

Le présent tutoriel vous permet
d'appréhender l'outil et et les
fonctionnalités de GestRGPD crée
par Alsaperfo ©.

Cet outil vous permet de gérer, en
interne, la mise en conformité au
Règlement Général pour la
Protection des Données.

Tutoriel GestRGPD

Edition Juillet 2023

Alsaperfo SAS



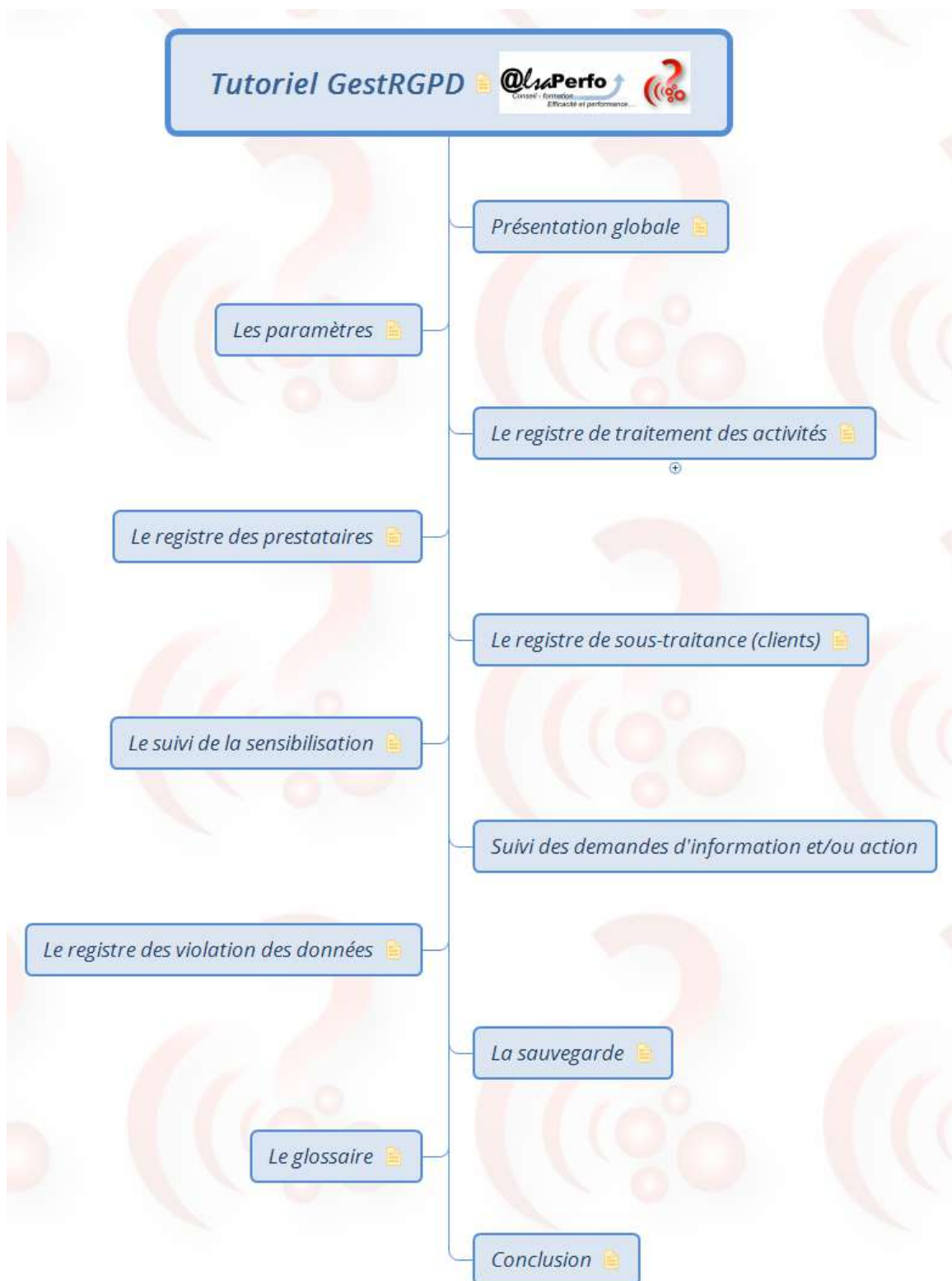
@lsaPerfo
Conseil - formation
Efficacité et performance...



Tutoriel GestRGPD

1. Présentation globale	3
2. Les paramètres	6
3. Le registre de traitement des activités	7
3.1. Renseignement d'une fiche d'activité	9
3.2. Modification d'une fiche d'activité	16
3.3. Suppression d'une fiche d'activité	16
3.4. Exporter les fiches d'activité	16
3.5. Exporter la cartographie des traitements.....	17
3.6. Visualiser l'importance des risques pour les activités	18
4. Le registre des prestataires.....	19
5. Le registre de sous-traitance (clients).....	20
6. Le suivi de la sensibilisation.....	22
7. Le suivi des demandes d'information ou actions	23
8. Le registre des violations des données	25
9. La sauvegarde	25
10. Le glossaire.....	26
11. Conclusion	27

Tutoriel GestRGPD



Pour lancer l'application GestRGPD, il suffit d'ouvrir le programme. Vous vous trouverez sous l'onglet «Commande». C'est sous cet onglet que se situe le tableau de bord - Gestion RGPD. L'application fonctionne sous Excel de Microsoft. Ce fichier dispose de macros, il vous faudra activer ces dernières avant de pouvoir travailler avec GestRGPD. La mise à jour des liens n'est pas nécessaire. Lorsque vous êtes invité à mettre à jour les liaisons, vous pourrez cliquer sur «Continuer sans mettre les liaisons à jour».

GestRGPD - le tableau de bord de la gestion RGPD Version 4.3

Quitter

Passer en mode plein écran
"Esc" pour en sortir

Informations entreprise

Activités de traitement

- Paramétrage risques et mesures
- Création d'une activité de traitement
- Gestion fiches de traitement
Renseignement / modification / suppression
- Généraliser le registre des traitements
- Cartographie des activités de traitement
- Visualisation graphique de l'importance des risques

Registre des prestataires

Nombre de prestataires	7
------------------------	---

Registre de sous-traitance

Nombre de fiches clients	7
--------------------------	---

Nous sommes le :
mardi 9 mai 2023

Nombre de fiches d'activités de traitement	14
--	----

Suivi des sensibilisations

Date de la dernière sensibilisation	16/01/2022
-------------------------------------	------------

Registre de violation des données

Date du dernier incident	#N/A
--------------------------	------

Demandes de droit d'accès

Nombre de demandes traitées	11
-----------------------------	----

Tutoriel

Glossaire

Sauvegarde

@AlsPerfo
Conseil - Formation
Efficacité et performance...

L'utilisation de cet outil est soumise à l'autorisation de Alsaperfo®. L'outil est proposé dans le cadre d'une formation à son utilisation. Toute modification des codes et du programme est interdite.

1. Présentation globale

Le Règlement Général pour la Protection des Données (RGPD) impose à toute structure traitant des données à caractère personnel, de pouvoir prouver sa conformité au dit règlement. Il n'est plus nécessaire d'envoyer quelconque document à la CNIL, mais bien de suivre régulièrement les traitements réalisés par l'organisme.

A ce titre, GestRGPD est un fichier Excel contenant des macros, qui intègre les obligations relatives à ce règlement. Dans l'article 35 du RGPD, le traitement de certaines données dites sensibles impose de réaliser une analyse d'impact. Ces éléments peuvent déjà être intégrés dans GestRGPD, mais l'analyse d'impact poussée peut être réalisée grâce au logiciel PIA (Privacy Impact Assessment) mis à disposition par la CNIL (Commission Nationale de l'Informatique et des Libertés), qui propose un rapport d'analyse d'impact, une cartographie des risques et le plan d'actions.

L'analyse d'impact est obligatoire lorsque le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

Certaines données à caractère personnel sont considérées comme sensible au sens large du terme :

- Numéro de sécurité sociale (NIR)
- Données biométriques
- Données bancaires

Ces dernières ne conduisent pas automatiquement à la réalisation d'une analyse d'impact.

Les données considérées comme sensibles aux yeux de la loi informatique et liberté sont les suivantes :

- Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle
 - Infractions, condamnations, mesures de sécurité
- cf: articles 8 et 9 de la [Loi-I&L] et l'article 8 de la [Directive-95-46].

La notion de risque doit s'apprécier en termes de gravité et de probabilité pour les personnes concernées. Le déclenchement d'une menace s'appuie sur plusieurs typologies de risques que sont les risques humains (externes et internes), le risque terrain (exemple : accès à des locaux non sécurisés, catastrophe naturelle, casse matériel, ...), et le risque informatique (cyberattaques, intrusions, ...).

Les risques peuvent notamment être : l'accès aux données par des personnes non autorisées, la modification non désirée des données, la disparition des données etc.

La CNIL est venue préciser qu'un traitement est présumé comporter un risque important pour la vie privée des personnes si le traitement remplit au moins deux des critères suivants :

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

L'analyse d'impact doit contenir :

- une description systématique des traitements envisagés et de leurs finalités ;
- une évaluation de la nécessité/proportionnalité des traitements ;
- une évaluation des risques pour les droits et libertés des personnes ;
- les mesures envisagées pour faire face aux risques.

GestRGPD fonctionne sur tout ordinateur sous environnement Windows, muni d'Excel. Il faudra, lors du lancement de l'application, « activer les Macros ». La mise à jour des liens proposés n'est pas nécessaire pour fonctionner.

Les obligations auxquelles sont soumises les structures traitant des données à caractère personnel sont les suivantes :

- 1) Tenir un registre de traitement des activités pour les actions conduisant à utiliser des données personnelles (gestion de la paie, opérations de communication, gestion des clients, ...)
- 2) Assurer la co-responsabilité en cas de recours à un prestataire lequel utilisera des données que la structure lui a confiées. Cette opération est facilitée dans *GestRGPD* par la tenue d'un registre de prestataire.
- 3) Proposer une fiche de sous-traitance si la structure agit comme prestataires, donc sous-traitant, pour les opérations réalisées au profit d'une entreprise tierce et pour laquelle la structure utilise des données personnelles qui lui ont été confiées.
- 4) Assurer un suivi de la sensibilisation en interne concernant les sujets pouvant entraîner une compromission des données à caractère personnel.
- 5) Assurer un suivi des violations éventuelles de données à caractère personnel, d'en informer les intéressés, d'en informer la CNIL et de conduire à dépôt de plainte éventuellement.
- 6) Continuellement veiller à la sécurisation des données à caractère personnel et du patrimoine de l'entreprise. Disposer de processus mis à jour et réaliser des opérations d'audits du système de traitement des données.

2. Les paramètres

Les paramètres concernent l'entreprise.

Il convient de renseigner ces différents champs au préalable de tout renseignement ultérieur.

Ces éléments sont intégrés dans les différents documents que l'on voudra créer.

Informations Entreprise / Structure		
Entreprise	ALSAPERFO	
Coordonnées	Voie	
	Code postal	
	Commune	
	Adresse de messagerie/site	www.entreprise@ent.fr
	Numéro de téléphone	
SIRET / SIREN		
Maison mère	Nom	
	Activité	
Coordonnées	Voie	
	Code postal	
	Commune	
	Adresse de messagerie	
	Numéro de téléphone	
Lien vers la déclaration RGPD de la maison mère		
Dirigeant	Nom	André SCHWENK
	Fonction	
Coordonnées	Voie	
	Code postal	
	Commune	
	Adresse de messagerie	dede@dede.fr
	Numéro de téléphone	
Délégué protection des données (si applicable)	Nom	
	Numéro DPD	
Coordonnées	Voie	
	Code postal et commune	
	Adresse de messagerie	contact@alsaperfo.fr
	Numéro de téléphone	
Paramètres Commande Base Cartographie_des_activités Fiche_de_tr		

3. Le registre de traitement des activités

La création du registre de traitement des activités répond à l'article 30 du RGPD.

Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles. Il permet notamment d'identifier :

- les parties prenantes ;
- les catégories de données traitées ;
- à quoi servent ces données, qui y accède et à qui elles sont communiquées ;
- combien de temps les données personnelles sont conservées ;
- comment elles sont sécurisées.

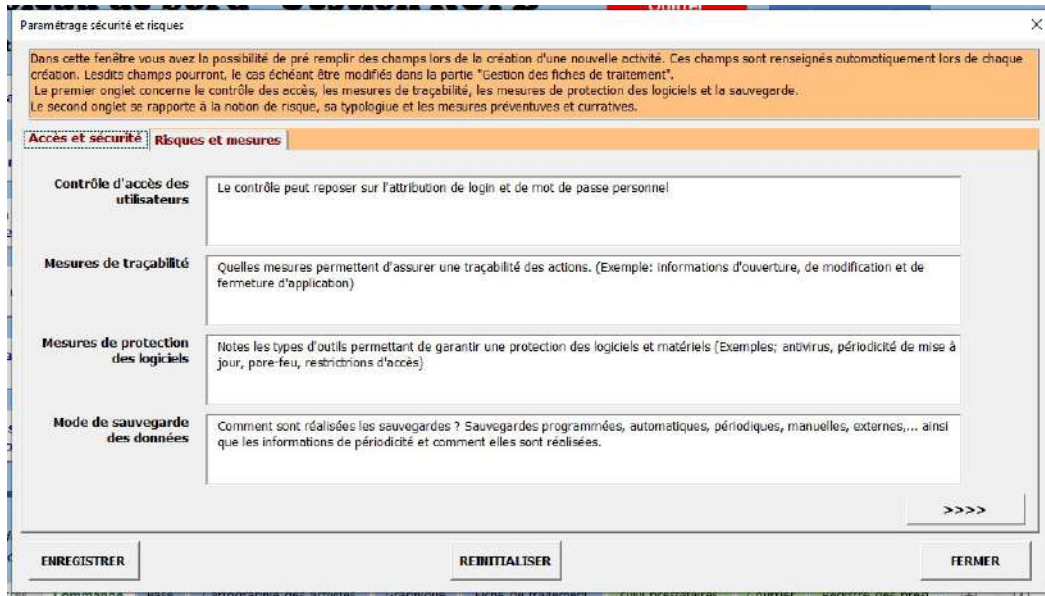
A partir du tableau de bord, il est possible de gérer la partie concernant les activités de traitement.



L'activité de traitement signifie toute utilisation faite de données à caractère personnel dans un but prédéfini (exemple : gestion de la paie, gestion des factures, ...)

La création d'une nouvelle activité de traitement s'effectue en renseignant les différents champs proposés. L'ensemble des champs est requis. Il y a la possibilité de choisir des activités proposées, mais non encore intégrées dans votre base de traitement, mais vous disposez également de la possibilité de créer une toute nouvelle activité de traitement. Cette dernière n'est qu'à renseigner directement dans le champ concerné.

Afin d'automatiser une certaine partie de la démarche, il conviendra de paramétrer les éléments de sécurité, qui sont souvent communes aux différentes activités de l'entreprise, ainsi que des risques auxquels l'entreprise peut être exposée. Ce paramétrage s'effectue en cliquant sur « Paramétrage des risques et mesures ».



Dans cette fenêtre vous avez la possibilité de pré remplir des champs lors de la création d'une nouvelle activité. Ces champs sont renseignés automatiquement lors de chaque création. Lesdits champs pourront, le cas échéant être modifiés dans la partie "Gestion des fiches de traitement".

Le premier onglet concerne le contrôle des accès, les mesures de traçabilité, les mesures de protection des logiciels et la sauvegarde.

Le second onglet se rapporte à la notion de risque, sa typologie et les mesures préventives et curatives.

Pour créer une nouvelle activité, il suffit d'activer le bouton « Création d'une activité de traitement » et de renseigner les champs requis.

Si une activité de traitement existe déjà, vous en serez informé lors de l'enregistrement de cette dernière. Les champs sont ensuite réinitialisés, vous permettant de renseigner une nouvelle activité.

Pour le service concerné, il en va de même. Il s'agit de renseigner le champ.

Le bouton « réinitialiser » va vider les champs renseignés sans procéder à l'enregistrement.

La validation de l'intégration d'une nouvelle activité de traitement dans la base se réalise en cliquant sur le bouton « Enregistrer »

Votre nouvelle activité est ainsi créée. Pour renseigner les éléments relatifs à cette activité vous devrez passer par le tableau de bord de gestion RGPD en cliquant sur le bouton «Renseignement d'une fiche d'activité».

3.1. Renseignement d'une fiche d'activité

Après avoir cliqué sur le bouton «Renseigner une fiche d'activité» apparaîtra une fenêtre globale, reprenant les éléments déjà renseignés lors de la création de l'activité de traitement. Il y a possibilité de faire une recherche d'activité en utilisant les champs «activité de traitement», «Service traitant» ou «responsable de l'activité». Il y a également possibilité de sélectionner, directement dans la fenêtre de résultat, l'activité à compléter. Après avoir sélectionné l'activité, il faudra renseigner les champs relatifs à cette activité et requis par le RGPD.

Dans les zones de texte il est possible de passer à la ligne en appuyant simultanément sur « Shift » et « Entrée ».

Activité de traitement	Service traitant	Responsable de l'activité
Actions de promotion et de sollicitation	Comptabilité	Gérard Dupond
Actions de prospection	Ressources humaines	Hjk Ghjk
Activité de traitement test	Service responsable	Prénom Resp Nom
Actualisation des fichiers de prospection	Ressources humaines	Ghjdk FGHJK
Communication courrier postal	Ressources humaines	Ghjdk FGHJK;

Les différents onglets constituent ces pré requis et se doivent d'être renseignés.

La fenêtre de résultats présente les traitements déjà enregistrés. Il est possible de filtrer ces derniers en utilisant les champs placés au-dessus de la fenêtre.

Les activités présentées sont présentes dans la base mais ne sont pas nécessairement renseignées en totalité.

Le fait de sélectionner l'activité en question présente dans les différents champs présents, ceux qui sont déjà renseignés. Il convient ensuite de renseigner les champs obligatoires. S'il n'y a aucun élément à rajouter (exemple : pas de transfert de données vers un pays hors UE), on peut noter «Sans objet» dans le champs correspondant.

RECHERCHER		
Activité de traitement	Service traitant	Responsable de traitement
<input type="text"/>	<input type="text"/>	<input type="text"/>
Actions de fidélisation	Direction	André SCHWENK
Actions de promotion et de sollicitation	Comptabilité	Gérard DUPOND
Actions de prospection	Ressources humaines	Hjk GHJK
Actions de tests produits	Recherche et développement	Pré1 Nom1
Actualisation des fichiers de prospection	Ressources humaines	Ghjkl FGHJK

Dans l'outil de gestion des fiches d'activité, les onglets font référence aux éléments demandés dans le cadre du RGPD et permettent, en cas de demande de l'autorité de contrôle, d'attester du suivi des actions et de la prise en compte de la protection des données à caractère personnel.

Le premier onglet concerne directement l'activité de traitement. Les premiers champs (activité, service, responsable de l'activité et ses coordonnées) sont pré-remplis suite à la création préalable de l'activité de traitement.

Activité de traitement	Données	Transfert ou destinataires	Mesures de sécurité	Importance du risque	Commentaire
Activité de traitement	<input type="text"/>				Responsable du traitement
Service traitant	<input type="text"/>				<input type="text"/>
Finalité(s) et sous-finalité(s)	<input type="text"/>				
Infos bases légales	Raison légale	<input type="text"/>			
Applications ou logiciels	<input type="text"/>				<input type="button" value="Suivant"/>

Il faut ensuite renseigner le champ concernant la finalité de l'activité, ainsi que les sous finalités éventuelles. En d'autres termes, quel est l'objectif de l'activité de traitement et quels peuvent être les objectifs connexes, entraînant un traitement des données similaire à l'objectif principal.

Le champ de la raison légale indique sur quel principe l'organisme s'appuie pour légitimer le traitement des données à caractère personnel, dans le cadre de cette activité.

Pour chacune de vos finalités, il s'agit de garantir alternativement :

- L'exécution du contrat,
- L'obligation légale,
- L'exécution d'une mission d'intérêt public,
- L'intérêt vital,
- L'intérêt légitime ou
- Le consentement

Il est possible de visionner les différentes définitions en cliquant sur le bouton vous ramenant sur le glossaire.

Finalement, dans cet onglet on trouve le champ relatif aux applications métier utilisées voire les logiciels utilisés dans le cadre du traitement de cette activité.

Nota : un outil de messagerie comprend des données à caractère personnel et se doit d'être indiqué également dans ce champ.

L'onglet «Données» indique la catégorie des individus concernés (ex: collaborateurs, adhérents, clients, ...).

Les données générales sont sélectionnées en cochant les cases prévues. Si des données à caractères personnel ne figurent pas dans la liste proposée, on peut les intégrer dans le champ «Autres».

Il faut également indiquer si l'activité en question intègre des données sensibles. Sélection «Oui/Non».

Si «Oui» est sélectionné, il faut indiquer dans la rubrique «Autres», la typologie de données sensibles en question et le cadre exact de leur utilisation.

Données sensibles : elles sont décrites à l'article 8 de la loi informatique et libertés, et à l'article 9 du RGPD. Certaines données ne peuvent être ni collectées, ni traitées au regard de leur caractère sensible, sauf si la personne a donné son consentement.

Il s'agit des données de santé, des données à caractère racial ou ethnique, des opinions politiques ou syndicales, des convictions religieuses, des données relatives à la vie sexuelle.

L'utilisateur d'une plateforme devra donc se montrer particulièrement vigilant dans la rédaction de ses commentaires s'il veut être en conformité avec la réglementation : il s'interdira par exemple de divulguer l'état de santé de ses clients (séjour à l'hôpital, description d'une maladie). L'utilisation de ce type de données impose de réaliser une analyse d'impact et est soumis à l'autorisation préalable de l'autorité de contrôle.

Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier.

Au-delà, les données peuvent être archivées, sur un support distinct.

La durée de conservation déclarée dans le registre du traitement doit correspondre à la période durant laquelle les données restent accessibles ou consultables, par opposition avec la période d'archivage des données pendant laquelle celles-ci ne sont plus destinées à être utilisées et sont de ce fait, conservées sur un support distinct au sein d'un service d'archives, voire supprimées.

The screenshot shows the 'Données' tab of a form. At the top, there are navigation tabs: 'Activité de traitement', 'Données' (selected), 'Transfert ou destinataires', 'Mesures de sécurité', 'Importance du risque', and 'Commentaire'. Below the tabs, there is a text input field for 'Catégorie de personnes concernées'. Under 'Données collectées', there are several checkboxes: 'Nom / Prénom', 'Date de naissance', 'Adresse postale', 'Adresse mail', 'Numéro de téléphone', 'Numéro national d'identité', 'Relevé d'identité bancaire', 'Carte vitale', 'Curriculum Vitae', and 'Photo d'identité'. Under 'Données sensibles', there are checkboxes for 'Permis de conduire', 'Diplôme / attestation', 'Données de géolocalisation', 'Enregistrement vidéo', and 'Empreintes papillaires'. There is also a dropdown menu and a text input field for 'Autres'. At the bottom, there is a 'Durée de conservation' section with a dropdown menu and a 'Suivant' button.

L'onglet «Transfert ou destinataires» indique le cheminement des données à caractère personnel relatifs à l'activité en question.

On y indique également si des données sont transférées en dehors des pays de l'UE (il est à noter que la Suisse est considérée comme étant membre de l'UE dans le cadre de l'application du RGPD).

Si des données étaient transférées hors UE, on indique la ou les destinations en question.

The screenshot shows the 'Transfert ou destinataires' tab of a form. At the top, there are navigation tabs: 'Activité de traitement', 'Données', 'Transfert ou destinataires' (selected), 'Mesures de sécurité', 'Importance du risque', and 'Commentaire'. Below the tabs, there are three text input fields: 'Destinataires internes' (with the instruction 'Notez ici les autres destinataires internes, devant utiliser les données dans le cadre du traitement de cette activité.'), 'Destinataires externes (hors sous-traitants)' (with the instruction 'Notez ici les destinataires externes, utilisant les données hors cadre d'une sous-traitance contractualisée et dans le cadre légal du licéité du traitement.'), and 'Sous-traitant(s)' (with the instruction 'Notez ici les destinataires avec lesquels vous avez contractualisé des opérations de traitement. Les organismes qui traitent des données à caractère personnel pour votre compte, ou qui peuvent avoir accès à ces données.'). Below these fields, there is a dropdown menu for 'Transfert hors UE' and a text input field for 'Si OUI, indiquez la destination'. At the bottom, there are three buttons: 'Informations transferts', 'Carte de protection des données dans le monde', and 'Suivant'.

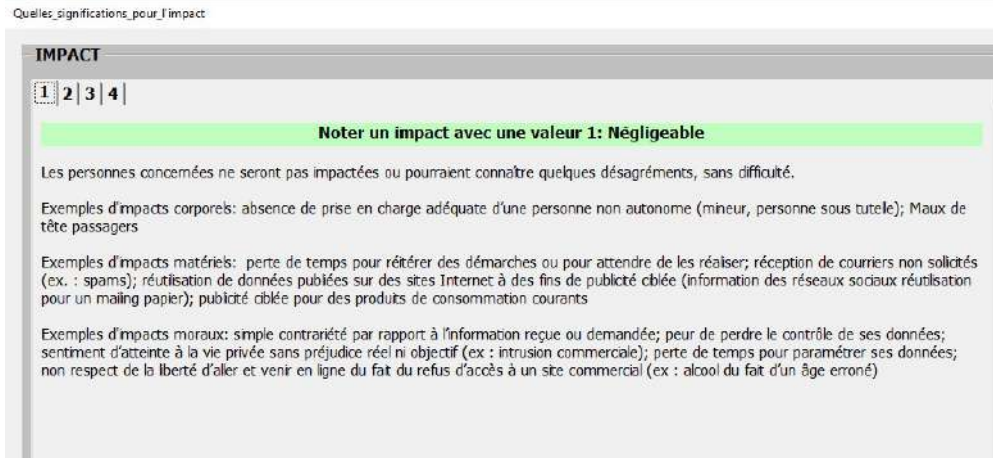
L'onglet «Mesures de sécurité» expose les mesures prises dans le cadre de la sécurisation des données à caractère personnel, ainsi que de la traçabilité en vue d'optimiser cette sécurisation. Ces mesures seront organisationnelles (habilitations, organisation hiérarchique, ...), techniques (mise en place de restrictions d'accès, sécurisation des systèmes d'informations, dont les pare-feu, anti-virus, sécurisation des mots de passe et tout outils concourant à la lutte contre les intrusions dans le réseau, ...)

