



CSEC

DECLARATION PREALABLE



12 juin 2025 – IN – CSEC

Monsieur le Président, Mesdames et Messieurs les élus,

Nous sommes aujourd'hui confrontés à une situation d'une gravité inédite pour notre entreprise. Un incident majeur de protection des données personnelles, relevant du RGPD, vient d'être révélé.

Ce qui distingue cet événement des précédents, c'est l'implication directe d'un partenaire externe, gestionnaire d'une partie du parc automobile d'Orange.

À ce jour, l'identité de ce sous-traitant n'a pas été communiquée, ce qui suscite une vive inquiétude parmi les personnels et appelle à une transparence immédiate et totale de la part de la Direction.

Cet incident ne se limite pas à une simple faille technique ou organisationnelle. Il met en cause la sécurité des données de collaborateurs utilisant des véhicules de service et de fonction, tout en exposant Orange à un risque réputationnel majeur.

Dans un contexte où la protection des données personnelles constitue un enjeu de confiance et de responsabilité, chaque nouveau manquement fragilise la crédibilité de notre groupe, déjà mise à mal par la succession d'incidents et de sanctions publiques pour non-respect du RGPD.

Les conséquences de tels événements dépassent le cadre interne : elles sont largement relayées par la presse et les réseaux sociaux, ce qui accentue la perte de confiance de nos clients, partenaires et actionnaires, et peut entraîner des répercussions commerciales et financières durables.

I. Précisions attendues sur la nature et l'ampleur de la fuite

À ce stade, il est établi que des cybercriminels ont pu accéder à différentes catégories de données personnelles, parmi lesquelles figurent les noms et prénoms, les numéros de permis de conduire, les adresses électroniques professionnelles, les plaques d'immatriculation, ainsi que les marques et types de véhicules.

Nous demandons à la Direction de préciser sans délai le périmètre exact des personnels concernés, en indiquant s'il s'agit de l'ensemble des utilisateurs de véhicules de service et de fonction ou seulement d'une partie d'entre eux. Il est également indispensable d'obtenir une liste exhaustive des données compromises, ainsi qu'une confirmation formelle qu'aucune autre information sensible, telle que des données bancaires, médicales ou des adresses personnelles, n'a été exposée.

II. Chronologie détaillée et respect des obligations réglementaires

Pour comprendre pleinement la gestion de cette crise, nous sollicitons la communication d'une chronologie précise des faits : date de la compromission, date de la découverte de l'incident, date de la notification à la CNIL et date d'information des personnels concernés. Il est essentiel de rappeler que la réglementation impose une notification à la CNIL dans un délai de 72 heures après la découverte de l'incident, ainsi qu'une information aux personnes concernées dans les meilleurs délais. Nous attendons la transmission des preuves attestant du respect de ces obligations par Orange et son sous-traitant, ainsi qu'une explication sur la coordination opérée entre les différents acteurs impliqués.

III. Conséquences concrètes pour les personnels et mesures d'accompagnement

Des signalements récents font état de la réception de SMS frauduleux par certains collaborateurs, les invitant à régulariser une amende. Cette situation démontre que des individus malveillants détiennent désormais leurs coordonnées et les plaques d'immatriculation associées à leurs véhicules professionnels.

Les risques encourus par les personnels sont multiples : usurpation d'identité, réception d'amendes injustifiées, tentatives de phishing, et émission de procès-verbaux illégaux en cas d'utilisation frauduleuse de leur permis de conduire.

Face à ces menaces, il est impératif que la Direction mette en place un accompagnement personnalisé pour chaque victime, incluant la désignation d'un référent dédié, la diffusion d'une documentation claire sur les démarches à suivre, et la prise en charge de l'ensemble des démarches de contestation, tant sur le plan administratif que juridique. Il serait inacceptable que les personnels supportent seuls les conséquences de cette défaillance.

IV. Plan d'action correctif et contrôle des partenaires

Nous exigeons la présentation d'un plan d'action détaillé, couvrant à la fois les mesures correctives déjà engagées et celles à venir, aussi bien chez Orange que chez le partenaire concerné. Ce plan devra inclure la description des procédures internes appliquées pour la gestion des incidents de sécurité, les modalités de contrôle et d'audit des sous-traitants ayant accès à des données sensibles, ainsi que les actions prévues pour renforcer la sécurité des systèmes d'information. Il est indispensable que des audits réguliers soient instaurés, en toute indépendance, afin de garantir la conformité des pratiques et la sécurité des traitements opérés par les partenaires externes. Nous attendons également que la Direction précise la répartition des responsabilités entre Orange et son sous-traitant, et qu'elle indique les suites juridiques envisagées en cas de manquement avéré à la réglementation.

V. Transparence sur la communication et gestion de crise

Pour garantir la cohérence et la fiabilité de l'information, nous demandons à être systématiquement tenus informés de toute communication officielle adressée à la presse, aux clients ou aux autorités concernant cet incident. Il est essentiel que les représentants du personnel disposent des mêmes éléments que ceux diffusés publiquement, afin de prévenir toute confusion ou interprétation erronée. Nous attendons également la communication des procédures internes d'Orange et de ses partenaires en matière de gestion des incidents de sécurité, afin de pouvoir évaluer la conformité des pratiques et l'efficacité des dispositifs de réaction.

VI. Suivi, dialogue social et inscription à l'ordre du jour du CSEC

Nous demandons que l'ensemble de ces questions et de ce dossier soient inscrits à l'ordre du jour du prochain CSEC, et qu'un suivi régulier soit assuré jusqu'à la résolution complète de l'incident et la mise en œuvre de toutes les mesures correctives. Il est indispensable que des points d'étape réguliers soient présentés lors des instances représentatives du personnel, afin de garantir la transparence et l'efficacité du dispositif de gestion de crise. Nous attendons également la désignation d'un interlocuteur dédié, chargé de centraliser les retours des personnels et de coordonner l'accompagnement des victimes.

VII. Engagements attendus et conclusion

La sécurité, la conformité réglementaire et la sérénité des personnels d'Orange doivent rester des priorités absolues. Nous attendons de la Direction qu'elle prenne des engagements clairs et concrets sur l'ensemble des points évoqués, qu'elle mette en place un dispositif d'accompagnement à la hauteur de la gravité de la situation, et qu'elle fasse preuve d'une transparence totale dans la gestion de cette crise. Nous vous remercions de bien vouloir confirmer la prise en compte de cette demande et de nous transmettre, dans les meilleurs délais, tous les éléments nécessaires à une discussion constructive lors de la prochaine instance.

Dans l'attente de vos réponses et de vos engagements, nous restons à la disposition de la Direction pour tout échange visant à garantir la protection des personnels et la restauration de la confiance au sein de notre entreprise.



**CHOISISSEZ
CEUX
QUI
AGISSENT !**



Les Elus CFE-CGC du CSEC

Abonnements gratuits : bit.ly/abtCFE-CGC
Tous vos contacts : bit.ly/annuaire CFECGC



cfecgc-orange.org

