LIVRE BLANC

VOTRE ORGANISME DE FORMATION

FACE AU RGPD

Explications et conseils
pour aborder sereinement le RGPD lorsque l'on est organisme de formation

ARGALIS
www.argalis.fr

Le présent livre blanc est un document informatif qui a pour vocation d'apporter des renseignements au sujet du règlement européen sur la protection des données à caractère personnel. Aucun conseil juridique n'est contenu dans le présent document.

L'équipe Argalis vous propose ce livre blanc dans le but d'offrir une explication claire et constructive de cette mesure qui, dès le mois de mai 2018, entrera en vigueur partout en Europe et touchera aussi bien les entreprises de biens et de services que les organismes de formation.

Pour toute question relative à ce règlement veuillez vous adresser à un cabinet d'avocats spécialisé.

VOTRE ORGANISME DE FORMATION FACE AU RGPD

QU'EST-CE QUE LE RGPD ?

Le RGPD ou Règlement Général sur la Protection des Données entrera en vigueur le 25 mai 2018. Cette nouvelle réglementation européenne est destinée à renforcer la protection des données personnelles en redéfinissant les règles et obligations applicables aux traitements des données des personnes physiques.

Ce règlement s'applique à tous les types de renseignements personnels, que leur traitement soit ou non automatisé, entièrement ou en partie. Toute organisation de l'Union Européenne susceptible de détenir des données à caractère personnel est soumise à ce règlement, quels que soient sa taille, son statut ou son domaine d'activité. Les organisations hors Union Européenne sont également concernées si elles fournissent des biens et des services aux personnes situées dans l'UE.

Les organismes de formation n'échappent donc pas à la règle et devront même adopter une approche bien particulière face au RGPD. Car les organismes de formation ne sont pas des entreprises comme les autres ! La multiplicité des acteurs (clients professionnels ou particuliers, employés, formateurs, organismes financeurs, Dirrecte, sous-traitants…) place les organismes de formation au cœur d'importants flux d'informations qu'il convient de manier avec précaution.

TEXTE OFFICIEL

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Consultez le texte réglementaire officiel sur le site de la CNIL

DÉFINITIONS

DONNÉE PERSONNELLE

Une donnée personnelle est une information sur une personne physique, permettant de l'identifier directement ou indirectement.

Exemple : nom, prénom, adresse, habitudes de consommation, adresse IP, etc...

Certaines données, à priori anonymes, deviennent des données à caractère personnel, dès lors que leur regroupement ou recoupement permet d'identifier une personne physique. On parle alors de donnée indirectement identifiante.

DONNÉE SENSIBLE

Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

TRAITEMENT DE DONNÉES

« Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. » (Art. 4.2 du RGPD)

Exemple : le fait de collecter les noms et prénoms de vos apprenants constitue un traitement de données. Enregistrer l'adresse du domicile de vos formateurs ou l'adresse email d'un client est également du traitement de données.

Est dénommée traitement automatisé d'informations nominatives toute opération aboutissant à la constitution informatique de fichiers ou de bases de données, et ce quel que soit le moyen ou le support informatique, ainsi que toute procédure de consultation, de télétransmission d'informations nominatives, quel que soit le moyen de télécommunication utilisé.

Exemple : les données conservées sous format Excel sur un ordinateur, dans un fichier dont la personne n'a pas connaissance, relèvent d'un traitement de données automatisé.

RESPONSABLE DU TRAITEMENT

« Personne physique ou morale soit une autorité publique, un service ou un organisme, qui seul ou conjointement définit les finalités et les moyens du traitement des données à caractère personnel. C'est lui qui met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire. »

DESTINATAIRE

« Personne physique ou morale, autorité publique, service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers. »

POURQUOI CE RÈGLEMENT ?

À l'heure du Big Data, du foisonnement des outils numériques et de la démocratisation des objets connectés, une mise à jour des textes de loi en matière de protection des données personnelles était nécessaire afin de prendre en compte les avancées technologiques de ces 20 dernières années. Le nouveau règlement permet aussi d'harmoniser la législation au niveau européen pour garantir des droits équivalents aux citoyens de chaque pays membre de l'UE.

Nous sommes régulièrement invités à partager des données personnelles avec un tiers (réseau social, service de messagerie, commerçants, employeur…) pour pouvoir acheter un bien ou utiliser un service, communiquer avec ses amis ou encore collaborer avec ses collègues. Mais une fois nos données confiées, que deviennent-elles ? Qui les protège ? Qui y a accès ?