Activité de traitement	Données	Transfert ou destinataires	Mesures de sécurité	Importance du risque	Commentaire
Contrôle d'accès des utilisateurs	Le contrôle peut reposer sur l'attribution de login et de mot de passe personnel				
Mesures de traçabilité	Quelles mesures permettent d'assurer une traçabilité des actions. (Exemple: informations d'ouverture, de modification et de fermeture d'application)				
Mesures de protection des logiciels	Notes les types d'outils permettant de garantir une protection des logiciels et matériels (Exemples; antivirus, périodicité de mise à jour, pare-feu, restrictions d'accès)				
Mode de sauvegarde des données	Comment sont réalisées les sauvegardes ? Sauvegardes programmées, automatiques, périodiques, manuelles, externes,... ainsi que les informations de périodicité et comment elles sont réalisées.				
Chiffrement des données	<input type="text"/>	Contrôle des sous-traitants		<input type="text"/>	
Autres mesures	Indiquez ici les autres mesures prises comme la sécurisation physique ou les méthodes de chiffrement (outils, spécificités,...)				Suivant

L'onglet mesurant «L'importance du risque» permet d'analyser les risques potentiels auxquels sont soumises les différentes activités. Les risques peuvent être de différentes dimensions et sont souvent interconnectés.

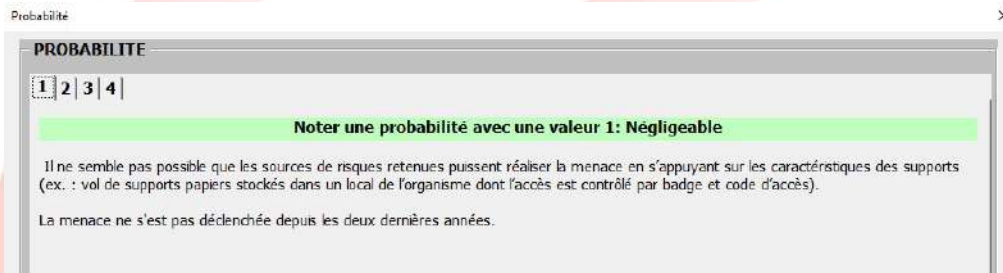
Activité de traitement	Données	Transfert ou destinataires	Mesures de sécurité	Importance du risque	Commentaire
Types de risques	<div style="border: 1px solid red; padding: 5px;"> Donnez les types de risques auxquels cette activité peut être confrontée. Risques humains : internes ou externes, vols, sabotage, imprudence, organisation... Risques terrain : accès non sécurisés, risque électrique, matériel... Risques cyber : intrusion réseau, piratage, vol de données, perte d'intégrité, ... </div>				
Impact	<input type="text" value="0"/>	<input type="text" value="?"/>	Mesures préventives	<input type="text"/>	
Probabilité	<input type="text" value="0"/>	<input type="text" value="?"/>	Mesures curatives	Investigation, dépôt de plainte, utilisation des sauvegardes, révision des processus.	
					Suivant

Cet onglet permet également d'évaluer l'impact, si les données se trouvaient compromises (valeurs de 1 à 4 , 1 étant un impact négligeable et 4 étant un impact maximal)



De même il s'agit ensuite d'évaluer la probabilité que le risque survienne (valeurs de 1 à 4, 1 étant une probabilité négligeable, et 4 une probabilité forte.

En cliquant sur le «?» les valeurs sont expliquées.



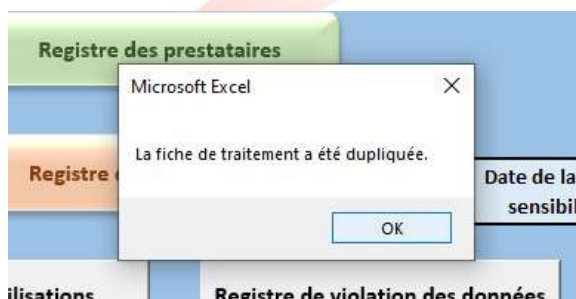
L'importance du risque correspond au produit « IMPACT » X « PROBABILITE » et est reporté sur la fiche de traitement de l'activité.

Impact	2
	Les personnes concernées par une compromission pourraient connaître des désagréments significatifs, qu'elles pourraient surmonter malgré quelques difficultés
Probabilité	3
	Il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports. La menace ne s'est pas déclenchée l'année dernière.
Importance du risque	6

L'onglet « Commentaire et recommandations » contribue à l'optimisation du traitement.



Lorsque les éléments requis auront été renseignés, il suffira de cliquer sur le bouton «Modifier» pour mettre à jour la base de traitement.



Il est possible de dupliquer la fiche en cliquant sur «Dupliquer». L'ensemble des éléments est ainsi dupliqué et une copie de l'activité de traitement est créée. Cette dernière apparaît dans la fenêtre de résultat et peut être modifiée comme toute fiche présente dans cette fenêtre.

La visualisation de la fiche de traitement s'effectue en cliquant sur le bouton «Voir la fiche de traitement»

Le bouton «Fermer» ferme cette fenêtre.

ATTENTION : Si aucune enregistrement n'est réalisé (bouton «Modifier»), l'enregistrement ne sera pas effectif.

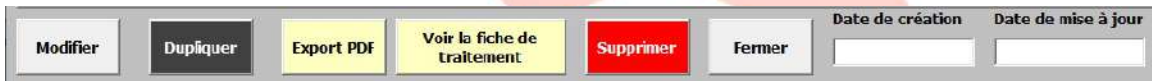
La date de mise à jour est automatiquement intégrée dans la fiche de traitement et dans la base de traitement.

3.2. Modification d'une fiche d'activité

A l'instar du renseignement de la fiche d'activité de traitement, la modification est possible sur tous les champs après sélection de l'activité concernée.

La modification est effective après avoir cliqué sur le bouton «Modifier»

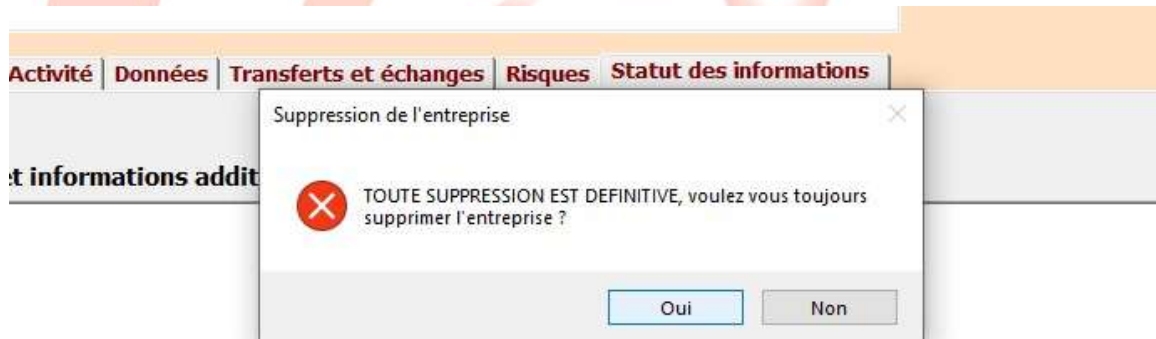
La date de mise à jour est automatiquement intégrée dans la base de traitement.



