VEILLE JURIDIQUE - Données personnelles

Etat des lieux

Une entreprise comme ARES Formation, une école, manipule des données personnelles tous les jours (nom, prénom, adresse, date de naissance d'élèves comme formateurs, CV, contrats).

Pour toute donnée physique, remise sur papier, les dossiers sont rangés puis archivés, 5 ans après le départ de la personne de l'entreprise, ce qui prend en compte : un étudiant ayant fini ses études, un formateur ayant arrêté son contrat et de même pour les salariés.

De plus, de nombreuses données sont conservées sur l'application web "PPAP" propre à ARES. Les utilisateurs renseignent leur nom, prénom, numéro de téléphone, adresse, date de naissance, peuvent y ajouter un CV et importer de nombreux fichiers dans des éléments de type "GED" sous forme d'un "Drive" (c'est-à-dire une gestion électronique des documents). Actuellement l'application web stocke et garde un historique et une traçabilité grâce à des "logs" sur une seule et même base de données. Des utilisateurs peuvent être considérés comme inactifs et donc ne plus avoir d'accès à l'application, mais leurs données seront toujours stockées.

Dernièrement, ARES met régulièrement en place des enquêtes, sondages sur la satisfaction de l'application web "PPAP" en prenant en compte les données engagées.

Présentation générale et historique des données personnelles

Tout d'abord, la CNIL (Commission Nationale de l'Informatique et des Libertés) est une autorité administrative indépendante, c'est le régulateur des données personnelles, elle peut imposer des sanctions à ceux qui ne respectent pas le RGPD.
Avant la CNIL il existait le projet SAFARI, entre 1970 et 1972 (**S**ystème **A**utomatisé pour les **F**ichiers **A**dministratifs et le **R**épertoire des **I**ndividus). Ce projet avait pour but d'homogénéiser la récolte des données, fiches administratives des Français, en attribuant un identifiant unique pour pouvoir créer un répertoire interconnecté. C'est ainsi qu'a été créée cette commission le 6 janvier 1978, avec la loi "Informatiques et libertés" après l'arrêt du projet SAFARI que les Français trouvaient invasif et une atteinte aux libertés.

Selon la CNIL, "Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise."

Les données personnelles s'inscrivent dans le RGPD. Cependant, une protection des données personnelles ne signifie pas forcément se plier au RGPD, mais elle peut s'en rapprocher.

De plus, l'ANSSI est un autre régulateur de données. "Autorité nationale en matière de cybersécurité et de cyberdéfense en France, l'ANSSI a cinq grandes missions : défendre, connaître, partager, accompagner, réguler.". L'ANSSI propose plusieurs certifications afin de monter en compétences en matière de Cybersécurité.
Actuellement la plateforme SecNumacademie n'est pas disponible mais propose une expérience de formation et certification (MOOC). Une nouvelle version sera disponible courant 2026.
https://secnumacademie.gouv.fr/
En ce qui concerne le monde professionnel, le plus intéressant sont les formations de Niveau 2 : pour les professionnels utilisant le numérique ou les étudiants voire de

Niveau 3 : Approfondissement : pour ceux qui travaillent déjà dans la cybersécurité. A la fin de ces certifications, la plateforme propose des attestations de réussite.

Le RGPD correspond au règlement général sur la protection des données. Il est entré en vigueur le 25 mai 2018. Selon le site du gouvernement : “Le RGPD impose à tous les professionnels un strict encadrement du traitement des données, quels que soient leur secteur et leur taille. “

Le RGPD a 3 objectifs principaux :

- Renforcer les droits des personnes,
- Responsabiliser les acteurs traitant des données,
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

Dernières informations concernant les données personnelles

La Commission européenne souhaite assouplir la réglementation du RGPD, le 19 novembre 2025 avec des mesures dites « Digital Omnibus ».

Dans ce cadre, une proposition concernant les données personnelles serait soumise, modifiant l’article 9 du RGPD qui concerne le “Traitement portant sur des catégories particulières de données à caractère personnel”.
Ainsi, la proposition modifierait la définition de données sensibles : la protection renforcée des données pourrait s’appliquer uniquement si les informations révèlent directement, explicitement l’origine ethnique, la religion ou encore la santé. Toute analyse implicite ou déduction ne sera plus prise en compte.