Face à ses questions, le RGPD redéfinit le cadre du traitement des données personnelles en accordant de nouveaux droits aux citoyens européens pour une meilleure protection de leurs données et une meilleure visibilité sur l'utilisation qui en est faite, tout en responsabilisant davantage les organisations qui collectent et utilisent ces données.

Trois objectifs majeurs se distinguent :

- Renforcer le droit des citoyens
- Renforcer le contrôle et l'application des sanctions sur le territoire européen
- Responsabiliser les acteurs de la donnée

UN PEU D'HISTOIRE

1978

La Loi Informatique et Libertés du 6 janvier 1978 définit pour la première fois un cadre pour la collecte et le traitement des données personnelles.

1995

La directive n°95/46/CE est adoptée en 1995.

2004

La directive européenne n°95/46/CE est transposée en droit français par la loi 2004-801 du 6 août 2004

2012

Initiation du projet de nouveau règlement européen dans un but d'harmonisation des lois européennes en matière de protection des données personnelles.

2016

Le nouveau règlement est adopté le 27 avril 2016.

2018

Le RGPD entre en vigueur le 25 mai 2018.

QUELLES SONT LES EXIGENCES DU RGPD ?

6 PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES

L'article 5 du RGPD définit les principes applicables au traitement des données à caractère personnel.

EXTRAITS

1. LICÉITÉ, LOYAUTÉ, TRANSPARENCE

« Les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. »

PRINCIPE DE LICÉITÉ

Selon l'article 6 du RGPD, un traitement de données à caractère personnel n'est licite que s'il remplit au moins l'une des conditions suivantes :

a. La personne concernée a consenti au traitement
b. Le traitement est nécessaire à l'exécution d'un contrat
c. Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis
d. Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique
e. Le traitement est nécessaire à l'exécution d'une mission d'intérêt public
f. Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers

2. LIMITATION DES FINALITÉS

« Les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales. »

3. MINIMISATION DES DONNÉES

« Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. »

4. EXACTITUDE

« Les données doivent être exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder. »

5. LIMITATION DE LA CONSERVATION

« Les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée. »

6. INTÉGRITÉ ET CONFIDENTIALITÉ

« Les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. »

DES DROITS RENFORCÉS POUR LES PERSONNES CONCERNÉES

Dans son chapitre III, le RGPD définit les droits des personnes concernées vis-à-vis du traitement de leurs données personnelles.

EXTRAITS

1. LE DROIT D'ACCÈS (ART. 15)

« La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel […] »

2. LE DROIT DE RECTIFICATION (ART. 16)

« La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. »

3. LE DROIT À L'EFFACEMENT OU « DROIT À L'OUBLI » (ART. 17)

« La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais […] »

4. LE DROIT À LA LIMITATION DU TRAITEMENT (ART. 18)

« La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement […] »

5. LE DROIT À LA PORTABILITÉ DES DONNÉES (ART. 20)

« Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle […] »

6. LE DROIT D'OPPOSITION (ART. 21)

« La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. »

7. LE DROIT DE NE PAS FAIRE L'OBJET D'UNE DÉCISION FONDÉE EXCLUSIVEMENT SUR UN TRAITEMENT AUTOMATISÉ (ART. 22)

« La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant

des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. »

« ACCOUNTABILITY », « PRIVACY BY DESIGN » ET « PRIVACY BY DEFAULT »

A travers l'article 25, le RGPD introduit les principes de « Privacy by Design », et « Privacy by Default ». Le premier consiste à mettre en œuvre les mesures appropriées en matière de protection des données dès la conception d'un traitement afin d'assurer sa conformité au RGPD, tandis que le second consiste à mettre en œuvre les mesures nécessaires pour garantir que seules les données nécessaires sont collectées et traitées, et ceci avec le niveau de protection maximal. Les organisations se doivent donc d'être dans une démarche proactive de protection des données personnelles, avant que le risque ne se manifeste.

Ces principes et les diverses mesures prévues au RGPD sous-tendent un principe plus global de responsabilisation des organisations vis-à-vis de leur conformité au RGPD désigné sous le terme « Accountability ». Au travers de cette logique d'accountability, les organisations ont une obligation de mise en œuvre responsable des mesures nécessaires au respect des règles en matière de protection des données personnelles et doivent en assurer la traçabilité et pouvoir en rendre compte à travers une documentation détaillée.

ACCOUNTABILITY, DÉFINITION DE LA CNIL

« L'accountability désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. »

DES SANCTIONS EN CAS DE MANQUEMENT

Au-delà d'un rôle d'enquête et de recadrage, le RGPD accorde un véritable pouvoir de sanction aux autorités de contrôle (CNIL) en cas de manquement de la part d'une organisation. Le non-respect des exigences du RGPD peut ainsi entraîner l'application d'une amende pouvant aller jusqu'à 4% du chiffre d'affaires annuel mondial de l'établissement ou 20 millions d'euros, le montant le plus haut étant retenu.

QUELS IMPACTS POUR LES ORGANISMES DE FORMATION ?

LES SPÉCIFICITÉS DE L'ORGANISME DE FORMATION

Nous l'évoquions au début de ce livre blanc : un organisme de formation n'est pas une entreprise comme les autres et notamment au regard des exigences du RGPD. Les traitements de données réalisés par un organisme de formation ne relèvent pas uniquement d'intérêts commerciaux puisqu'ils servent aussi diverses obligations légales vis-à-vis des employés, des apprenants, des clients ou encore des instances de contrôle.

En raison de leur activité, les organismes de formation détiennent et partagent ainsi des données personnelles au sein de flux d'informations variés parmi lesquels :

- Les flux pédagogiques : feuilles d'émargement, attestations de formation, évaluations...
- Les flux contractuels : propositions commerciales, conventions de formation, contrats de sous-traitance...
- Les flux comptables : factures, reçus, subrogations...
- Les flux RH : bulletins de paie, CV...
- Les flux de contrôle : bilan pédagogique et financier...

Chacun des flux d'information dont un organisme de formation est la source ou le destinataire est susceptible de contenir des données à caractère personnel et sera donc impacté par le RGPD.

Les organismes de formation sont particulièrement sensibles au RGPD dans la mesure où chaque prestation concerne, en règle générale, plusieurs acteurs :

- L'apprenant, qui n'est pas toujours le client
- Le client professionnel (par exemple l'employeur de l'apprenant) ou particulier, qui n'est pas toujours l'unique financeur de la formation
- Le financeur, qui paye et qui a également un rôle de contrôle sur la bonne réalisation de la prestation

- Le sous-traitant, si la prestation est réalisée par un formateur externe
- Les organismes publics qui s'assurent du bon usage des fonds alloués à la formation professionnelle et établissent des statistiques

LES PRINCIPALES OBLIGATIONS ET POINTS DE VIGILANCE

Plusieurs nouvelles obligations verront le jour dès l'entrée en vigueur du règlement européen sur la protection des données le 25 mai 2018. En voici les principales ainsi que les points de vigilance à prendre en compte dans une démarche de mise en conformité de l'organisme de formation.

RESPECTER LES DROITS DES PERSONNES CONCERNÉES

Cela va de soi ! Les droits des personnes physiques vis-à-vis du traitement de leurs données personnelles sont repris plus haut dans ce livre blanc, sous forme d'extraits. Nous vous conseillons cependant de vous reporter au texte de loi officiel pour plus détails sur les conditions d'application de ces droits.

ACTION CONCRÈTE POUR VOTRE ORGANISME DE FORMATION

- S'assurer que les procédures en place permettent aux personnes concernées d'exercer leurs droits et de traiter les demandes dans un délai d'un mois maximum.

COLLECTER ET CONSERVER SEULEMENT CE QUI EST NÉCESSAIRE

La réglementation impose de veiller à ne collecter que les informations nécessaires à la finalité du traitement (« Privacy by Default »). Par ailleurs, si la durée de conservation de ces données reste toutefois libre, il convient de ne pas dépasser la durée nécessaire à l'accomplissement des finalités pour lesquelles les données ont été collectées. En d'autres termes, les données doivent être supprimées aussitôt qu'elles ne présentent plus d'intérêt légitime pour le responsable de traitement.

ACTION CONCRÈTE POUR VOTRE ORGANISME DE FORMATION

- Vérifier que les données que vous collectez habituellement ont une utilité pour la finalité prévue et définissez vos futurs traitements en veillant à respecter cette règle.

- Fixer des durées de conservation raisonnables au regard de l'utilisation qui est faite des données. Notez qu'il faudra vous référer en premier lieu à la durée de conservation fixée par la loi (ex. Code du travail, référentiel de formation…) dans la mesure où elle existe.