3.3. Suppression d'une fiche d'activité

On peut supprimer définitivement une activité de traitement en cliquant sur le bouton «Supprimer» (rouge) après sélection dans la fenêtre de résultats.

ATTENTION : toute suppression est définitive.



3.4. Exporter les fiches d'activité

Depuis la fenêtre «Gestion des traitements»:

Après sélection de l'activité dans la fenêtre de résultat, il vous est possible d'exporter la fiche de traitement sous format PDF dans un dossier qui est créé automatiquement au sein du dossier RGPD.

En activant le bouton d'export de fiche d'activité de traitement depuis le tableau de bord de gestion RGPD:

On peut, soit choisir une seule fiche à exporter en utilisant la liste déroulante reprenant l'ensemble des activités de traitement gérées, soit choisir d'exporter la totalité des fiches dans le dossier Fiche de traitement (ce dossier sera créé automatiquement s'il n'existe pas).

La fiche de traitement d'activité choisie est directement visible dans l'onglet en question



3.5. Exporter la cartographie des traitements



Nom	Modifié le	Type	Taille
Actions de fidélisation	28/03/2022 22:19	Document Adobe ...	121 Ko
Actions de promotion et de sollicitation	28/03/2022 22:19	Document Adobe ...	119 Ko
Actions de prospection	28/03/2022 22:19	Document Adobe ...	122 Ko
Actions de tests produits	28/03/2022 22:19	Document Adobe ...	119 Ko
Actualisation des fichiers de prospection	28/03/2022 22:19	Document Adobe ...	120 Ko
Communication courrier postal	28/03/2022 22:19	Document Adobe ...	120 Ko
Communication via le site internet et ou ...	28/03/2022 22:19	Document Adobe ...	118 Ko
Gestion de la dotation en matériel téléph...	28/03/2022 22:19	Document Adobe ...	123 Ko
Gestion des archives	28/03/2022 22:19	Document Adobe ...	126 Ko
Gestion des autorisations d'accès	28/03/2022 22:19	Document Adobe ...	122 Ko
Gestion des clients CRM	28/03/2022 22:19	Document Adobe ...	119 Ko
Gestion des commandes	28/03/2022 22:19	Document Adobe ...	121 Ko
Gestion des contrats	28/03/2022 22:19	Document Adobe ...	120 Ko
Gestion des dotations individuelles (véhi...	28/03/2022 22:19	Document Adobe ...	123 Ko
Gestion des factures	28/03/2022 22:19	Document Adobe ...	120 Ko
Gestion du service après vente	28/03/2022 22:19	Document Adobe ...	123 Ko
Gestion et vente de biens immobiliers	28/03/2022 22:19	Document Adobe ...	121 Ko
Maintenance chez le professionnel	28/03/2022 22:19	Document Adobe ...	119 Ko
Maîtrise des dépenses liées à l'utilisation ...	28/03/2022 22:19	Document Adobe ...	124 Ko
Vidéosurveillance vidéoprotection	28/03/2022 22:19	Document Adobe ...	121 Ko



Lors de l'activation du bouton dévolu à la **cartographie des traitements**, une copie à jour des activités de traitements est réalisée.

Il est possible de visualiser cette cartographie des traitements.

Ou l'exporter directement en version PDF

Cartographie des activités de traitement	
A date du : 29/03/2022	
ALSAPERFO	
Voie postale /	
Site web	www.entreprise@ent.fr
Numéro de téléphone	
SIREN / SIRET	
Dirigeant	
Prénom / Nom	André SCHWENK
Fonction	
adresse de messagerie	dede@dede.fr
Numéro de téléphone	
Délégué à la protection des données (ou assimilé)	
Prénom / Nom	
N° DPO	
adresse de messagerie	contact@alsaperfo.fr
Numéro de téléphone	
Date de mise à jour	Activités de traitement
03/03/2022	Actions de fidélisation
03/03/2022	Actions de promotion et de sollicitation
03/03/2022	Actions de prospection



3.6. Visualiser l'importance des risques pour les activités



Dans la zone de traitement des activités, le bouton « Visualisation graphique de l'importance des risques des activités de traitement », permet d'accéder à l'outil de visualisation. Ce dernier présente l'importance du risque pour chaque activité de traitement, de l'activité ayant la valeur d'importance du risque la plus élevée, à celle ayant la valeur la plus faible.

Le degré d'importance repose sur la prise en compte de l'impact potentiel par rapport à la probabilité que ce risque survienne (**impact X probabilité**).



4. Le registre des prestataires

Le registre des prestataires permet d'assurer le suivi des structures avec lesquelles votre organisme a contractualisé le traitement de données à caractère personnel que nous leur avons confiées.

Prestataire	Mission	Point de contact
TEST12	Formation test10	Délégué à la protection des doi
TEST13	Formation test11	Délégué à la protection des doi
TEST14	Formation test12	Délégué à la protection des doi
TEST15	Formation test13	Délégué à la protection des doi
TEST16	Formation test14	Délégué à la protection des doi

En activant le «Registre des prestataires», vous pouvez apporter les informations requises et intégrer le contrat qui vous lie.

Un prestataire est intégrable dans la base après avoir renseigné les champs et en appuyant sur «Ajouter», ou encore de modifier des éléments d'un prestataire (après avoir choisi le prestataire en question dans la fenêtre de résultats) qui se trouve déjà en base en cliquant sur «Modifier», et après avoir apporté les modifications requises.

Il est également possible de désactiver la ou les entreprise(s) qui ne travaille(nt) plus pour vous de manière temporaire, voire la ou les réactiver le cas échéant.

La suppression peut être envisagée, cette dernière est cependant définitive.

Lorsque l'on ne connaît pas le nom et prénom du DPO (délégué à la protection des données), il suffit de sélectionner «DPO» dans le menu déroulant et de ne pas renseigner le champ «Nom prénom».

Lorsqu'une date de validation (date de signature de contrat par exemple) est intégrée dans le champ concerné, la case «RGPD valide» est activée par défaut.

Cette fenêtre permet, de plus, de générer automatiquement un fichier sous format PDF, nommé « courrier de co-responsabilisation ». Ce courrier, préformaté pourra être envoyé à l'entreprise qui n'a pas encore assuré sa démarche RGPD, ou du moins, qui n'a pas intégré les éléments «RGPD» dans le contrat de prestation.

Le fichier «Courrier de co-responsabilisation» est exporté vers de dossier nommé «Courrier» qui se trouve dans le dossier «02_Prestataires»

La possibilité d'exporter le registre des prestataire est offerte en cliquant sur le bouton «Registre des prestataires». Ainsi, un fichier, sous format PDF est exporté dans le dossier «02_Prestataires». Le fichier sera automatiquement daté.