De plus, la CNIL a créé l’IA Act le 13 juin 2024 afin de réguler et présenter des obligations aux fournisseurs de systèmes d'IA. Cela devient la législation européenne sur l’IA. Ainsi, depuis décembre 2024, la CNIL ne s’oppose pas à ce que les entreprises puissent exploiter les données personnelles afin d’entraîner une intelligence artificielle sur la base de *« l’intérêt légitime ».*

Aussi, la CNIL a sondé 2 082 Français âgés de 15 ans et plus en 2024 afin de “savoir s’ils avaient subi une utilisation frauduleuse ou non contrôlée de leurs

données personnelles, ainsi que sur les préjudices matériels ou immatériels qui en ont découlé.”

- https://www.cnil.fr/fr/cybercriminalite-risques-et-consequences-pour-les-donnees-personnelles

UTILISATION FRAUDULEUSE DES DONNÉES PERSONNELLES	PRÉVALENCE	PART MENANT À UN PRÉJUDICE	PART MENANT À UN PRÉJUDICE MORAL (STRESS, ANXIÉTÉ)	PART MENANT À UN PRÉJUDICE FINANCIER	PRÉJUDICE FINANCIER MOYEN
Une fraude à l'identité	16 %	70 %	28 %	24 %	915 €
Un démarchage non sollicité	24 %	35 %	15 %	29 %	691 €
Une fraude ou tentative de fraude financière	5 %	65 %	26 %	75 %	592 €
Divulgation d'informations « compromettantes »	7 %	76 %	27 %	18 %	609 €
Du chantage ou du harcèlement	4 %	71 %	19 %	13 %	450 €

Utilisations frauduleuses des données personnelles perçues lors des trois dernières années par les répondants

Problématique

Actuellement il n’existe aucun archivage des données sur “PPAP”, avec une seule base de données pour tout gérer bien que les données sensibles telles que les mots de passe soient cryptées.

De plus, il n’existe aucune mention légale des données expliquant aux utilisateurs quelles données sont conservées, dans quel but, pour combien de temps et il n’existe aucune demande de consentement claire et visible. Seule une attestation d’entrée avec le règlement intérieur et le processus de gestion des demandes est mise en place.

Propositions de solutions

Plusieurs solutions sont exécutables afin d'aider à la protection des données et donc des utilisateurs. Le but est d'atteindre une transparence et une symétrie des informations.

Tout d'abord, la CNIL propose de tenir un registre des traitements. Cela signifie garder une traçabilité de plusieurs catégories :

- Les acteurs dans le traitement des données (ceux qui traitent et ceux qui sont traités).
- La catégorie des données traitées
- Pour quelles raisons les données sont collectées, quels acteurs ont accès à ces données, et vers qui elles sont redirigées
- La durée de conservation des données
- La manière dont les données sont sécurisées

En ce qui concerne le registre, il peut se formuler de cette manière :

Nom et coordonnées		**Délégué à la protection des données (le cas échéant)**		**Représentant (le cas échéant)**	
Nom		**Nom**		**Nom**	
Adresse		**Adresse**		**Adresse**	
Email		**Email**		**Email**	
Téléphone		**Téléphone**		**Téléphone**	
Département (secteur)	**Finalité du traitement**	**Catégories de personnes**	**Catégories de données personnelles**	**Qui traite la donnée**	**Temps de conservation**
Nom du secteur	*Pourquoi ?*	*Qui est visé ?*	*Quelles données ?*	*Pour qui?*	*Sur combien de temps ?*
Nom du secteur	*Pourquoi ?*	*Qui est visé ?*	*Quelles données ?*	*Pour qui?*	*Sur combien de temps ?*