SÉCURISER LES TRAITEMENTS DE DONNÉES

Le responsable de traitement est tenu de mettre en œuvre, dès la conception du traitement puis tout au long de l'utilisation des données, les mesures appropriées afin de garantir le niveau de protection le plus élevé possible.

ACTION CONCRÈTE POUR VOTRE ORGANISME DE FORMATION

- Utiliser des méthodes de pseudonymisation (remplacement de certaines données par un pseudonyme) et de chiffrement (cryptage) des données afin de séparer les données personnelles de l'identité de la personne ou de les rendre illisibles en l'absence du code de décryptage adéquat.
- Effectuer des sauvegardes régulières et sur différents supports sécurisés.
- Limiter l'accès aux données en utilisant des outils accessibles par identifiant et mot de passe individuels et en gérant des niveaux d'habilitation de vos collaborateurs en fonction de leurs activités au sein de l'organisme de formation.

NOTIFIER LES FAILLES DE SÉCURITÉ

En cas de violation de données à caractère personnel, et si cette violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, le responsable de traitement doit notifier la violation en question à la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance.

ACTION CONCRÈTE POUR VOTRE ORGANISME DE FORMATION

- Mettre en place une procédure de gestion des failles de sécurité (identification, correction, démarches juridiques, communication aux personnes concernées…).
- Préparer un modèle de notification à destination de la CNIL.
- Préparer un modèle de communication à destination des personnes concernées par l'éventuelle fuite de données (apprenants, clients professionnels, collaborateurs).

INFORMER LES PERSONNES ET OBTENIR LEUR CONSENTEMENT PRÉALABLE

Pour tout traitement de données il est impératif d'informer la personne physique sur la finalité du traitement et d'obtenir son consentement préalablement à la collecte des données. Il faut également être en mesure de prouver que la personne a consenti à l'opération de traitement des données de manière libre.

ACTION CONCRÈTE POUR VOTRE ORGANISME DE FORMATION

- Rédiger les notes d'informations relatives au(x) traitement(s) de données que vous effectuez en termes simples et clairs (données collectées, finalité du traitement, durée de conservation, les coordonnées du responsable de traitement, un rappel des droits des personnes vis-à-vis de leurs données). Vous pourrez ensuite les communiquer aux personnes concernées en les intégrant à différents documents comme par exemple vos conditions générales d'inscription, le règlement intérieur applicable aux stagiaires…
- Recueillir le consentement des personnes dès que possible et au plus tard au moment de la collecte des données, par exemple grâce à une case à cocher dans un formulaire, qu'il soit papier ou numérique. Attention, pour que le consentement soit valable, la case en question ne doit surtout pas être pré-cochée !
- Mettre en place une mesure de conservation des consentements obtenus. En fonction de la méthode de recueil adoptée vous pourrez opter pour l'archivage papier, numérique, ou une base informatique…

ENCADRER LA SOUS-TRAITANCE

Avant le RGPD, la plupart des obligations en matière de protection des données personnelles concernaient uniquement le responsable de traitement. Ces obligations sont désormais étendues au sous-traitant qui traite les données à caractère personnel pour le compte du responsable du traitement, et en cas de manquements, l'un et l'autre pourraient ainsi voir leur responsabilité engagée. Dans ce contexte, le RGPD impose qu'un contrat écrit soit établi entre le responsable de traitement et le prestataire. Au-delà de décrire le traitement en lui-même (finalité, durée, destinataire…), ce contrat prévoit que le sous-traitant s'engage à ne traiter les données à caractère personnel que sur instruction documentée du responsable du traitement, à mettre en œuvre les mesures de sécurité nécessaires à la protection des données, à ne pas faire lui-même appel à un sous-traitant sans l'autorisation du responsable du traitement…

ACTION CONCRÈTE POUR VOTRE ORGANISME DE FORMATION

- Mettre à jour les contrats avec vos sous-traitants (formateurs externes, gestionnaires de plateforme e-learning, cabinet comptable…) en ajoutant ou révisant les clauses relatives à la protection des données personnelles.

ÊTRE EN MESURE DE DÉMONTRER LA CONFORMITÉ AU RGPD

Le responsable de traitement doit être en mesure de prouver, notamment en documentant ses mécanismes et procédures internes, qu'il remplit l'ensemble de ses obligations vis-à-vis du RGPD.