Registre des prestataires

A date du : 15/04/2022

NOM de L'ENTREPRISE			
Adresse	Rue et nom de rue		
Commune	0000 Commune		
Site web	www.entreprise@ent.fr		
Numéro de téléphone	0300000000		
SIREN / SIRET	8885588800001		
Responsable	Identité du Dirigeant	www.entreprise@ent.fr	0
DPO	Identité du DPO	contact@alsaperfo.fr	0300000000

PRESTATAIRES			
Nom	Co responsabilité établie	Date de validation	Activité
ALSAPERFO	OUI	01/03/2022	
BEPERFO	OUI	02/04/2022	Inactif
CEPERFO	OUI	02/02/2022	
DEPERFO	NON		Inactif

5. Le registre de sous-traitance (clients)

Le registre de sous-traitance sert à prouver la prise en compte du RGPD au niveau de vos clients. Par clients, dans ce cadre, on entend les structures qui vous ont mandatées pour traiter les données à caractère personnel dont elles disposent, à leur profit.

Par exemple, un organisme de formation sera sous-traitant d'une entreprise qui lui demande d'organiser et de conduire une action de formation au profit de ses collaborateurs. Ainsi, cet organisme de formation utilisera des données à caractère personnel des intéressés pour mener cette action.

Il s'agit en fait d'assurer la co-responsabilité dans le cadre de la sécurisation desdites données.

Fiche de sous-traitance

X

RECHERCHER

Entreprise ALSAPERFO TEST4 TESTING1 TESTING3	Activité Gestion des formations Test4 activité activité conofncklj, testing again
---	--

Registre de sous traitance

Afficher uniquement les sous traitances désactivées

Réactiver **Désactiver**

Informations client | **Activité** | **Données** | **Transferts et échanges** | **Risques** | **Statut des informations**

Nom entreprise TESTING3	SIRET/SIREN 545454544	Nom et prénom du responsable Juju Huhuhu
-----------------------------------	---------------------------------	--

Adresse k,k,k,k,k	Adresse Mail vbn...d
Code postal 565665	Nom et prénom du DPO Fftrf Tftrtg
Commune JHHKKHHDH	Adresse Mail ghkl
Site web kjhkhjkh	Suivant
Tél. 455454445	

Export de la fiche de sous traitance **Ajouter** **Modifier** **Supprimer** **Fermer**

Ce registre reprend les caractéristiques suivantes :

Les informations de l'organisme client, c'est à dire pour lequel notre structure est sous-traitance, les différents points de contact, le type de mission dévolu, les données traitées, les transferts éventuels ainsi que les outils, fréquence et supports utilisés, le contrat qui lie les parties, les mesures organisationnelles et techniques mises en œuvre, les risques potentiels.

Le renseignement des différents champs permet de peupler la base de sous-traitance.

Il est ainsi possible d'exporter une fiche de sous-traitance, si le client la demande, mais aussi d'exporter une cartographie reprenant l'ensemble des structures pour lesquelles on agit comme sous-traitant.

Dans la fenêtre de ce registre on peut créer une nouvelle structure, la modifier, la désactiver, la réactiver, mais aussi purement et simplement la supprimer.

ATTENTION : toute suppression est définitive.

On peut choisir de n'afficher que les entreprises «désactivées» pour les réactiver ou tout simplement pour consultation, voire modification.

Lorsque l'on réalise l'export de la cartographie des clients, un fichier sous format PDF est exporté dans le dossier «03_Clients».

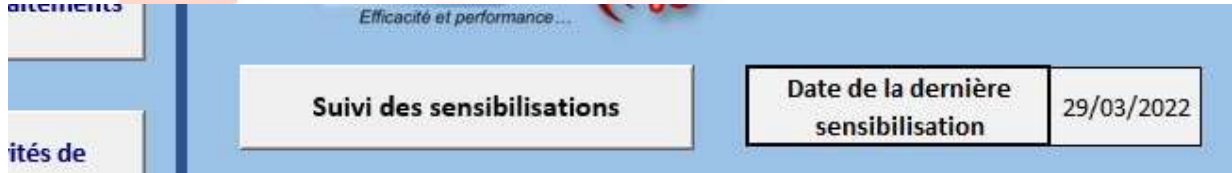
Les éléments suivants se trouvent dans cet export :

Les informations de votre entreprise, la raison sociale de votre client, est ce que la validité du RGPD est notifiée, la date de la notification ainsi que l'activité (travaillez-vous encore pour lui) ou non pour ce client.

6. Le suivi de la sensibilisation

La sensibilisation aux risques est une obligation périodique et régulière imposée par le RGPD. Pour assurer le suivi des sensibilisations, le fichier comporte un onglet qui prend en compte la date de réalisation de la sensibilisation, le sujet, l'intervenant et le ou les destinataires de l'action de sensibilisation.

On peut accéder à cet onglet en cliquant sur le bouton «Suivi des sensibilisations».



Une fois les éléments saisis dans la feuille dédiée au suivi des sensibilisations, il faudra cliquer sur le bouton «Tableau de bord» pour revenir au tableau de commande.

Date	Sujet	Intervenant	Pour qui	Commentaire	Tableau de bord
18/01/2022	Sensibilisation aux risques humains, terrain et Informatiques	André SCHWENK contact@alsaperfo.fr	Dirigeant de l'entreprise	Sensibilisation menée au sein de l'entreprise dans le cadre de la formation à l'accompagnement "conformité RGPD" Le livrable concernant la sensibilisation est mis à disposition au sein de l'entreprise	
29/03/2022	Mise à jour concernant les attaques cyber	André SCHWENK contact@alsaperfo.fr	Dirigeant de l'entreprise	Sensibilisation menée au sein de l'entreprise dans le cadre de la formation à l'accompagnement "conformité RGPD" Présentation des dernières attaques, point sur la nécessité de disposer d'une cellule de crise	

La date de la dernière sensibilisation apparaîtra sur ce tableau de commande.

7. Le suivi des demandes d'information ou actions

Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction (cf article 15 du Règlement général sur la protection des données)

Vous devrez être en mesure de lui faire parvenir une copie des données que vous détenez sur lui et le renseigner sur :

- les finalités d'utilisation de ces données,
- les catégories de données collectées,
- les destinataires ou catégories de destinataires qui ont pu accéder à ces données,
- la durée de conservation des données ou les critères qui déterminent cette durée,
- l'existence des autres droits (droit de rectification, d'effacement, de limitation, d'opposition),
- la possibilité de saisir la CNIL,
- toute information relative à la source des données collectées si celles-ci n'ont pas directement été récoltées auprès de vous,
- l'existence d'une prise de décision automatisée, y compris en cas de profilage, et la logique sous-jacente, l'importance et les conséquences pour vous d'une telle décision,
- l'éventuel transfert de vos données vers un pays tiers (non-membre de l'UE) ou vers une organisation internationale.

