**Logo/En-tête de l’entreprise**

**Date, lieu**

**Nom, Prénom du salarié**

**Objet : Notification de violation potentielle de données personnelles**

Bonjour Madame, Monsieur,

Nous souhaitons vous informer d’un incident de sécurité subit par AKTO, notre opérateur de compétences et pouvant impliquer vos données personnelles.

En effet, AKTO a constaté le 23 mars qu’une intrusion par des personnes externes à l’organisme s’est produite dans leur système d’information.

Les investigations sont encore en cours à ce stade pour déterminer si des informations ont été exfiltrées : cette violation de données pourrait concerner certaines de vos informations personnelles dans le cadre des formations professionnelles auxquelles vous avez participé et qui ont été financées par AKTO et qui peuvent différer selon votre statut au moment de la formation (stagiaire~~s~~ de la formation inscrit à France Travail, salarié, alternant) :

* *Nom, prénom, adresse e-mail, adresse, numéro de téléphone, NIR (dans le cas d’un contrat d’apprentissage)*
* *Date de naissance, sexe, département, commune de naissance*
* *Statut de travailleur handicapé, et droits attachés à la RQTH*
* *Equivalence jeune, extension BOE, inscrit à France Travail (numéro d’inscription, durée en mois)*
* *Nationalité, régime Social, type de minimum social*
* *Inscrit sur la liste de sportif de haut niveau RQTH*
* *Dernier diplôme ou titre préparé, dernière classe / année suivie, intitulé du dernier diplôme ou titre préparé, diplôme ou titre le plus élevé obtenu*
* *Projet de création ou reprise d'entreprise oui / non*

Dès la découverte de l’incident, AKTO a immédiatement mis en œuvre les actions suivantes :

* *Isolement du réseau informatique, renforcement des protocoles de sécurité*
* *Un dépôt de plainte a été effectué ;*
* *Une notification auprès de la Commission Nationale de l’Informatique et des Libertés (CNIL) a également été effectuée, conformément à la réglementation en vigueur.*

Afin de protéger vos informations personnelles, nous vous recommandons de prendre les précautions suivantes : soyez vigilants et attentifs aux signaux faibles et forts à observer au quotidien sur vos appareils

* *Courriel avec hyperlien (phishing)*
* *Pièce jointe douteuse*
* *Connexions ou activités inhabituelles sur vos adresses mail*

Anticipez

* *Modifiez vos mots de passe en les rendant robustes (phrase avec des signets, majuscules, minuscule, chiffres, caractères spéciaux, au moins 12 caractères)*
* *Ne pas inscrire les identifiants et mots de passe de vos outils et autres applications sur un document libre de type OneNote, Text, Word, Excel ou autre tableur sans protection. Utilisez un coffre-fort de mots de passe fiable.*

Soyez réactifs

* *En cas de doute ou de menace avérée, prévenir la DSI / la DPO / le Service XXX*

AKTO et nous-mêmes regrettons très vivement cet incident dont nous sommes victimes, et nous vous assurons de notre plein engagement pour renforcer la sécurité de vos données.

Nous vous tiendrons informés dès que nous aurons plus d’informations concernant cette intrusion, si des mesures supplémentaires devaient être prises de votre côté.

Nous comprenons que cette situation puisse susciter des questions ou demandes d’information complémentaire, vous pouvez nous contacter à l’adresse suivante XXX

Cordialement,

[Nom de l’entreprise] [Coordonnées de l’entreprise]