

RGPD

TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL AU SEIN DU CCGPE-DGEO

LES TRAITEMENTS OPÉRÉS PAR LE CCGPE-DGEO DANS LE CADRE DE SES MISSIONS DÉCRÉTALES

Phase	Etape	Action	Acteurs
1. Collecte d'informations	Récolte de fichiers Excel (FP) reprenant les participants à des actions de formation ou d'accompagnement via boîte mail sécurisée.	Enregistrement des fichiers Excel	Gestionnaires administratifs et financiers du CCGPE-DGEO
	Si nécessaire et à la demande du bénéficiaire : support pour le transfert de données de ou vers un outil Access		Responsable SMART FSE
2. Correction	Récolte de données concernant les travailleurs actifs dans le projet FSE (liste + contrats de travail ou assimilé et données salariales) (TCE/PERS)	Enregistrement des noms, n° de matricule et temps consacré au projet dans des tableaux Excel Enregistrement des contrats de travail et des Doc12 (enseignement)	Gestionnaires administratifs et financiers du CCGPE-DGEO
	Correction des fichiers via échanges avec les opérateurs de formation (écoles, CTA, CEFA, ASBL...)	Echanges avec le bénéficiaire en vue de corriger ou de compléter les informations reçues	Gestionnaires administratifs et financiers du CCGPE-DGEO
	3. Consolidation	Consolidation des différents fichiers reçus par projet co-financé par le FSE+ ou l'AMIF	Opérations de consolidation et de suppression des doublons
4. Contrôle de premier niveau	Vérification des informations	Extraction d'un échantillon de Participants en vue d'effectuer un contrôle in situ de la véracité des informations fournies	Gestionnaires administratifs et financiers du CCGPE-DGEO
		Vérification des tableaux de calcul du coût salarial pour les personnes sous statut d'employé.	
5. Calculs du coût salarial	Etablissement des dépenses de la FWB à destination du FSE	Extraction des données salariales de la datawarehouse pour le personnel enseignant sur base du n° de matricule et	Gestionnaires administratifs et financiers du CCGPE-DGEO

		calculs de détermination du coût	
6. Transmission	Transmission des informations à l'Agence du Fonds Social Européen (AFSE) ¹	Téléchargement des fichiers consolidés sur la plate-forme de l'Agence Fonds Social Européen	Chefs de projets du CCGPE-DGEO

TRAITEMENTS ULTÉRIEURS

Ces données peuvent alors être utilisées à des fins de statistiques, d'archivage ou de recherche et à des fins d'audit externe.

Les organismes suivants peuvent exiger la transmission des données ci-dessus :

- Agence FSE
- Direction de l'Audit des projets européens (DAPE)
- Cellule d'Audit de l'Inspection des Finances (CAIF)
- Commission (DG Regio, DG Emploi)
- Cour des Comptes européennes
- Inspection des finances
- Cour des Comptes belge

CADRE LÉGAL

Convention relative à la désignation du Centre de Coordination et de Gestion – Enseignement obligatoire de la Communauté Française comme organisme intermédiaire établie entre le CCGPE-DGEO et l'Agence FSE

Décret CCGPE-DGEO	https://www.gallilex.cfwb.be/document/pdf/32886_007.pdf
-------------------	---

Règlement (UE) n° 2021/1060 : articles 42, 69	https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32021R1060
---	---

Règlement (UE) 2021/1057 : articles 17, 34, annexes I et II	https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021R1057&from=EN
---	---

Règlement (UE) 2021/1147 : article 33, 34, annexe V	https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021R1147&from=EN
---	---

OBJECTIFS DE CETTE COLLECTE

Le CCGPE-DGEO collecte les DACP dans un but de transmission aux administrations en charge de la gestion des fonds européens.

CONSERVATION DES DONNÉES AU SEIN DU CCGPE-DGEO

Les fichiers sont enregistrés sur un serveur de fichiers ETNIC via une plateforme partagée accessible uniquement au personnel du CCGPE-DGEO sur base d'accès délivrés par ETNIC

Les règles européennes portent l'obligation de conservation des données à 8 ans après la fin de la programmation pour laquelle elles ont été récoltées. Exemple : programmation 2021-2027, conservation jusqu'en 2035.

GESTION DES INCIDENTS

¹ L'Agence FSE a publié une note RGPD à l'intention des opérateurs consultable en suivant ce lien : https://fse.be/fileadmin/sites/fse/uploads/documents/Programmation_FSE_2021-2027/Guides_PDF_accessible/note_RGPD_operateur_022022.pdf

Des mesures de sécurité adéquates sont mises en place afin de prévenir les accès physiques inutiles ou non autorisés aux supports contenant les données à caractère personnel.

Un incident de sécurité peut correspondre à une action malveillante délibérée, au non-respect de la politique de sécurité ou d'une manière générale à toute atteinte aux informations, à toute augmentation des menaces sur la sécurité de l'information ou à toute augmentation de la probabilité de compromission des opérations liées à l'activité de traitement des informations.

Mesures(s) organisationnelle(s)

- Tout incident lié à la protection et à la sécurisation des données à caractère personnel est notifié dans les meilleurs délais au Délégué à la protection des données (DPD) et au Conseiller en sécurité (CSI) du MFW-B. Une équipe de gestion de l'incident est mise en place afin de prendre les mesures nécessaires adaptées à l'incident rencontré sur le plan juridique, technique et organisationnel.
- Dans le cas d'un incident de type informatique, c'est l'ETNIC (en tant que sous-traitant) qui prend les mesures relatives à la sécurité physique et logistique des ressources sous sa responsabilité, hébergées dans ses data centers. Le DPD et le CSI de l'ETNIC sont intégrés dans l'équipe de gestion de l'incident.
- Les accès aux systèmes et aux données sous la responsabilité du MFW-B et de l'ETNIC font l'objet de traces et de logs pour la gestion et la surveillance des systèmes. Ces traces et logs peuvent contenir des DACP concernant les personnes sous la responsabilité du demandeur. En effet, l'ETNIC peut prendre les mesures nécessaires pour qu'il soit possible, par la combinaison des informations tenues à jour par les différents composants de l'application métier, de parvenir à une reconstruction complète de l'ensemble du flux de données d'une transaction spécifique.
- L'accès aux traces et aux logs respecte les prescrits de la politique de sécurité du MFW-B et de l'ETNIC en la matière, qui garantit la confidentialité des données informatiques contenant des DACP.
- En cas d'incident physique, la procédure de gestion des incidents de sécurité du MFW-B doit assurer l'analyse, l'évaluation et le traitement des incidents afin d'en limiter l'impact et d'empêcher que des incidents similaires ne se produisent de nouveau.

ENGAGEMENT

Les agents en charge du traitement s'engagent à :

- Ne pas transférer et/ou communiquer les DACP à d'autres destinataires que ceux mentionnés ci-dessus;
- Ne pas utiliser les DACP collectées pour d'autres finalités que celles mentionnées ci-dessus ;
- A ne pas conserver les DACP fournies au-delà du délai de conservation mentionné ci-dessus ;
- A détruire les DACP dès la fin de leur exploitation ;
- Conserver toutes les traces et documents relatifs à ce traitement dans un espace de stockage et de partage de documents sécurisé tel que décrit ci-dessus.