Ensuite, il serait conseillé pour l'entreprise de ne collecter que les données strictement nécessaires afin d'éviter une conservation inutile de données non-essentielles.
Enfin, une des solutions proposées serait de s'assurer une sécurité des données avec des mots de passe plus robustes et changés plus régulièrement en suivant les recommandations de la CNIL (~ 12 caractères, majuscule, minuscule, caractère spécial, chiffre), des sauvegardes très régulières avec un archivage des données, mais aussi de permettre aux utilisateurs d'avoir un contrôle sur ces dernières (accès, rectification, suppression, opposition). Également l'utilisateur pourrait avoir le droit d'accès à ses données (sous forme de copie).
Actuellement l'utilisateur sur PPAP peut modifier ses informations personnelles (adresse, code postal, ville, téléphone, email, date de naissance ainsi que les données concernant la situation de handicap d'un utilisateur) .

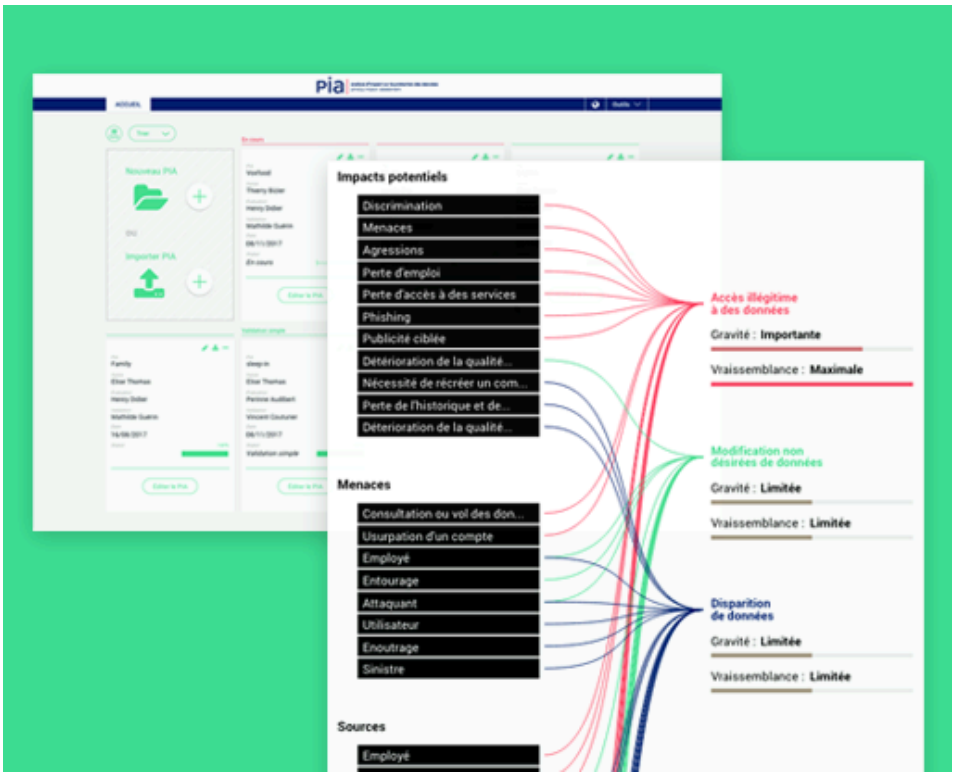
De manière plus régulière, l'entreprise peut mettre en place une analyse d'impact relative à la protection des données (AIPD). Elle est composée de :

- Une description détaillée du traitement (aspects techniques et opérationnels compris).
- Selon la CNIL : "L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux" c'est-à-dire tout ce qui est fixé par la loi concernant les données et leur conservation
- Une étude plus technique des impacts, risques et sécurité concernant la sécurité des données

L'idée est ici pour ARES de se préparer et à chaque nouveau traitement puisqu'une AIPD doit se faire en amont d'un déploiement, cela peut alors permettre une sécurité et une organisation optimale d'un nouveau traitement de données, par exemple lors de l'ajout d'une nouvelle fonctionnalité comprenant des données personnelles sur PPAP et de minimiser le risque de fuites de données. L'AIPD est mise en place par le responsable de traitement (souvent la direction de l'école) coordonné avec le DPO. Ce n'est pas un outil à transmettre à la CNIL mais il peut être nécessaire de le garder à disposition en cas de contrôle, cela agit comme preuve de moyen mis en place.

