

	POLITIQUE DE CONFORMITE AU RGPD	Type	Procédure Qualité
		Identification	QUA 1 421 01
	Processus S2 Systèmes d'Information	Version	01
		Date	28/01/2025

POLITIQUE DE CONFORMITE AU RGPD

Document en cours de validité

Date	Version	Motif	Rédacteur	Approbateur
28/01/2025	01	Edition initiale	DPO	Directrice
			Vérificateur	
			Animateur Qualité	

Historique du document

Date	Version	Motif	Rédacteur	Vérificateur	Approbateur

SOMMAIRE

1	Objet	3
2	Réglementation	3
3	Politique de conformité au RGPD	3
3.1	Introduction	3
3.1.1	Données à caractère personnel – Définition	3
3.1.2	Responsable de la collecte et du traitement des données	3
3.2	Les données collectées	4
3.3	Durée de conservation.....	5
3.4	Finalité de la collecte et du traitement des données	5
3.5	Destinataires des données collectées.....	5
3.6	Base juridique de la collecte et du traitement des données	6
3.7	Transfert des données	6
3.8	Droit sur les données personnelles	6
3.8.1	Droit d'accès.....	6
3.8.2	Droit de rectification	6
3.8.3	Droit à l'effacement	6
3.8.4	Droit à la limitation des données.....	7
3.8.5	Droit d'opposition	7
3.8.6	Droit à la portabilité.....	7
3.8.7	Droit de définir des directives relatives au traitement des données personnelles après votre décès.....	7
3.9	Confidentialité de votre identifiant et de votre mot de passe	8
3.10	Mesures de sécurité	8
3.11	Cookies.....	8
3.12	Modification de la Politique de conformité au RGPD	8
3.13	Contact.....	8

1 Objet

Ce document vise à informer les adhérents et les salariés des adhérents suivis par le PRISSM des conditions dans lesquelles les données à caractère personnel sont traitées par le PRISSM.

Cette politique de conformité au RGPD est susceptible de faire l'objet de modifications régulières afin de tenir compte des activités et de la législation applicables au PRISSM.

Après un état des lieux des données collectées et traitées par nos services (notamment celles relatives aux salariés, aux entreprises adhérentes, aux sous- traitants), le PRISSM a mis en place des mesures de protection supplémentaires et adapté ses configurations (process, matériel, logiciels, réseau, archivage...) afin de répondre aux exigences du RGPD.

2 Réglementation

Articles 1 et 14 du règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dit « RGPD ») ainsi que par la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiés en juin 2019.

Remplaçant la Loi Informatique et Libertés, ce texte vise au renforcement du cadre de protection des données personnelles.

Cette réglementation s'applique à toutes les entreprises, associations, collectivités de l'Union Européenne.

3 Politique de conformité au RGPD

3.1 Introduction

3.1.1 Données à caractère personnel – Définition

Le terme « données à caractère personnel » désigne toutes les données qui permettent d'identifier un individu directement ou indirectement, par agrégation de plusieurs données, ce qui correspond notamment à vos nom, prénom(s), pseudonyme, photographie, adresse de courrier électronique, numéro(s) de téléphone, date de naissance, ainsi qu'à tout autre renseignement que nous pourrions vous demander et que vous choisirez de nous communiquer à votre sujet.

3.1.2 Responsable de la collecte et du traitement des données

La réglementation relative à la protection des données personnelles (règlement général sur la protection des données (RGPD) et loi Informatique et Libertés) a vocation à protéger les informations relatives à la vie privée des citoyens, qu'elles soient d'ordre professionnel ou personnel. Ainsi, même les informations collectées dans un contexte professionnel sont protégées par la réglementation.

Le respect de la réglementation en matière de protection des données n'exonère pas le PRISSM du respect des autres obligations auxquelles il est par ailleurs soumis. Les principes du RGPD et de la loi Informatique et Libertés ne doivent en effet pas permettre de déroger à d'autres règles, issues par exemple du code du travail ou du code de la santé publique.

Afin de répondre à cette réglementation, l'association PRISSM a désigné un Délégué à la Protection des Données/Data Protection Officer (DPD/DPO).

