Fiche de traitement des données à caratère personnel n°2840

Définition du traitement

Nom du traitement :

Le Cnam - Elections professionnelles

Dates du scrutin :

Scrutin du jeudi 01 décembre 08:00 au jeudi 08 décembre 17:00

Description du traitement :

Mise en place d'une solution de vote électronique pour le compte de **Le Cnam**

Finalité du traitement :

Respect d'une obligation légale : Organiser des élections conformes à la réglementation, permettre l'identification et l'authentification des utilisateurs et le suivi des membres du bureau et organisateurs

Enjeux du traitement :

Garantir un accès sécurisé aux plateformes de votes et la sincérité du scrutin

Méthode d'authentification :

Un identifiant généré aléatoirement par le système est envoyé sur l'adresse institutionnelle.
L'électeur se connecte à l'aide de cet identifiant et des 4 derniers chiffres de son numéro de sécurité sociale (hors clé)
Il doit alors saisir un numéro de téléphone pour recevoir un code à usage unique lui permettant ainsi d'accéder à son espace (scrutins / listes électorales / candidatures).

Responsable du traitement :

Le Cnam
292 Rue Saint-Martin
75141 PARIS CEDEX 03
Siret : 19753471200017

Sous-traitant :

LegaVote SARL
110 av. Barthelemy Buyer
69009 LYON

Référence du traitement :

Fiche de registre n°2840

Date de création du traitement :

16/05/2022

Mise à jour du traitement :

07/09/2022

Suppression des données :

Suppression de la totalité des données prévue le 09/12/2024.
Avant suppression définitive, la société LegaVote en demandera l'autorisation au responsable du traitement.
Une fois la suppression déclenchée, le responsable du traitement recevra automatiquement un PV de confirmation de destruction des données.

Contacts

Responsable du traitement : Le Cnam

Valia Morgenbesser
Adresse email : valia.morgenbesser@lecnam.net

Sous-traitant : LegaVote

Hamza Mhannaoui
Téléphone : 06 27 56 74 67
Adresse email : h.mhannaoui@legavote.fr

Eva Perréol
Chef de projet
Téléphone : 06 64 63 28 55
Adresse email : eva@legavote.fr

Données personnelles concernées

Données concernant les électeurs

Données concernées	Description	Durée de conservation
Nom / Prénom	Données transmises utilisées pour identifier l'électeur afin de remplir la fiche d'émargement	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Adresse email	Donnée transmise nécessaire à l'envoi des codes d'accès	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Numéro de téléphone	Donnée récoltée au moment de la connexion de l'électeur afin de sécuriser l'authentification	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Date de naissance	Donnée transmise à des fins de contrôle des homonymes	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Numéro étudiant / numéro de personnel ou autre donnée non triviale	Donnée transmise pour confirmer l'identité de l'électeur lors de son authentification, voir méthode d'authentification	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Composante/collège/secteur	Données transmises nécessaires à l'affectation aux scrutins	Jusqu'à expiration des délais de recours et d'archivages réglementaires

Données concernant les candidats

Données concernées	Description	Durée de conservation
Nom / Prénom	Données transmises permettant d'identifier les candidats	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Sexe	Donnée transmise à des fins de contrôles de la conformité des candidatures	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Date de naissance	Donnée transmise afin de gérer les potentiels cas d'égalité	Jusqu'à expiration des délais de recours et d'archivages réglementaires

Données concernant les membres du bureaux, organisateurs, experts

Données concernées	Description	Durée de conservation
Nom / Prénom	Données transmises utilisées pour établir les PV	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Adresse email	Donnée transmise nécessaire pour la création de l'accès aux interfaces de suivi et la signature des PV	Jusqu'à expiration des délais de recours et d'archivages réglementaires
Numéro de téléphone	Donnée optionnelle renseignée par l'utilisateur permettant la signature numérique des PV	Jusqu'à expiration des délais de recours et d'archivages réglementaires

Mesures de sécurité

Chiffrement

L'intégralité des données présentes au sein de la base de données sont chiffrées à l'aide d'un procédé de chiffrement au repos (AES256).
Le flux de synchronisation entre la plateforme principale et celle de secours est chiffré. Tous les échanges de données entre les plateformes de vote et les utilisateurs sont chiffrés via le protocole https (TLS 1.2 et 1.3).
Le bulletin est chiffré directement sur le navigateur de l'électeur (RSA4096) puis inséré dans une enveloppe chiffrée (RSA2048+AES256) et utilise un flux continu pour aller dans une urne numérique sans horodatage (ne permettant ainsi aucun rapprochement avec l'électeur).
Une fois le scrutin terminé, l'archive de la plateforme est conservée chiffrée (chiffrement AES256).
Certaines données importées au sein du système sont chiffrées avec un sel (BCRYPT) ne permettant plus à quiconque d'accéder à la donnée d'origine. C'est notamment le cas pour la conservation de la donnée non triviale permettant l'authentification des électeurs.