Pour mettre en place une AIPD, une entreprise comme ARES Formation peut utiliser un outil comme le logiciel open-source “PIA” qui propose une base de connaissance juridique : *“L’outil inclut les points juridiques qui garantissent la licéité du traitement, ainsi que les mesures protectrices des droits des personnes concernées. Il dispose aussi d’une base de connaissance contextuelle accessible à tout moment lors de la réalisation de votre analyse et dont les contenus, reposant sur le RGPD ainsi que sur les guides AIPD et le guide sécurité de la CNIL, s’adaptent aux éléments étudiés du traitement.”*

- https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil



En ce qui concerne la transparence de la collecte des données :

1. Sur PPAP, il pourrait être nécessaire de créer une page “Mentions Légales” avec un rappel précisant quelles données sont utilisées, dans quel but les données sont stockées, sur combien de temps elles peuvent être conservées, mais aussi qu’un utilisateur a le droit de rétractation sur ses données (pouvoir les supprimer), dans quel cas et comment ces données seront archivées.

À la suite de ceci, l’utilisateur devra attester qu’il a pris connaissance de ces informations.

https://www.economie.gouv.fr/entreprises/developper-son-entreprise/innover-et-numeriser-son-entreprise/mentions-sur-votre-site-internet-les-obligations-respecter#

Utilisation de données personnelles : quelles informations donner à l'internaute ?

Le **Règlement général sur la protection des données (RGPD)** précise les informations que vous devez rendre disponibles.

Ainsi, **en cas de collecte de données personnelles des internautes** (nom, prénom, adresse mail, photo, etc.), vous avez un **devoir de transparence**, qui vous oblige à :

- **obtenir le consentement éclairé de l'internaute,**
- **l'informer sur le motif et l'usage des données collectées.**

Afin de respecter votre devoir d'information au moment de la collecte de données personnelles, vous devez donner accès aux informations suivantes :

- identité et coordonnées de l'organisme responsable du traitement de données comme le **délégué à la protection des données (DPO)**, ou un point de contact sur les questions de protection des données personnelles,
- base juridique du traitement de données (consentement de l'internaute, respect d'une obligation prévue par un texte, exécution d'un contrat, etc.),
- finalité des données collectées (Par exemple : pour prise de décisions automatisée, pour prévenir la fraude, parce que les informations sont requises par la réglementation, etc.),
- caractère obligatoire ou facultatif du recueil des données et les conséquences pour la personne en cas de non-fourniture des données,
- destinataires ou catégories de destinataires des données,
- durée de conservation des données,
- droits de l'internaute : droit de refuser la collecte, droit d'accéder, de rectifier et d'effacer ses données, et droit de déposer une plainte auprès de la Cnil,
- transfert de données à caractère personnel envisagés à destination d'un État n'appartenant pas à l'Union européenne.

2. Aussi, il serait approprié pour l'entreprise ARES Formation de préparer un plan d'action, un plan de réponse de prévention en cas de fuite de données afin de garder une transparence totale et une méthodologie à respecter.
3. De plus, il serait bon pour PPAP de posséder un système d'archivage de données en ligne afin de respecter le délai déjà existant pour tous les documents papier, c'est-à-dire 5 ans après le départ d'une personne de l'école. Ici, dès lors que son compte est inactif.
4. Aussi, l'utilisateur sur PPAP doit avoir :
    - Droit d'accès : pouvoir consulter les données renseignées
    - Droit de rectification : pouvoir corriger ou mettre à jour des données inexactes
    - Droit à la portabilité : pouvoir récupérer ses données
    - Droit à l'oubli : pouvoir demander la suppression de ses données

5. Enfin, ARES Formation pourrait nommer un DPO, un délégué à la protection des données afin d'être accompagné dans ces démarches mais aussi de pouvoir accompagner les utilisateurs ayant des questions ou requêtes.

