommissionement ou la mise au rebut du matériel.

Maintenance pour des besoins de sécurité

Le Fournisseur doit appliquer et tester préalablement sur un environnement de test tout patch de sécurité devant être déployé sur le Service Xaas/Cloud. C'est seulement à l'issue de tests positifs sur l'environnement de test que le Fournisseur pourra déployer le patch sur l'environnement de production.

Services rendus par des tiers

Le Fournisseur doit notifier l'Acquéreur de toute intervention prévue de services tiers (ex. data center services) dans la fourniture du Service.

Relocalisation des données

Le Fournisseur doit notifier l'Acquéreur dans le cas où les données de l'Acquéreur (y compris les données de sauvegarde) sont relocalisées vers un autre centre de données que ceux initialement convenus dans le Contrat.

ACCESS ET UTILISATION DES SYSTÈMES OU RESSOURCES DE L'ACQUÉREUR

Cette section ne s'applique que si l'Acquéreur permet au Fournisseur l'accès et l'utilisation de ses systèmes pour l'exécution du contrat.

Physique

Si l'Acquéreur fournit un accès et/ou des équipements d'interconnexion installés dans les locaux du Fournisseur, le Fournisseur s'assure que :

- le contrôle d'accès physique soit appliqué dans l'espace technique où l'équipement est installé ; et
- l'accès physique à cet équipement soit strictement limité aux seules personnes ayant besoin de cet accès aux fins d'exécution du Contrat et dûment autorisées par le Fournisseur.

Systèmes de l'Acquéreur

Le Fournisseur s'engage à :

- accéder et utiliser les systèmes de l'Acquéreur aux seules fins de la fourniture des Livrables ;
- s'assurer que les accès et le transfert de données ne sont pas utilisés pour réaliser une attaque (ex. vérification de programmes malveillants);
- respecter les moyens d'accès et les règles définies par l'Acquéreur et fournies au Fournisseur au préalable (ex. respecter le plan d'adressage réseau et les temps de réponse communiqués par l'Acquéreur);
- s'assurer que quiconque intervenant pour le compte du Fournisseur ayant besoin d'utiliser les systèmes de l'Acquéreur est dûment autorisé par le Fournisseur et que ses données d'identification ont été fournies à l'Acquéreur ;
- s'assurer que seules les ressources du Fournisseur dûment autorisées sont connectées aux systèmes de l'Acquéreur.

Ressources du Fournisseur

NOTA: Cette section est seulement applicable entre l'Acquéreur d'Orange et le Fournisseur. Pour DTAG, le Fournisseur accèdera uniquement au réseau de l'Acquéreur en utilisant la solution d'accès distant de DTAG.

Si les Ressources du Fournisseur sont utilisées pour accéder et/ou s'interconnecter avec les systèmes de l'Acquéreur, le Fournisseur s'engage à :

- suivre les bonnes pratiques de sécurité de gestion de ces Ressources (ex : maintenir les Ressources à jour avec les derniers patchs de sécurité tels que les anti-malware logiciel et des patchs des systèmes d'exploitation, configurer des privilèges restreints pour les utilisateurs, configurer la restriction des droits d'exécution depuis des supports amovibles, mettre en place des mécanismes de verrouillage de sessions sur les Ressources après une courte période d'inactivité…) ;
- s'assurer que les Ressources (incluant les tokens d'authentification , les mobiles et les numéros de téléphone associés) sont dédiées au Fournisseur et seulement utilisées par ses employés et tiers convenus pour fournir les Livrables ;
- mettre en place un contrôle d'accès réseau sur les Ressources du Fournisseur utilisées pour l'exécution du service ;
- mettre en place un système d'authentification forte (ex. authentification à deux facteurs) pour les accès à ces Ressources, et assurer la traçabilité de l'utilisation de ces Ressources pour tous les utilisateurs ;
- conserver ces journaux pour la durée convenue dans le NPA et/ou la Commande (y compris les documents associés tels qu'un Accord de Confidentialité ou un Contrat de Traitement des Données), ou défaut pour une durée maximum de 6 mois ;
- fournir à l'Acquéreur à sa demande un extrait des journaux conservés.

Si l'Acquéreur fournit des comptes au Fournisseur, le Fournisseur s'engage à :

- assurer la traçabilité de l'attribution et l'utilisation de ces comptes;

- conserver les traces associées pendant la durée convenue dans le NPA et/ou la Commande (y compris les documents associés tels qu'un Accord de Confidentialité ou un Contrat de Traitement des Données), ou défaut pour une durée maximum de 6 mois.; et
- fournir à l'Acquéreur à sa demande un extrait des traces conservées.

Systèmes et applications de l'Acquéreur

Si l'Acquéreur fournit des comptes au Fournisseur, le Fournisseur s'engage à :

- notifier sans délai l'Acquéreur lorsqu'un compte n'est plus nécessaire et ;
- s'assurer que les comptes fournis pour des communications serveur sont utilisés pour cette seule finalité.

Management des Ressources de l'Acquéreur

Si l'Acquéreur fournit des Ressources Physiques (logiciel, matériel, ordinateur, clé USB, badge, tablette, smartphone, accès ou équipement d'interconnexion …) au Fournisseur, celui-ci doit surveiller et contrôler étroitement l'utilisation de ces Ressources. A la fin du contrat, le Fournisseur s'engage à restituer les Ressources de l'Acquéreur encore en sa possession.

SERVICES PROFESSIONNELS ET SÉCURITÉ

Sensibilisation et Formation

Le Fournisseur doit s'assurer que ses employés ainsi que les tiers participant à la fourniture des Livrables :

- possèdent les compétences de sécurité appropriées (e.x pour gérer les incidents de sécurité); et
- connaissent le contenu et la mise en œuvre des règles de sécurité.

Les règles de sécurité spécifiques à l'Acquéreur

Si l'Acquéreur fournit des règles spécifiques de sécurité pour réaliser les Services Professionnels, le Fournisseur doit s'assurer que ses employés et tous les tiers sont informés des règles avant le démarrage des activités.

Sous-Traitants

Si le Fournisseur fait appel à des sous-traitants pour réaliser le contrat de l'Acquéreur, le Fournisseur doit spécifiquement les identifier comme des sous-traitants et s'assurer de la mise en œuvre des mesures appropriées nécessaires au respect des exigences du présent document .

Traitement des Livrables sensibles

Sur demande particulière de l'Acquéreur et en accord avec le Contrat, le Fournisseur s'engage à employer uniquement du personnel ayant fait l'objet d'une procédure de vérification (ex. vérifications par les autorités nationales), pour traiter des Livrables sensibles, et ce aussi bien avant le déploiement que durant toute la phase opérationnelle de maintenance.

DÉFINITIONS ET ABRÉVIATIONS

Contrat	désigne tout contrat signé par BuyIn, DTAG et/ou Orange avec le Fournisseur et contenant la référence à la présente ISA.
Actifs	désigne, conformément à la norme ISO/IEC 27005, les actifs primaires et actifs supports.
Backdoor	désigne une fonctionnalité ou un défaut d'un Livrable permettant un accès non autorisé discret/furtif aux données.

