



Responsabilité en matière de RGPD (protection de données)

Consignes

Le **Règlement Général sur la Protection des Données (RGPD** ou encore **GDPR**, *General Data Protection Regulation*), est un règlement européen qui constitue le texte de référence en matière de protection des données à caractère personnel. Ce règlement est transposé dans la législation nationale et nous oblige à respecter des procédures précises afin de respecter les données personnelles des travailleurs et de nos affilié.e.s.

Cette fiche information à destination des délégué.e.s et militant.e.s de notre secteur sert comme information générale en attente d'un règlement de la CGSP Fédérale.

- Tout.e délégué.e doit veiller à remettre à tout candidat affilié, le **bulletin d'affiliation le plus récent** (auquel il faut joindre le formulaire de domiciliation européenne SEPA) sur lequel est reprise la mention suivante : « *Je confirme avoir pris connaissance de la politique de confidentialité de la CGSP (consultable via <https://cgspalbru.be/affiliation/>) et être en accord avec celle -ci.* »

A défaut de cette mention, la déclaration de confidentialité CGSP (accessible sur notre site web) doit être remise au travailleur dans son rôle linguistique.

- L'unique base de données correcte reprenant les coordonnées des affilié.e.s est celle tenue à jour par la centrale (sur base des informations ou mises-à-jour communiquées par les affilié.e.s). Le.La responsable d'une section peut demander au secrétariat un exemplaire de la liste reprenant les affilié.e.s de sa section. Toutefois, il.elle doit s'engager à **ne pas la reproduire ni à la distribuer** et à la **détruire** dès que la vérification sera effectuée et ceci **au plus tard 30 jours après réception**.
- Certaines sections tiennent des **listes internes**. Attention à leur mise à jour et à la confidentialité de ces listes (désignation d'un.e ou deux camarades responsables [Président.e ou permanent.e.s p.ex.], en prévoir un accès limité (mot de passe sur le fichier), etc.
- Nous ne pouvons plus utiliser les données, numéros de téléphone ou photos des affilié.es ou de tout.e travailleur.se non-affilié.e sans leur **autorisation explicite écrite** (attention sur les réseaux sociaux p.ex.).

Cette mesure est valable également dans le cadre de la constitution d'un dossier de défense, d'une enquête dans un service spécifique (ex. : prise de contact avec des travailleur.se.s de ce service via leur numéro personnel (obtenu informellement d'une tierce personne)). L'utilisation des numéros de téléphone privé obtenus sans l'accord des intéressé.e.s est considérée comme une infraction pénale si dépôt de plainte.

- Whatsapp/Messenger/Réseaux sociaux : un numéro de téléphone, une adresse mail personnelle, etc. ne peut être utilisé sans **autorisation écrite de l'intéressé.e**, sous peine d'être condamné.e à de lourdes amendes. Faites attention en utilisant des groupes de discussion (Whatsapp, etc.) avec des affilié.e.s (ne jamais les ajouter sans leur accord), et si vous le faites exceptionnellement, **verrouillez la discussion** afin que des messages ne peuvent y être ajoutés sans l'accord du responsable de groupe.

Les **logos** officiels ou **dénominations CGSP-FGTB**, ne peuvent être utilisés sans autorisation de la centrale.

- Le secteur demande de désigner un.e **responsable GDPR** au sein de chaque section, qui servira de point de contact pour les questions relatives à la protection des données.
- Tout.e affilié.e a le droit d'envoyer un courrier/e-mail demandant de **supprimer toutes ses coordonnées** de nos bases de données. Tant au niveau de la centrale qu'au niveau de la section, de toute liste parallèle, archive, etc. Ceci peut notamment impacter le (non-)paiement de la prime syndicale p.ex. si les données du travailleur sont effacées. Si une telle demande devait vous parvenir, transférez-là, par mail, au **DPO de la CGSP** (dpo@cgsp.be) avec le secrétariat en copie (alr.bruxelles@cgspacod.be). Le DPO se chargera de la **procédure particulière**.
- En cas de **perte de gsm/pc/tablette/liste papier** contenant des données personnelles d'affilié.e.s ou de délégué.e.s : prévenir immédiatement les responsables du secteur, qui en informeront à leur tour le DPO de la CGSP.
- En cas d'**envoi de mails à des groupes** de destinataires (en particulier en dehors des gens de la section ou de la centrale): **toujours mettre les destinataires en cci**.
- A la demande d'affilié.e.s, la centrale peut communiquer les **coordonnées** (numéro de téléphone connu, adresse mail) **de délégué.e.s** qui sont renseigné.e.s à la centrale.
- Ne laissez pas traîner de listes, de dossiers personnels ou des mails d'affilié.e.s, etc. sur **votre bureau**.

(Information: cette liste n'a pas la prétention d'être une liste exhaustive et détaillée qui reprend toutes les possibilités légales. La législation étant très spécifique, contraignante et complexe, elle peut servir comme ligne conductrice aux sections et au secteur pour appliquer au mieux la législation en vigueur. La fiche sera par conséquent adaptée régulièrement en fonction.)



Verantwoordelijkheden inzake de **AVG** (gegevensbescherming)

Richtlijnen

De **Algemene Verordening Gegevensbescherming (AVG of GDPR, General Data Protection Regulation)**, is een Europese verordening die de referentietekst omvat wat betreft de bescherming van gegevens van persoonlijke aard. Deze verordening is in een nationale wettekst gegoten en verplicht ons ertoe precieze procedures te volgen om de persoonlijke gegevens van de werknemers en leden te respecteren.