Etude d'impact et évolution possible

L'impact de ces propositions concerne toute l'application et l'entreprise dans sa globalité. Tout d'abord, elle touche à l'infrastructure réseau puisqu'il pourrait être nécessaire d'ajouter des serveurs, des bases de données, mais aussi des serveurs de stockage, préparer des scripts de sauvegarde et d'archivage réguliers.
De plus, il est important de noter que la CNIL ne demande pas une obligation de résultat mais principalement une obligation de moyen. C'est-à-dire qu'il est nécessaire de pouvoir prouver que les moyens ont été mis en place même s'ils ont échoué, attestant de preuves.
Il faut aussi s'assurer que le temps de conservation des données est en accord avec les besoins administratifs de l'entreprise (conservation des dossiers scolaires par exemple sur 5 ans après la fin de la formation de l'élève) .
Pour l'entreprise ARES Formation, il serait judicieux de créer 2 registres des traitements, un registre pour toutes les données physiques, matérielles collectées ainsi qu'un registre pour toutes les données dématérialisées en particulier, celles propres à l'application "PPAP".

Analyse financière

Cette nouvelle infrastructure peut avoir un certain coût : des serveurs de stockage OVH peuvent coûter entre 54 euros et 200 euros par mois.
De plus, l'engagement d'un DPO qui n'est pas déjà présent dans l'équipe possède aussi son coût (le salaire moyen d'un DPO est de 38 000 euros/an brut).

Enfin, sur le code l'impact financier sera moindre puisqu'il s'agira de :

- Créer une page de Mentions légales avec un formulaire d'acceptation

- Ajouter une possibilité de “suppression des données” en plus de la modification déjà existante.

Ceci ne représente aucun coût déjà réalisable sur le code actuel de l’application.

Inconvénients

C’est un projet qui nécessite une organisation soutenue et une rédaction minutieuse. Le registre de traitement est une tâche qui demande beaucoup de temps puisqu’elle n’impacte pas uniquement les données renseignées sur PPAP, mais aussi toute donnée sur papier.

Cette protection des données ajoute des coûts supplémentaires (infrastructure, DPO, etc.). De plus, c’est une obligation qui demande une technique précise des données manipulées qui ne doit pas entraver la continuité de service pour les élèves, tuteurs, formateurs, salariés sur l’ENT.

L’expérience utilisateur peut aussi être altérée avec l’ajout de mentions légales mais également de demandes de changement de mot de passe régulières si mises en place.

Conclusion : est-ce recommandé de renforcer la protection des données ?

La protection est un enjeu essentiel. Pour une école comme ARES Formation, il semble utile de renforcer la protection des données puisque cela permet une clarté de travail et une gestion plus optimisée en interne. C’est une standardisation des traitements mais surtout un moyen de cartographier ses processus.

Aussi, ces méthodes mises en place permettent de prévenir les risques (fuites de données, piratage, perte de données) et renforcer la sécurité d’un ENT (espace de travail numérique) comme PPAP qui gère des notes, bulletins, gestion de tickets interne, contrats de travail. Cela permet par ailleurs de s’assurer de l’exactitude et de l’intégrité de la donnée.

De plus, c’est une transparence nécessaire pour les utilisateurs et permet d’instaurer un climat de confiance avec ces derniers, à ne pas négliger : un utilisateur doit savoir quelles données sont traitées sur PPAP, dans quel but et qui les collecte.

Enfin, c'est un engagement juridique et éthique que de pouvoir répondre aux attentes de la CNIL par une justification de moyen et non de réussite.

Sources :

Feedly

Sites officiels du gouvernement :

- https://cnil.fr/fr
- https://www.cnil.fr/fr/comprendre-le-rgpd
- https://www.economie.gouv.fr/entreprises/gerer-son-entreprise-au-quotidien/assurer-sa-cybersecurite-et-la-protection-de-ses/le#
- https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- https://www.politico.eu/article/donnees-personnelles-leurope-va-assouplir-sa-reglementation-dans-les-semaines-a-venir/
- https://cnil.fr/fr/actualites
- https://www.lemondeinformatique.fr/actualites/lire-la-refonte-du-rgpd-par-l-ue-inquiete-98455.html
- https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd