Mardi 19 mai 2026

CONCERNE : NOTIFICATION INCIDENT RGPD

Chers administrateurs,
Chers membres,
Chers partenaires,
Chers bénéficiaires,

Nous vous informons que le 06/05/2026, les systèmes informatiques du Centre de Revalidation Fonctionnelle IMPULSO ont subi une cyberattaque par « ransomware ». Ces systèmes informatiques sont partagés avec la Plateforme picarde de Concertation en santé mentale.

Par la présente notification, nous vous fournissons les informations requises en vertu de l'article 34 du règlement (UE 2016/679), plus communément appelé le RGPD (Règlement Général sur la Protection des Données) concernant cet incident.

Que s'est-il passé ?

Des individus non autorisés ont compromis le serveur de notre structure, chiffrant l'ensemble des fichiers qui y étaient stockés, rendant leur exploitation impossible. L'incident a été immédiatement pris en charge par notre service informatique avec le soutien de spécialistes en cybersécurité. Les systèmes concernés ont été isolés et soumis à une enquête technique approfondie. A ce jour, compte tenu des mesures de sécurité supplémentaires activées et des procédures de remédiation mises en œuvre, aucune situation critique supplémentaire liée à l'incident n'a été constatée.

Mesures prises pour atténuer les risques

Nous avons immédiatement pris les mesures suivantes afin de limiter l'impact de l'incident et éviter que la situation ne se reproduise, notamment :

1. Nous avons immédiatement fait appel à une société spécialisée dans la cybersécurité ;
2. Notre gestionnaire informatique a sécurisé les systèmes affectés, en identifiant les menaces latentes présentes sur le réseau et en supprimant les composants résiduels potentiels résultant de la compromission ;
3. Les systèmes compromis ont été isolés ;
4. Notre gestionnaire informatique restaure actuellement l'infrastructure affectée ;
5. La société spécialisée dans la cybersécurité mène une analyse forensique (méthode visant à collecter, analyser et préserver des preuves électroniques suite à une cyberattaque), afin de déterminer avec précision l'étendue et la dynamique de l'incident ;
6. Les différentes autorités compétentes ont été informées.

D'autres interventions techniques sont en cours afin de renforcer les niveaux de protection de l'infrastructure. L'adoption et la mise en œuvre de mesures techniques et organisationnelles supplémentaires visant à prévenir de futures violations ont été instaurées.

Ce que vous pouvez faire ?

Pour votre protection, nous vous recommandons de prendre certaines précautions numériques au cours des prochains mois :

- Soyez particulièrement vigilant face aux e-mails, SMS ou appels téléphoniques inattendus sollicitant des informations personnelles ou des actions urgentes ;
- Vérifiez toujours l'identité de l'expéditeur et évitez d'ouvrir des liens ou des pièces jointes suspects ;
- Ne communiquez jamais vos mots de passe ou données confidentielles.

Si vous souhaitez signaler toute activité suspecte, nous vous remercions de le faire en utilisant les coordonnées fournies dans la section « Contact » de cette communication.

Contact

Nous restons à votre disposition pour toute question ou information complémentaire concernant cet incident.

Vous pouvez nous contacter à l'adresse mail suivante : **j.desprets@crf-impulso.be**

Nous vous prions de nous excuser pour cet incident et nous renouvelons notre engagement à assurer le plus haut niveau de protection de vos données personnelles. Nous vous tiendrons informé(e)s de toute information complémentaire le cas échéant.

Nous vous prions d'agréer, Madame, Monsieur, l'expression de nos salutations distinguées.

Johan DESPRETS

Pour le **CRF IMPULSO**
Av. de la Joyeuse Entrée,84
7000 Mons