Deze informatiefiche voor de afgevaardigden en militanten van onze sector dient als algemene informatiebron in afwachting van een reglement van de Federale ACOD.

- Afgevaardigden moeten ervoor zorgen dat alle kandidaat leden het **meest recent aansluitingsbulletin** krijgen (waaraan een SEPA-domiciliëringsmandaat wordt gevoegd) waarop volgende zin vermeld staat: *“Ik bevestig kennis genomen te hebben van het vertrouwelijkheidsbeleid van de ACOD (te raadplegen op <https://acodlrbbbru.be/lidworden/>) en ermee in te stemmen”*.

Indien deze vermelding ontbreekt, dient het vertrouwelijkheidsbeleid van de ACOD (dat terug te vinden is op onze website) aan de werker overhandigd te worden in zijn/haar taalrol.

- De enige correcte gegevensbank die alle gegevens van de leden omvat, is die dat door de centrale bijgewerkt wordt (op basis van de informatie die door de leden wordt gecommuniceerd). De afdelingsverantwoordelijke mag het secretariaat om een ledenlijst van zijn/haar afdeling vragen. Hij/Zij verbindt zich ertoe deze lijst **niet te kopiëren of uit te delen** en deze te **vernietigen** nadat de lijst nagekeken is en dit **binnen de 30 dagen na ontvangst**.
- Bepaalde afdelingen houden **intern lijsten** bij. Zorg ervoor dat deze bijgewerkt worden, let op de vertrouwelijke aard van deze lijsten (één of twee kameraden als verantwoordelijke aanduiden [Voorzitter/-ster of vrijgestelde bv.]) en voorzie een beperkte toegang (wachtwoord om document te openen), enz.
- We mogen de gegevens, het telefoonnummer of de foto's van de leden of niet-aangesloten werkers niet meer gebruiken zonder hun **expliciete schriftelijke goedkeuring** (opgelet voor sociale media bv.).

Deze maatregel is ook van toepassing in het kader van de opstelling van een verdedigingsdossier of een onderzoek binnen een specifieke dienst (bv. telefonisch contacteren van een werker/-ster van deze dienst op hun privénummer (informeel verkregen via een derde persoon)). Het gebruik van een privételefoonnummer dat zonder goedkeuring van de betrokken persoon werd verkregen, wordt beschouwd als een inbreuk mocht er een klacht worden ingediend.

- WhatsApp/Messenger/Sociale netwerken: het telefoonnummer, een persoonlijk e-mailadres, enz. mag niet worden gebruikt zonder **schriftelijke goedkeuring van de betrokken persoon**, waarvoor zware boetes worden opgelegd. Let goed op met het gebruik van discussiegroepen (Whatsapp, enz.) met leden (nooit toevoegen zonder hun akkoord), en in geval van een uitzonderlijk gebruik, **versleutel steeds het gesprek** zodat er geen berichten gepost kunnen worden zonder de goedkeuring van de groepsverantwoordelijke.

Er mag **geen gebruik** worden gemaakt van de officiële **logo's of benaming ACOD-ABVV** zonder **goedkeuring van de centrale**.

- 0 De sector vraagt een **AVG-verantwoordelijke** aan te duiden binnen elke afdeling, die de contactpersoon zal zijn voor vragen inzake de gegevensbescherming.
- 0 Alle leden hebben het recht een brief/e-mail te sturen met de vraag **alle gegevens uit onze gegevensbanken te verwijderen**. Zowel op het niveau van de centrale als op niveau van de afdeling en alle lijsten, archieven, enz. Dit kan er bv. toe leiden dat de vakbondspremie niet kan worden uitbetaald als de gegevens van de werker werden verwijderd. Indien u dergelijk verzoek zou krijgen, stuur deze door via e-mail naar de DPO van de ACOD (dpo@cgsp.be) met het secretariaat in kopie (lrb.brussel@cgspacod.be). **De DPO zal zich over de specifieke procedure ontfemen.**
- 0 In geval van verlies van **een GSM/PC/tablet/papieren lijst** die de persoonlijke gegevens van de leden of afgevaardigden bevat: onmiddellijk de sectorverantwoordelijken verwittigen, die op hun beurt de DPO van de ACOD zullen inlichten.
- 0 Indien er **e-mails naar een groep geadresseerden worden verstuurd** (meer bepaald naar mensen die geen deel uitmaken van de afdeling of de centrale): **alle geadresseerden in cci zetten**.
- 0 Op vraag van de leden mag de centrale de **gegevens** (gekend telefoonnummer, e-mailadres) van de **afgevaardigde**, die gekend zijn bij de centrale, doorgeven.
- 0 Laat geen lijsten, persoonlijke dossiers of e-mails van leden, enz. slingeren op **je bureau**.

(Informatie: deze lijst is niet uitputtend, noch gedetailleerd en omvat niet alle wettelijke bepalingen. Aangezien de wetgeving zeer specifiek, bindend en complex is, kan deze een leidraad vormen voor de afdelingen en de sector om de geldende wetgeving zo goed mogelijk toe te passen. De fiche zal bijgevolg regelmatig worden bijgewerkt.)