CHECK-ELECTRO

Suivi de chantiers électrique et chauffage

Conditions d’utilisation et information sur la protection des données

Version 2.2 · 1er novembre 2026

1. Responsable, champ d’application et contact

Le site Check-Electro et l’application « Suivi de chantiers électrique et chauffage » sont exploités par Étienne Collaud (ci-après « l’exploitant »). Ces conditions s’appliquent au site, au formulaire de renseignements, à la démo et aux espaces clients. Pour toute question ou demande relative aux données, utilisez le formulaire de cette page en indiquant « Protection des données ».

La LPD protège les données personnelles des personnes physiques. Selon la fonction concernée, l’exploitant peut agir comme responsable du traitement (par exemple pour les demandes reçues par le formulaire, la gestion des comptes et la sécurité du service) ou comme sous-traitant lorsqu’il héberge et traite des données pour le compte d’une entreprise cliente. Le rôle concret dépend des décisions prises et des instructions données pour le traitement.

Pour les données de chantier et les données de leurs collaborateurs ou contacts, les administrateurs de l’entreprise cliente choisissent les personnes autorisées, leurs droits et les données saisies. L’entreprise cliente détermine les finalités et les instructions relevant de son activité; l’exploitant traite les données nécessaires au fonctionnement du service selon les instructions convenues et ses obligations légales.

2. Période gratuite et abonnement

L’application est gratuite pendant sa phase de démarrage, jusqu’au 31 décembre 2026 inclus. À partir du 1er janvier 2027, la poursuite de l’utilisation nécessitera un abonnement à très bas coût. Le prix exact, les prestations incluses et les modalités seront communiqués avant toute souscription. Aucun abonnement payant ne sera activé sans information préalable sur son prix et ses conditions.

3. Données traitées et finalités

Selon les fonctions utilisées, les données peuvent inclure : nom, société, coordonnées, messages, données de connexion, adresse e-mail et adresse IP d’une demande de démo, comptes utilisateurs, chantiers, contacts, mesures, rapports, photos, plans, documents, équipements et journaux techniques ou de suivi.

Elles sont utilisées pour répondre aux demandes, fournir les fonctions, gérer les comptes, assurer l’assistance, protéger le service, détecter les abus et respecter les obligations légales. Elles ne sont pas vendues. Les informations d’une entreprise sont accessibles aux administrateurs et utilisateurs autorisés par cette entreprise, ainsi qu’aux prestataires nécessaires au service dans la mesure de leurs fonctions.

4. Obligations principales de protection des données (LPD)

Chaque responsable du traitement respecte les exigences qui s’appliquent à son rôle et au traitement concerné. En particulier, il doit :

- Traiter les données de manière licite, de bonne foi et proportionnée; les collecter pour des finalités déterminées et reconnaissables, limiter les données à ce qui est nécessaire et les supprimer ou les anonymiser lorsqu’elles ne sont plus nécessaires, sous réserve des obligations de conservation.
- Informer les personnes concernées de façon préalable, claire, compréhensible et facilement accessible. L’information indique notamment l’identité et les coordonnées du responsable, les finalités et, le cas échéant, les destinataires, les pays de destination et les garanties applicables aux transferts à l’étranger.
- Maintenir les données exactes et prendre des mesures raisonnables pour les corriger ou les effacer lorsqu’elles sont inexactes et que la loi le prévoit.

- Protéger les données par des mesures techniques et organisationnelles adaptées aux risques, à la nature des données et à l'état de la technique. Ces mesures visent notamment à prévenir l'accès, la divulgation, la perte, l'altération ou la destruction non autorisés; elles sont réévaluées lorsque les risques ou les systèmes évoluent.
- Respecter la protection des données dès la conception et par défaut : limiter par défaut les données et accès au nécessaire, et intégrer les exigences de protection au développement et au fonctionnement des outils.
- Encadrer la sous-traitance par des instructions et des engagements appropriés. Le sous-traitant ne traite les données que pour les finalités convenues, protège leur confidentialité et leur sécurité et informe le responsable sans délai injustifié d'une violation de sécurité.
- Répondre aux demandes d'accès et, lorsque la loi le permet, de rectification, d'effacement ou de remise/portabilité. Une vérification raisonnable de l'identité peut être demandée; des exceptions légales et des obligations de conservation peuvent limiter une demande.
- Effectuer une analyse d'impact avant un traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux; si un risque élevé subsiste après les mesures prévues, consulter le PFPDT lorsque la loi l'exige.
- Notifier au PFPDT, aussi rapidement que possible, une violation de la sécurité susceptible d'engendrer un risque élevé pour la personnalité ou les droits fondamentaux. Informer également les personnes concernées lorsque cela est nécessaire à leur protection ou lorsque le PFPDT l'ordonne.
- Respecter les conditions applicables avant toute communication de données personnelles à l'étranger et documenter, lorsque la loi l'exige, les activités de traitement et les mesures prises. Des exceptions ou règles particulières peuvent s'appliquer selon la situation.

Les droits et obligations dépendent des faits, des rôles et des exceptions prévues par la LPD. Cette liste résume des obligations principales et ne constitue pas une garantie que chaque traitement est conforme par sa seule mention dans ces conditions.

5. Identifiants et sécurité des accès

- Chaque utilisateur conserve ses identifiants confidentiels, choisit un mot de passe unique et suffisamment robuste, ne le partage pas et verrouille ses appareils.
- L'entreprise cliente attribue à chacun uniquement les droits nécessaires, contrôle régulièrement les comptes et retire sans délai l'accès des personnes qui n'en ont plus besoin.
- L'utilisateur signale immédiatement à l'administrateur de son entreprise tout accès suspect, perte d'appareil, divulgation d'identifiants ou activité inhabituelle. Il cesse d'utiliser un appareil possiblement compromis.
- L'entreprise et ses utilisateurs maintiennent à jour leurs appareils, navigateurs et logiciels de sécurité, protègent leur réseau et évitent les postes partagés ou réseaux non fiables pour accéder à des données confidentielles.

