Action & Démocratie
Le bureau national

à

Monsieur Edouard GEFFRAY
Ministre de l'Éducation nationale
110, rue de Grenelle
75357 Paris SP 07

Paris, le 25 août 2026

Objet : Sécurité des systèmes d'information et protection des données des personnels

Monsieur le Ministre,

Depuis plusieurs mois, les incidents de cybersécurité affectant les systèmes d'information de l'Éducation nationale se succèdent et prennent une ampleur particulièrement préoccupante.

En mars dernier, une intrusion dans le système COMPAS a conduit à l'exfiltration de données concernant environ 243 000 agents. En avril, une attaque visant ÉduConnect a compromis les données personnelles de plus d'un million d'élèves.

Dans la nuit du 25 juillet, une nouvelle intrusion, réalisée au moyen d'un compte professionnel compromis, a cette fois visé un système d'information consacré à la formation des personnels. Selon les premières informations communiquées par votre ministère, les données susceptibles d'avoir été exfiltrées concernaient des agents ayant exercé en académie depuis 2001 et pouvaient comprendre, outre leur identité et leur situation professionnelle, leur adresse postale, leur numéro de téléphone et, pour certains, leur numéro de sécurité sociale.

L'affaire a pris une dimension nouvelle au mois d'août. Non pas en raison d'une nouvelle intrusion dans ce système, mais parce que les auteurs de l'attaque de juillet l'ont revendiquée et ont publié une partie des données qu'ils affirment avoir dérobées. Votre ministère a indiqué le 18 août avoir constaté cette mise en ligne et poursuivre ses investigations afin de déterminer précisément la nature et l'étendue des données exfiltrées, notamment celles qui pourraient concerner des élèves.

Pour les personnels concernés, cette publication fait cependant franchir un seuil supplémentaire : une adresse personnelle, un numéro de téléphone ou un numéro de sécurité sociale divulgués ne peuvent être modifiés aussi simplement qu'un mot de

Action&Démocratie / CFE-CGC
Secrétariat national (pour toute correspondance) : 9 rue de la Charente - 68270 WITTENHEIM • **Siège social :** 142 rue de Rivoli - 75001 PARIS
Tél. 09 50 88 61 54 ou 07 71 78 84 52 • contact@actionetdemocratie.com • https://actionetdemocratie.com

passe. Leur diffusion peut exposer durablement les victimes à des tentatives d'hameçonnage ciblé, de fraude ou d'usurpation d'identité.

Nous savons qu'aucun système informatique n'est invulnérable et qu'une cyberattaque ne suffit pas, à elle seule, à démontrer une défaillance de ceux qui en sont victimes. Mais lorsque plusieurs incidents importants surviennent en quelques mois, il devient légitime de s'interroger sur leur répétition et sur les mesures prises pour prévenir les suivants.

Cette question se pose avec d'autant plus d'acuité que les mesures de sécurisation décidées à la suite de l'attaque de juillet ont conduit, dans plusieurs académies, à suspendre ou à perturber l'accès à des messageries et applications professionnelles. À quelques jours de la rentrée, les conséquences ne sont donc plus seulement celles d'une fuite de données : elles affectent directement le fonctionnement des services.

Action & Démocratie/CFE-CGC souhaite dès lors connaître précisément les enseignements tirés des incidents intervenus depuis le début de l'année 2026, les mesures prises après chacun d'entre eux, ainsi que les moyens humains et budgétaires consacrés à la sécurisation des systèmes d'information du ministère et des académies.

Nous souhaitons surtout attirer votre attention sur un aspect moins visible de cette crise, mais qui nous paraît essentiel : la place accordée aux personnels dont la sécurité des systèmes d'information constitue précisément le métier.

Des personnels ITRF chargés de l'administration et de la sécurité de ces systèmes nous font état des difficultés qu'ils peuvent rencontrer lorsqu'ils signalent des vulnérabilités, demandent l'application des prescriptions de sécurité de l'État ou sollicitent des audits. Nous disposons notamment de témoignages faisant état d'alertes dont la prise en compte s'est heurtée, localement, à des résistances hiérarchiques.

Nous ne prétendons évidemment pas établir, à partir de ces témoignages, un lien de causalité avec les attaques intervenues cette année. Mais ils justifient une question qui ne peut être éludée : l'organisation actuelle du ministère garantit-elle que les alertes émises par ses propres spécialistes de la sécurité informatique soient effectivement entendues, transmises au niveau approprié et suivies d'effet ?

La cybersécurité ne saurait en effet reposer principalement sur la vigilance individuelle des agents auxquels il est demandé, après chaque incident, de changer leurs mots de passe ou de se méfier des tentatives d'hameçonnage. Elle suppose en amont une véritable culture de la sécurité, des moyens adaptés, des responsabilités clairement établies et la capacité, à tous les niveaux de l'institution, d'entendre ceux dont c'est la compétence.

Les personnels susceptibles d'être concernés par l'attaque de juillet ont été informés individuellement. Cette information était évidemment indispensable. Elle ne peut

cependant constituer le terme de la réponse qui leur est due, particulièrement depuis que certaines des données dérobées ont été rendues publiques.

Nous vous demandons donc de préciser les mesures que le ministère entend prendre pour accompagner durablement les agents dont les données ont été compromises et les protéger contre les conséquences qui pourraient apparaître dans les mois ou les années à venir. Nous souhaitons également savoir quelles garanties seront apportées aux personnels quant à la sécurisation des systèmes auxquels ils doivent nécessairement confier leurs données personnelles et professionnelles.

Il ne s'agit pas pour nous de rechercher précipitamment des responsabilités avant que les faits soient établis. Il s'agit de tirer toutes les conséquences d'une succession d'incidents dont la gravité impose désormais des réponses précises.

Car au-delà de la sécurité des systèmes d'information, c'est aussi la confiance des personnels dans la capacité de leur employeur à protéger les données qu'il leur impose de lui confier qui est en jeu.

Nous vous prions de croire, Monsieur le Ministre, en l'assurance de notre considération distinguée.