ACTION CONCRÈTE POUR VOTRE ORGANISME DE FORMATION

- Rédiger et tenir à jour un Registre des Traitements de Données. La CNIL explique ce qu'il doit contenir et met à disposition un modèle sur son site internet. Ce registre doit recenser et détailler tous les traitements de données de l'organisme de formation.
- Rassembler les documents relatifs à l'information des personnes, au recueil du consentement ainsi qu'aux mesures mises en place pour veiller à l'exercice de leurs droits (procédures, modèles, exemples). Les preuves de consentement doivent également être consultables.
- Rassembler les contrats avec les sous-traitants avec qui vous partagez des données ainsi que les procédures en cas de violation de données.

PAR OÙ COMMENCER ?

Pour amorcer la mise en conformité de votre organisme de formation vis-à-vis des exigences du RGPD vous pouvez commencer par :

CARTOGRAPHIER LES TRAITEMENTS DE DONNÉES

Afin d'être en mesure d'estimer l'impact du RGPD sur l'activité de votre organisme de formation il est conseillé de procéder à une cartographie des traitements des données personnelles. Il s'agit de :

- Identifier les traitements et les données traitées.

- Identifier les acteurs, internes ou externes, qui interviennent dans ces traitements.
- Identifier les flux des données en précisant leur provenance et leur destination.

DÉSIGNER UN RESPONSABLE DE TRAITEMENT (ET PEUT-ÊTRE UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES)

La définition du responsable de traitement est large, si bien qu'au sein du RGPD ce terme désigne « l'entité » qui traite les données. Sur le plan opérationnel, il convient de nommer une personne interne à l'organisme de formation afin d'assurer ce rôle pour chaque traitement de données que vous aurez identifié. Le responsable de traitement sera en charge de « [mettre en œuvre] les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au [RGPD]. Ces mesures sont réexaminées et actualisées si nécessaire ».

Dans certains cas (traitement de données sensibles ou suivi régulier à grande échelle notamment), il est obligatoire de nommer un délégué à la protection des données personnelles (DPO), qui s'assure que tout est mis en œuvre dans l'entreprise pour garantir la conformité. Le DPO doit être nommé sur la base de ses qualités professionnelles, de son expertise en matière de protection des données personnelles et de son impartialité. Il est notamment le point de contact entre l'organisme de formation et les autorités de contrôle.

RÉALISER LES ÉTUDES D'IMPACT NÉCESSAIRES

L'étude d'impact ou Privacy Impact Assessment est obligatoire pour les traitements de données sensibles, tels que des numéros de sécurité sociale par exemple. Cette étude consiste à analyser un traitement afin d'évaluer la nature et la gravité des risques qu'il engendre au regard des droits et libertés des personnes, et de prévoir les mesures correctives appropriées afin de le rendre plus sécurisé.

Afin d'aider les entreprises à réaliser cette étude d'impact, la CNIL a mis en place le logiciel PIA, disponible gratuitement en téléchargement.

SENSIBILISER LES ÉQUIPES

Pour garantir une mise en place harmonieuse du RGPD au sein de votre organisme de formation, pensez à informer vos collaborateurs sur la protection des données personnelles, les principes et les enjeux.

LE SAVIEZ-VOUS ? ARGALIS, EST DÉJÀ CONFORME AU RGPD !

Le logiciel Argalis, outil de gestion dédié aux organismes de formation, vous aide d'ores et déjà à répondre à plusieurs obligations imposées par le RGPD :

SÉCURISATION DES DONNÉES

La solution Argalis inclut la sauvegarde et la sécurisation des données sans que vous ayez à vous en occuper ! Les données que vous traitez sont enregistrées et sauvegardées dans un espace cloud sécurisé hébergé en UE et utilisant les technologies de protection les plus performantes.

CONFIDENTIALITÉ

Argalis offre la possibilité d'administrer les rôles des utilisateurs afin de gérer les habilitations de chacun de vos collaborateurs. Un utilisateur accède ainsi uniquement aux données utiles à ses activités.

INFORMATION DES PERSONNES

Les modèles de documents inclus dans Argalis comportent les mentions nécessaires à l'information des personnes sur les traitements dont leurs données vont faire l'objet.

PORTABILITÉ DES DONNÉES PERSONNELLES

Argalis permet de répondre en un clic aux demandes d'accès et de portabilité des données personnelles grâce à l'export de fichiers numériques structurés et lisibles par les logiciels courants.

Envie d'en savoir plus ?
Contactez-nous aux coordonnées suivantes
+33 (4) 78 95 34 73
contact@argalis.fr
www.argalis.fr