Le DPO est un gage de confiance, spécialisé dans la protection des données personnelles. Il est chargé de veiller à la préservation de la vie privée et à la bonne application des règles de protection des données personnelles. Il est l'interlocuteur privilégié de la Commission Nationale de l'Informatique et des Libertés (CNIL), et de toutes personnes concernées par une collecte ou un traitement de données à caractère personnel.

Pour contacter le DPO : écrire à « PRISSM – A l'attention du DPO – 2 Rue Marie Gaëtana Agnesi Zone Europa 64000 Pau » ou par mail à dpo@prissm.fr.

Le DPO tient le registre des activités de traitements de l'association PRISSM qu'il met, le cas échéant, à la disposition de la CNIL.

Le PRISSM est votre principal interlocuteur pour traiter toute demande relative à vos données à caractère personnel.

3.2 Les données collectées

Les professionnels du PRISSM doivent veiller à ne traiter que les informations adéquates, pertinentes et limitées à ce qui est nécessaire au regard de l'objectif poursuivi (principe de minimisation).

Les données que nous traitons sont en principe recueillies directement auprès des personnes concernées. Cela signifie que le professionnel doit si besoin faire un tri dans les informations fournies par la personne concernée (travailleur, adhérent du PRISSM, salarié) afin de ne garder que celles qui lui permettent de remplir ses missions. Toutefois, certaines données des salariés dont le PRISSM doit assurer la prise en charge peuvent être recueillies de manière indirecte auprès de leurs employeurs, adhérents du PRISSM : données administratives et/ou données relatives à leur situation professionnelle.

Les différentes catégories de données que nous sommes amenés à traiter sont :

- Les informations administratives et de contact (nom, nom de naissance, prénom, sexe, date de naissance, lieu de naissance, adresse postale, numéro de téléphone, email professionnel et/ou personnel, numéro de sécurité sociale)
- Les informations relatives à la situation personnelle et familiale (situation de famille, nombre d'enfants, situation maritale)
- Les informations relatives à la formation, à l'emploi et au poste de travail (diplômes, niveau d'étude, emploi, nom de l'employeur, type de contrat de travail, date d'entrée dans l'entreprise adhérente, code Profession et Catégorie Socioprofessionnelle, conditions de travail, risques professionnels)
- Les données d'identification et d'authentification lors de l'utilisation des services en ligne proposés par le PRISSM
- Les données nécessaires à vos demandes de contact (formulaire de contact).

Dans le cadre de la tenue du Dossier Médical de Santé au Travail (DMST), le PRISSM est amené à collecter des données sensibles :

- Informations médicales en application de la législation en vigueur
- Informations sociales qui permettent une prise en charge globale du travailleur.

Les professionnels du PRISSM traitent également des informations portant sur d'autres personnes que les travailleurs dont ils assurent le suivi. Il peut s'agir de :

- Leurs propres personnels au titre de la gestion des ressources humaines, du recrutement
- Leurs fournisseurs
- Des sous-traitants
- Des représentants de ses adhérents
- Des membres bénévoles du PRISSM siégeant au conseil d'administration et à la commission de contrôle.

Le PRISSM ne collecte pas de données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale d'une personne.

3.3 Durée de conservation

Les données à caractère personnel sont conservées pendant une durée limitée qui n'excède pas la durée nécessaire aux finalités de collecte. Les délais de conservation des données sont portés à la connaissance des personnes, et varient selon la nature des données, la finalité des traitements, ou les exigences légales ou réglementaires.

Les données médicales sont conservées conformément aux durées légales de conservation (cf. durée de conservation CNIL).

Les données comptables sont conservées 10 ans ou détruites en cas d'évènement particulier (exclusion pour défaut de paiement des cotisations, radiation).

3.4 Finalité de la collecte et du traitement des données

Nous mettons en œuvre des traitements de données à caractère personnel afin de vous apporter le service de santé au travail le plus adapté à vos besoins.

Une multitude de données personnelles peut être traitée dans un SPST, sous réserve que ces dernières soient toujours adéquates, pertinentes et limitées à ce qui est nécessaire au regard de l'objectif poursuivi par le fichier ou la base de données déployée.