Anonymisation

Le vote s'effectue à bulletin secret et ne permet pas de rapprochement entre un bulletin et l'électeur.

Cloisonnement des données

Une plateforme de vote indépendante est générée pour chaque prestation de la société LegaVote.
Toutes les données à caractère personnel sont échangées via une zone de partage de documents sur ladite plateforme ne permettant qu'aux chefs de projets responsables de l'organisation de télécharger les documents.

Contrôle des accès logiques des électeurs

Un identifiant généré aléatoirement par le système est envoyé sur l'adresse institutionnelle.
L'électeur se connecte à l'aide de cet identifiant et des 4 derniers chiffres de son numéro de sécurité sociale (hors clé)
Il doit alors saisir un numéro de téléphone pour recevoir un code à usage unique lui permettant ainsi d'accéder à son espace (scrutins / listes électorales / candidatures).
Après 5 tentatives infructueuses, le compte est bloqué et doit faire l'objet d'un traitement par l'équipe technique de la société LegaVote.

Contrôle d'intégrité

Intégrité des données : Nous utilisons un stockage des données en base InnoDB qui permet des transactions ACID (atomiques, cohérentes, isolées et durables).

Intégrité des fichiers : Chaque connexion au serveur et chaque modification de fichier

déclenche une notification à l'équipe technique LegaVote.
Dans le cas où un vote est scellé, ces notifications sont également envoyées par email aux membres du bureau et organisateurs du vote.

Au niveau de la plateforme de vote, toutes les minutes, un processus automatique vient contrôler l'intégrité de certaines données ou fichiers, en plus des contrôles manuels en début/fin d'élection et des contrôles potentiellement déclenchés par les membres du bureau.

Traçabilité

L'ensemble des actions utilisateurs (dates de connexions, erreurs de connexions, téléchargement de fichiers, accès aux ...) sont journalisées dans les registres d'activité de la plateforme de vote.
Ces registres sont horodatés (à l'aide d'un système d'horodatage fourni par un tiers de confiance qualifié, certifié RGS*) à intervalles réguliers rendant toute reprise du registre impossible et garantissant ainsi son intégrité.

Disponibilité et résilience constante

Chaque système de vote est installé sur 2 hôtes en réplication sur 2 datacenters différents, distincts de 2 régions, que ce soit sur du niveau de sécurité CNIL 1, 2 ou 3.
Les données sont constamment répliquées sur 6 points de stockages.
Pour palier instantanément à toute panne matérielle, il est procédé à un basculement automatique d'un hôte à l'autre sans intervention ni coupure et sans perte de donnée (sur parc private cloud certifié ANSSI SecNumCloud avec technologie vSphere).
En cas de défaillance du datacenter entier (type incendie du datacenter), le basculement est également opéré sans perte de données sur le datacenter de secours.

Surveillance

Nos plateformes de vote sont constamment surveillées par des outils de monitoring internes et externes et renvoient des notifications email et sms au responsable de notre infrastructure et notre directeur technique, 24h/24, 7j/7.

Procédures de tests

Nous effectuons tous les trimestres un test de basculement d'hôte, de restauration d'archive de vote et de migration du datacenter pour contrôler l'efficacité de nos procédures.

Sous traitants

Nom du sous-traitant	Finalité	Lieu de traitement	Conformité art 28
OVH Cloud	Hébergement des plateformes de vote	Roubaix - France Strasbourg - France	Oui
OVH Cloud	Hébergement des sauvegardes	Roubaix - France	Oui
OVH Cloud	Hébergement de notre propre service d'envoi d'emails (service principal)	Roubaix - France	Oui
OVH Cloud	Service d'envoi de SMS (service principal)	Roubaix - France	Oui
Maileva	Service d'envoi de courriers postaux	site du Mans (NGA) - France Nanteuil-lès-Meaux et Crécy-la-Chapelle - France	Oui
Novarchive	Système d'Archivage Electronique	La Plaine Saint-Denis - France Clichy - France	Oui
Mailjet	Service d'envoi de SMS (service de secours)	Europe	Oui
Mailjet	Service d'envoi d'emails (service de secours)	Europe	Oui
AWS Paris	Service d'envoi d'emails (service de secours)	Paris, France	Oui