CVE	signifie « Common Vulnerabilities and Exposures » tel que défini sur le site http://cve.mitre.org/index.html.
CVSS	signifie « Common Vulnerability Scoring System » tel que défini sur le site http://www.first.org/cvss/.
Anomalie	désigne toute déviation de la qualité réelle du Livrable au regard de la qualité convenue contractuellement (ex. défaut, non-conformité des Livrables au regard des spécifications, défaut d'exécution conforme à la documentation associée).
Livrables	désigne tout équipement, produit et/ou service commandé sur la base du Contrat principal, y compris toutes les obligations majeures et accessoires.
Sécurité des informations	désigne, conformément aux normes ISO/IEC 27001 et ISO/IEC 27005, la sécurité dans le cadre du traitement des informations et des activités (actifs primaires) reposant sur des ressources techniques (y compris, entre autres, des technologies de l'information, des locaux, des installations et des réseaux) et non techniques (y compris, de façon non limitative, des actifs supports tels que du personnel, des partenaires, des organisations, des procédures et des conditions générales).
NPA	désigne un contrat conclu par une Société Affiliée de DTAG ou Orange dans le cadre d'un Accord-cadre de BuyIn, DTAG ou Orange, selon le cas, conclu par BuyIn. NPA correspond aux termes « Accord d'exécution », « Accord Propre au Projet » et « Accord du Projet » : toute disposition utilisant le terme « NPA » s'appliquera à ce type d'accords également.
Correctif Officiel	désigne une solution mise à disposition par le Fournisseur pour corriger complètement une Vulnérabilité, par un patch officiel ou une mise à jour.
Commande	désigne un bon de commande émis par l'Acquéreur. « Commande » correspond au terme « Bon de Commande » dans les Accords conclus par DTAG et ses Sociétés Affiliées. Toute disposition utilisant le terme « Commande » s'appliquera de la même façon à « Bon de Commande ».
Acquéreur	désigne la Société Affiliée DTAG ou Orange en tant que partie au NPA ou à la Commande. « Acquéreur » correspond au terme « Partie Passant une Commande » dans les Accords conclus par DTAG et/ou Orange et ses Sociétés Affiliées. Toute disposition établie à l'égard de l'Acquéreur dans la présente ISA s'appliquera de la même façon à la « Partie émettant une Commande ».
Réseau de l'Acquéreur	désigne le réseau géré par l'Acquéreur ainsi que toutes les infrastructures d'accès réseaux nécessaires pour les communications entre les Ressources de chacune des parties.
Ressources de l'Acquéreur	désigne les matériels, logiciels et/ou services appartenant à l'Acquéreur utilisés pour la fourniture des Livrables.
Production logicielle	désigne un logiciel : (i) s'appuyant principalement et/ou étant réalisé sur la base des exigences de DTAG et/ou Orange, et/ou les spécifications fournies par ou exclusivement pour l'Acquéreur, et/ou (ii) développé ou mis en oeuvre par le Fournisseur dans le cadre de ce Contrat (et/ou tout amendement ultérieur), et/ou tout TSA et/ou tout NPA et/ou toute Commande, et qui n'a pas d'antériorité. que celui-ci soit ou non protégé par des droits de propriétés intellectuelles, de même que tous les produits ou procédés résultant de celui-ci.
Statement of Compliance	désigne une annexe au Contrat décrivant les exigences de sécurité technique détaillées sur les Livrables.
Cahier des charges	désigne un document définissant les activités, Livrables et jalons d'un projet pour la fourniture de Livrables et/ou services par le Fournisseur à l'Acquéreur.
Ressources du Fournisseur	désigne les matériels, logiciels et/ou services appartenant au Fournisseur utilisés pour la fourniture des Livrables.

Correctif Temporaire	désigne un correctif mis à disposition du Fournisseur permettant de corriger temporairement une Vulnérabilité (ex. correctifs, outils ou solutions de contournement temporaires)
Vulnérabilité	désigne une faiblesse impactant la disponibilité, l'intégrité ou la confidentialité.
XaaS	désigne le modèle de fourniture en tant que service, incluant le SaaS (Software as a Service), le PaaS (Platform as a Service), le IaaS (Infrastructure as a Service) ou équivalent.
Zero-Day	désigne une Vulnérabilité non divulguée que des hackers peuvent exploiter pour porter atteinte à la sécurité des Livrables. La Vulnérabilité est dénommée "zero-day" (ou "zero-hour", ou "0-day" ou "day zero") parce que celle-ci n'a pas été publiquement signalée ou communiquée avant d'être utilisée, laissant le Fournisseur sans délai pour développer des correctifs ou proposer des solutions permettant de réduire l'impact.

- fin du document -