Les catégories de données susceptibles d'être collectées et utilisées seront différentes, selon que le traitement est constitué pour :

- Gérer le dossier médical en santé au travail (DMST)
- Réaliser des recherches, études et enquêtes
- Renseigner le dossier consacré à l'entreprise constitué notamment pour rédiger la fiche d'entreprise et mener toutes les actions en lien avec les missions imparties au PRISSM (conduite des actions en santé au travail, actions menées pour diminuer les risques professionnels)
- Gérer, au plan des ressources humaines, les salariés du PRISSM
- Recruter les salariés du PRISSM
- Assurer l'administration du PRISSM telle que la gestion de la base de données des adhérents, l'organisation des instances, la gestion des relations avec le comité social et économique.

3.5 Destinataires des données collectées

Afin d'accomplir les finalités précitées, les données personnelles sont accessibles uniquement :

- Au sein du PRISSM, au personnel dûment habilité selon la finalité du traitement poursuivi
- Aux professionnels de santé du PRISSM en charge du dossier médical en santé au travail (DMST)
- A nos prestataires de services et sous-traitants réalisant des prestations pour notre compte
- A nos partenaires dans le cadre d'enquêtes et d'études réalisées par le PRISSM. Les données traitées sont alors agrégées en statistiques anonymisées
- Aux administrations, organismes publics, autorités judiciaires sur demande et dans la limite de ce qui est permis par la réglementation

- Le PRISSM n'effectue aucune transmission des données sensibles recueillies dans l'exercice de ses missions, sauf exception légale ou réglementaire.

Les données personnelles qui figurent dans les dossiers entreprises sont utilisées exclusivement par les collaborateurs dont la fonction le nécessite.

3.6 Base juridique de la collecte et du traitement des données

- D'une manière générale, dès lors que le consentement des personnes est requis pour traiter leurs données, le PRISSM se charge d'informer les personnes et de recueillir leur consentement.
- Il peut être tenu de traiter les données en raison d'une obligation légale (gestion du dossier médical en santé au travail, élaboration de la fiche d'entreprise). Le recours à la base légale de la mission d'intérêt public peut également fonder les traitements mis en œuvre par les autorités publiques aux fins d'exécuter leurs missions.
- Il peut être tenu de traiter les données en raison d'un intérêt légitime (réalisation d'études et enquêtes, gestion des salariés du PRISSM, administration du PRISSM).

3.7 Transfert des données

Le PRISSM ne transfère pas de données personnelles en dehors de l'Union européenne.

3.8 Droit sur les données personnelles

3.8.1 Droit d'accès

Une personne concernée peut demander aux professionnels du PRISSM la confirmation que ce dernier détient des informations sur elle et la communication de ces dernières pour en vérifier le contenu.

Dans le cadre d'une telle demande, les personnes compétentes au sein du PRISSM peuvent être amenées à rappeler les caractéristiques de l'utilisation des informations (par exemple : objectifs, catégories d'informations traitées, destinataires, durée de conservation).

3.8.2 Droit de rectification

Une personne concernée peut demander que ses informations soient rectifiées si elles sont inexactes ou incomplètes. Ce droit permet d'éviter que le PRISSM utilise ou diffuse des informations erronées.

3.8.3 Droit à l'effacement

Une personne concernée est notamment en droit d'exiger l'effacement de ses données personnelles si :

- Les informations ne sont plus nécessaires au PRISSM au regard de l'objectif poursuivi par la collecte et l'utilisation des données.
- Les informations ont fait l'objet d'un traitement illicite.
- Les informations doivent être effacées pour respecter une obligation légale.

Le droit à l'effacement peut être écarté lorsque le traitement est nécessaire « pour des motifs d'intérêt public dans le domaine de la santé publique » et pour les traitements constitués pour « respecter une obligation légale » (cas du DMST). Par conséquent, le SPST peut ne pas répondre favorablement à la demande d'un travailleur d'effacer des données de son DMST.

3.8.4 Droit à la limitation des données

Une personne concernée peut demander à « geler » l'utilisation de ses données personnelles dans deux situations :

- Si elle conteste l'exactitude des données, le temps que les professionnels du PRISSM effectuent une vérification.
- Si l'organisme souhaite supprimer les données mais que la personne concernée souhaite quant à elle les conserver, notamment pour exercer un autre droit, en cas de contentieux par exemple.

Parallèlement à ce socle de droits, les personnes concernées peuvent disposer de droits complémentaires conditionnés au fondement légal du fichier, c'est-à-dire à la justification permettant de le mettre en œuvre.