Détails des traitements

OVH Cloud - Hébergement des plateformes de vote

2, rue Kellermann - 59100 Roubaix

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs Membres du bureau Experts Organisateurs	Toutes les données	Hébergement du serveur principal
Electeurs Membres du bureau Experts Organisateurs	Toutes les données	Hébergement du serveur de secours

Localisation du traitement

Société	Finalité	Localisation
OVH - France	Hébergement du serveur principal	Roubaix - France
OVH - France	Hébergement du serveur de secours	Strasbourg - France

Durées de conservation des données

Données concernées	Finalité	Durée
Toutes les données	Déroulement des opérations de vote	jusqu'au 19/12/2022

OVH Cloud - Hébergement des sauvegardes

2, rue Kellermann - 59100 Roubaix

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs Membres du bureau Experts Organisateurs	Toutes les données	Hébergement des sauvegardes de la plateforme de vote utilisée

Localisation du traitement

Société	Finalité	Localisation
OVH - France	Hébergement du serveur contenant les archives	Roubaix - France

Durées de conservation des données

Données concernées	Finalité	Durée
Toutes les données	Conservation des sauvegardes de la plateforme de vote contenant le code source de l'application et les données	jusqu'au 09/12/2024

OVH Cloud - Hébergement de notre propre service d'envoi d'emails (service principal)

2, rue Kellermann - 59100 Roubaix

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs	Adresse email, nom, prénom de l'électeur	Envoi des emails permettant l'authentification sur la plateforme de vote
Electeurs	Adresse email, nom, prénom de l'électeur Fichier PDF contenant l'adresse IP de l'électeur	Envoi des accusés de réception de vote
Membres du bureau Experts Organisateurs	Adresse email, nom, prénom	Envoi des pdf de scellements aux membres du bureau
Membres du bureau Experts Organisateurs	Adresse email, nom, prénom	Envoi des alertes par email
Membres du bureau Experts Organisateurs Observateurs	Adresse email, nom, prénom	Envoi des emails permettant la création des comptes

Localisation du traitement

Société	Finalité	Localisation
OVH - France	Hébergement de notre service d'envoi d'emails	Roubaix - France

Durées de conservation des données

Données concernées	Finalité	Durée
Contenu de l'email avec entêtes	Permettre l'envoi initial (et le renvoi si le serveur de destination n'est pas disponible)	maximum 48 heures

OVH Cloud - Service d'envoi de SMS (service principal)

2, rue Kellermann - 59100 Roubaix

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs	Numéro de téléphone, nom, prénom de l'électeur	Envoi de SMS permettant l'authentification sur la plateforme de vote
Membres du bureau de vote	Numéro de téléphone portable du membre du bureau de destination (si envoi de clé par SMS)	Envoi de clés aux membres du bureau de vote
Membres du bureau de vote	Numéro de téléphone portable du membre du bureau de destination	Envoi de SMS permettant la signature numérique des PV

Localisation du traitement

Société	Finalité	Localisation
OVH - France	Hébergement du service d'envoi de SMS	Roubaix - France

Durées de conservation des données

Données concernées	Finalité	Durée
Contenu du SMS Adresse email du destinataire Date d'envoi	Permettre l'envoi initial puis la conservation de statistiques d'envoi	90 jours

Maileva - Service d'envoi de courriers postaux

45/47 boulevard Paul Vaillant Couturier - 94200 Ivry-sur-Seine (France)

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs	Nom, prénom et adresse postale de l'électeur	Envoi des accès aux électeurs par courriers postaux

Localisation du traitement

Société	Finalité	Localisation
Maileva	Avant d'être envoyées en production, les données subissent une série d'actions techniques de prétraitement.	site du Mans (NGA) - France
Maileva	les données sont envoyées dans les serveurs des chaines éditiques de Maileva (Nanteuil-lès-Meaux et Crécy-la-Chapelle) pour impression, mise sous pli, affranchissement et remise physique des courriers au prestataire postal (La Poste).	Nanteuil-lès-Meaux et Crécy-la-Chapelle - France