L'exploitant met en œuvre des mesures adaptées à son service et réévalue les risques. Aucun service accessible par Internet ne peut garantir une sécurité absolue contre toute intrusion, attaque, panne ou erreur. L'utilisateur contribue à la protection de son compte et de son environnement informatique. Cette limite ne supprime aucune obligation légale de l'exploitant ou d'un autre responsable du traitement.

6. Données du client, sauvegardes et pertes

L'entreprise cliente répond des données qu'elle saisit, importe, partage ou exporte : exactitude, actualité, finalité, autorisations, confidentialité et droits de tiers. Elle évite d'enregistrer des données sensibles ou excessives qui ne sont pas nécessaires à ses travaux et informe les personnes concernées des traitements dont elle détermine les finalités.

L'application est un outil de travail et ne constitue pas, à elle seule, une archive ou une sauvegarde indépendante. L'entreprise exporte régulièrement les données et documents essentiels, conserve des copies sur un support distinct et vérifie qu'elle peut les relire. Avant toute suppression, remplacement ou modification importante, elle vérifie ses copies et exports.

Dans les limites du droit applicable, l'exploitant n'est pas responsable d'une perte ou altération résultant d'un défaut de sauvegarde côté client, d'une suppression ou modification par un utilisateur autorisé, d'informations erronées fournies par le client, d'un appareil ou compte client compromis ou d'un événement

échappant raisonnablement à son contrôle. Cette répartition ne couvre pas un dommage dont l'exploitant doit répondre en vertu du droit impératif.

7. Utilisations interdites et réaction aux abus

Il est interdit de tenter d'accéder à un compte, une entreprise ou un chantier sans autorisation, de contourner une mesure de sécurité ou une limitation de droits, de sonder ou tester le système sans accord écrit, d'extraire ou copier massivement les données, de perturber le service, d'introduire un virus ou code malveillant, d'usurper une identité ou d'utiliser le site pour enfreindre la loi ou les droits d'autrui.

En présence d'un motif raisonnable de sécurité, d'abus ou d'obligation légale, l'exploitant peut suspendre ou limiter un compte ou une fonction, préserver les journaux utiles et coopérer avec les autorités conformément à la loi. Lorsque cela est possible et ne compromet pas une enquête ou la sécurité, l'entreprise concernée est informée. L'utilisateur répond, dans les limites de la loi et des accords applicables, des dommages directs prouvés causés par son utilisation illicite ou la violation de ses obligations.

8. Disponibilité, décisions professionnelles et responsabilité

Le service peut être temporairement indisponible pour maintenance, incident, réseau ou panne d'un prestataire. Les fonctions, calculs, mesures, rapports et modèles générés sont des aides à l'organisation et à la documentation; ils ne remplacent pas le jugement d'un professionnel qualifié, les normes applicables ni les vérifications indépendantes nécessaires. Avant signature, transmission ou décision de sécurité, l'utilisateur compétent vérifie les valeurs, hypothèses, calculs et documents.

Dans la mesure autorisée par le droit suisse, l'exploitant n'est pas responsable des dommages indirects, pertes de bénéfice, d'exploitation ou de données résultant d'un usage inadapté, d'une faute de l'utilisateur, d'une indisponibilité externe ou d'un incident indépendant de sa volonté. Aucune disposition n'exclut une responsabilité qui ne peut être écartée par avance, notamment en cas de dol ou de faute grave, ni les droits impératifs des consommateurs ou des personnes concernées.

9. Conservation et exercice des droits

Les données sont conservées selon leur finalité, pendant la durée du compte, du suivi de la demande ou des obligations légales, puis supprimées ou anonymisées lorsqu'elles ne sont plus nécessaires, sous réserve des sauvegardes et délais légaux. Des prestataires techniques peuvent traiter des données pour l'hébergement et l'exploitation du service.

Toute demande d'accès, de rectification ou d'effacement peut être adressée via le formulaire de la page en précisant « Protection des données ». Les droits de remise ou de portabilité s'exercent dans les conditions définies par la LPD. L'identité du demandeur peut être vérifiée. Les demandes peuvent être limitées dans les cas prévus par la loi, notamment en présence d'obligations légales de conservation ou de droits de tiers.

10. Droit applicable et for

Le droit suisse s'applique. Dans la mesure où une convention de for est légalement admissible, les tribunaux compétents du canton de Fribourg sont désignés. Les fors impératifs prévus par la loi, notamment ceux protégeant les consommateurs et les personnes concernées par les données, demeurent réservés.

Sources officielles et informations complémentaires

Loi fédérale sur la protection des données (LPD, RS 235.1), notamment art. 6 à 9, 12, 16, 19, 22 à 24, 25 et 28 : fedlex.admin.ch - LPD.

PFPDT - Devoir d'informer : edoeb.admin.ch/fr/devoir-dinformer.

PFPDT - Sécurité de l'information et notification des violations : edoeb.admin.ch/fr/securite-de-linformation.

PFPDT - Analyse d'impact : edoeb.admin.ch/fr/analyse-dimpact-relative-a-la-protection-des-donnees-personnelles.

Ces conditions présentent un résumé informatif. Elles ne remplacent ni l'analyse juridique de chaque traitement ni les mesures opérationnelles requises par la LPD et l'OPDo. Version 2.2 · 1er novembre 2026.