3.8.5 Droit d'opposition

Si le fichier n'est pas fondé sur une obligation légale mais sur l'intérêt légitime du PRISSM (cas des fichiers utilisés pour la gestion des salariés, des adhérents), la personne concernée a le droit de s'opposer à l'utilisation de ses informations. Le responsable de traitement doit alors cesser d'utiliser ces informations sauf s'il est en mesure de justifier de l'existence de motifs légitimes et impérieux prévalant sur les intérêts et les droits et libertés de la personne concernée.

3.8.6 Droit à la portabilité

Les données à caractère personnel fournies peuvent être récupérées dans un format ouvert et lisible par machine afin de les stocker pour un usage personnel ou de les communiquer à un tiers désigné par la personne concernée.

3.8.7 Droit de définir des directives relatives au traitement des données personnelles après votre décès

La personne concernée dispose du droit de définir des directives relatives à la conservation, à l'effacement et à la communication des données à caractère personnel après son décès. Ces directives peuvent être générales, c'est-à-dire qu'elles portent alors sur l'ensemble des données à caractère personnel qui la concernent. Elles doivent dans ce cas être enregistrées auprès d'un tiers de confiance numérique certifié par la CNIL.

En transmettant de telles directives, la personne concernée donne expressément son consentement pour que ces directives soient conservées, transmises et exécutées selon les modalités prévues.

Les directives peuvent aussi être spécifiques aux données traitées par le PRISSM. Il convient alors de les transmettre aux coordonnées suivantes :

- Adresse mail : dpo@prissm.fr
- Adresse postale : DPO du PRISSM - 2 Rue Marie Gaëtana Agnesi Zone Europa 64000 PAU.

Avant de répondre à la demande, le PRISSM est susceptible de vérifier l'identité de la personne concernée et lui demander de nous fournir davantage d'informations.

Le PRISSM s'efforcera de donner suite à la demande dans un délai raisonnable et, en tout état de cause, dans les délais fixés par la loi.

En cas de réponse jugée insatisfaisante, la personne concernée peut introduire une réclamation auprès de la CNIL (<https://www.cnil.fr/fr/plaintes>), autorité de contrôle compétente en France, à l'adresse suivante : 3 Place de Fontenoy – TSA 80715 – 75334 PARIS CEDEX 07.

3.9 Confidentialité de votre identifiant et de votre mot de passe

En cas d'accès par identifiant et mot de passe : l'adhérent est responsable de la confidentialité de son identifiant et de son mot de passe pour accéder à l'espace adhérent. Il s'engage à conserver ce mot de passe secret et à ne le communiquer à personne. Il doit immédiatement contacter le PRISSM en cas de vol, de perte, de détournement ou d'utilisation non autorisée de ses identifiants de connexion ou s'il remarque que son compte a été utilisé à son insu.

3.10 Mesures de sécurité

Le PRISSM assure prendre toutes précautions utiles, mesures organisationnelles et techniques appropriées pour préserver la sécurité, l'intégrité et la confidentialité de vos données à caractère personnel et notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Le PRISSM exige également de tout sous-traitant qu'il présente des garanties appropriées pour assurer la sécurité, la protection et la confidentialité des données personnelles. Cette exigence passe par la mise en place de contrats, qui incluent pour le sous-traitant l'obligation de respecter le contenu du Règlement Européen sur la Protection des Données (RGPD). Ces contrats prévoient la réalisation, le cas échéant, de contrôles et d'audits.

3.11 Cookies

Les conditions de fonctionnement et d'utilisation de ces cookies sont décrits au sein de la Politique de Cookies.

3.12 Modification de la Politique de conformité au RGPD

Le PRISSM se réserve le droit de modifier à tout moment la présente Politique de conformité au RGPD en totalité ou en partie. Ces modifications entreront en vigueur à compter de la publication de la nouvelle Politique de conformité au RGPD. En tout état de cause, l'utilisation du site internet du PRISSM suite à l'entrée en vigueur de ces modifications vaudra reconnaissance et acceptation de la nouvelle Politique de conformité au RGPD.

3.13 Contact

Pour toute question relative à la présente Politique de conformité au RGPD ou aux données personnelles, contacter le PRISSM en :

- Adressant un mail au Délégué à la Protection des Données (dpo@prissm.fr)
- Adressant un courrier à (DPO du PRISSM – 2 Rue Marie Gaëtana Agnesi Zone Europa 64000 PAU).