Durées de conservation des données

Données concernées	Finalité	Durée
Toutes les données transmise à Maileva par LegaVote	Permettre la génération des données de production et le traitement des réclamations	90 jours après l'envoi
Données de production (générée à partir des données transmises)	Permettre l'envoi initial et le suivi des courriers	30 jours après l'envoi
Données de suivi après production (contenant pavés adresses des destinataires et références des courriers)	Statistiques d'envoi	400 jours après l'envoi
Logs contenant des informations de traçabilité des opérations clients ou des opérations internes	Assurer la traçabilité des opérations	90 jours après l'envoi
Toute les données (Serveurs de backup)	Assurer une continuité de service en cas de défaillance du système principal	48 heures

Novarchive - Système d'Archivage Electronique

22 RUE HENRI BARBUSSE 92110 CLICHY

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs Membres du bureau Experts Organisateurs Observateurs	La copie des programmes sources et des programmes exécutables La configuration du vote Les listes électorales finales (et mise à jour avec les changements de coordonnées) Les listes des demandes de rectifications Les listes d'émargement Les procès-verbaux de dépouillement Les registres d'activité L'ensemble des bulletins cryptés et décryptés	Archivage des éléments de contrôle a posteriori en fin d'élection pendant les délais réglementaires d'archivage

Localisation du traitement

Société	Finalité	Localisation
Datacenter Interxion IX5	Site de stockage principal	La Plaine Saint-Denis - France
Siège du groupe Rousselet	Site de stockage secondaire	Clichy - France

Durées de conservation des données

Données concernées	Finalité	Durée
Toutes les données transmises à Novarchive	Conservation des éléments de contrôle a posteriori	jusqu'au 09/12/2024

Mailjet - Service d'envoi de SMS (service de secours)

13bis rue de l'Aubrac, 75012 Paris (France)

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs	Numéro de téléphone, nom, prénom de l'électeur	Envoi de SMS permettant l'authentification sur la plateforme de vote
Membres du bureau de vote	Numéro de téléphone portable du membre du bureau de destination (si envoi de clé par SMS)	Envoi de clés aux membres du bureau de vote
Membres du bureau de vote	Numéro de téléphone portable du membre du bureau de destination	Envoi de SMS permettant la signature numérique des PV

Localisation du traitement

Société	Finalité	Localisation
Google Cloud Platform	Sites de stockage	Europe

Durées de conservation des données

Données concernées	Finalité	Durée
Numéro de téléphone du destinataire Date d'envoi du message	Permettre l'envoi initial puis la conservation de statistiques d'envoi	90 jours
Contenu du SMS	Permettre uniquement l'envoi initial	Pas de conservation une fois le message délivré

Mailjet - Service d'envoi d'emails (service de secours)

13bis rue de l'Aubrac, 75012 Paris (France)

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs	Adresse email, nom, prénom de l'électeur	Envoi des emails permettant l'authentification sur la plateforme de vote
Electeurs	Adresse email, nom, prénom de l'électeur Fichier PDF contenant l'adresse IP de l'électeur	Envoi des accusés de réception de vote
Membres du bureau Experts Organisateurs	Adresse email, nom, prénom	Envoi des pdf de scellements aux membres du bureau
Membres du bureau Experts Organisateurs	Adresse email, nom, prénom	Envoi des alertes par email
Membres du bureau Experts Organisateurs Observateurs	Adresse email, nom, prénom	Envoi des emails permettant la création des comptes

Localisation du traitement

Société	Finalité	Localisation
Google Cloud Platform	Sites de stockage	Europe

Durées de conservation des données

Données concernées	Finalité	Durée
Sujet de l'email Contenu de l'email Données expéditeur/destinataire	Permettre le bon acheminement	5 jours
Sujet de l'email Adresse email de destination	Affichage des statistiques	3 mois

AWS Paris - Service d'envoi d'emails (service de secours)

38 AV JOHN F KENNEDY L 1855 - 99137 LUXEMBOURG

Données concernées

Catégories de personnes	Données concernées	Fonctionnalité
Electeurs	Adresse email, nom, prénom de l'électeur	Envoi des emails permettant l'authentification sur la plateforme de vote
Electeurs	Adresse email, nom, prénom de l'électeur Fichier PDF contenant l'adresse IP de l'électeur	Envoi des accusés de réception de vote
Membres du bureau Experts Organisateurs	Adresse email, nom, prénom	Envoi des pdf de scellements aux membres du bureau
Membres du bureau Experts Organisateurs	Adresse email, nom, prénom	Envoi des alertes par email
Membres du bureau Experts Organisateurs Observateurs	Adresse email, nom, prénom	Envoi des emails permettant la création des comptes

Localisation du traitement

Société	Finalité	Localisation
AWS Paris	Stockage des données sur 3 zones de disponibilité	Paris, France