Généralement la demande est écrite, soit par courrier postal, soit par mail et il est indispensable de prendre en compte ces demandes et questions. Pour le délai de réponse voici ce que dit la CNIL : « *L'organisme doit vous répondre dans les meilleurs délais et au plus tard **dans un délai d'un mois**. Ce délai peut être porté à trois mois selon la complexité de la demande ou le nombre de demandes reçues par l'organisme (article 12.3 du RGPD). Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans ce même délai d'un mois.*

Si l'organisme ne vous répond pas dans le délai d'un mois ou refuse de faire droit à votre demande, vous pouvez adresser une plainte auprès de la CNIL avec les éléments attestant de vos démarches préalables. Pendant ce délai, vous pouvez demander la limitation du traitement, c'est-à-dire le « gel » de l'utilisation de vos données. »

Le suivi en question est réalisé en activant le bouton « Demande de droit d'accès »



The screenshot shows a dashboard with several data points:

Registre de violation des données	Date du dernier incident	#N/A
Demands de droit d'accès	Nombre de demandes traitées	11

Below the dashboard, there are three buttons: "Tutorial" (yellow), "Classer" (blue), and "Commenter" (grey).

S'ouvre une fenêtre permettant de renseigner les différents champs et de garder une trace de la demande, du canal de demande, de la date de la demande et de celle du traitement.

Rechercher

Type de demande | Origine | Moyen de contact

Type de demande	Origine	Moyen de contact
Rectification	Alain Dupont	Courrier
Rectification	azedfghj	Courrier
Suppression	bghjk	Mail
aaaaa	aaaa	aaaaa
Question	c	Courrier
Rectification	Jean Robert	Mail

Obligations en matière de droit d'accès

Afficher la base de gestion des demandes

Nombre de demandes: 11

Ajouter - Modifier

Origine:

Adresse mail:

Objet de la demande:

Moyen de contact:

Date de la demande:

Mesures prises:

Commentaire:

Date de la réponse: via

Nouvelle demande RGPD

Origine (NOM Prénom):

Adresse mail:

Objet de la demande:

Moyen de contact:

Date de la demande:

Commentaire:

Une demande déjà existante pourra être modifiée.

Pour une nouvelle demande, il suffira de la créer en cliquant sur « Nouvelle demande »

8. Le registre des violations des données

Lors d'une compromission volontaire ou accidentelle significative de données, il faudra prévenir les intéressés ainsi que la CNIL dans les 72h qui suivent la constatation de la compromission.

Pour suivre les compromissions éventuelles, il faut cliquer sur le bouton «Registre de violation des données» qui nous conduit à la feuille de suivi de ces violations.



La feuille de suivi des violations permet d'avoir l'historique des compromissions éventuelles. Cette feuille dispose également du lien de la CNIL pour accéder au compte rendu. Ce dernier sera à renseigner en cas de compromission. La date du dernier incident apparaîtra sur le tableau de commande.

Registre de suivi des violations de données à caractère personnel						Tableau de bord
Notification dans les 72h à l'intéressé et à la CNIL en cas de divulgation				https://notifications.cnil.fr/notifications/index		
Date	Type de violation	Personne concernée	Date de l'évènement	date d'information personne	date d'information CNIL	Commentaires / mesures

Pour revenir au tableau de commande, il faut cliquer sur le bouton «Tableau de bord».

9. La sauvegarde

Le bouton de sauvegarde permet de réaliser une sauvegarde de l'intégralité du fichier GestRGPD. Il n'y aura pas de copie des dossiers ou fiches diverses, puisque tous ces éléments figurent dans le fichier en question et peuvent, le cas échéant être exportés à la demande.



La sauvegarde va se situer dans le dossier «00_Sauvegardes» et sera automatiquement horodatée.

10. Le glossaire

Le glossaire mis à votre disposition reprend les termes généraux concernant le RGPD et vous permet ainsi d'avoir les explications nécessaires et les définitions officielles relatives à ces termes.

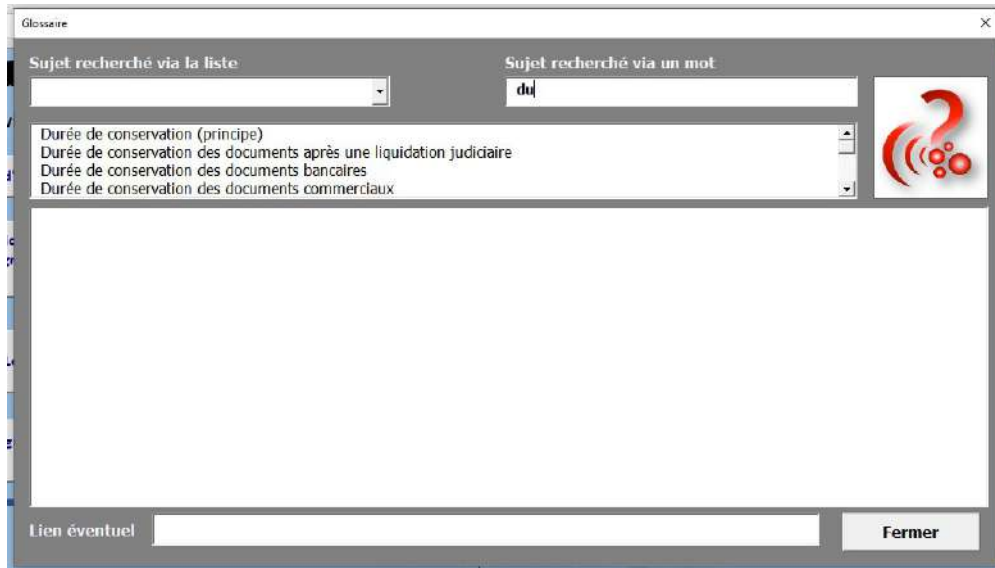
Pour y accéder, un clic sur le bouton glossaire ouvre ce dernier.

La recherche est réalisée grâce à la liste déroulante des termes, mais également en utilisant la recherche par mot.

La fenêtre des résultats propose ensuite les notions et en sélectionnant l'élément demandé, la définition apparaît dans la zone de texte.

Un lien relatif à la notion choisie peut éventuellement apparaître. Il suffit de double cliquer sur le lien en question pour être redirigé vers la page en question.

Cette opération nécessite d'être connecté à Internet.



11. Conclusion

Le présent fichier permet d'assurer le suivi de la gestion relative au RGPD en interne. Naturellement il s'agit là d'un outil à mettre à jour régulièrement. Ce n'est pas cet outil qui va assurer votre conformité mais bien les actions que vous menez en interne au regard de la protection des données et de la sécurisation du patrimoine de l'entreprise. Cet outil se veut être une aide dans l'optimisation des processus, plus qu'un simple outil de démonstration de la conformité de l'organisme.

Alsaperfo®, créateur de l'outil ne pourra pas être tenu responsable de la non-conformité au RGPD de votre organisme, ni du renseignement lacunaire des éléments demandés. Votre organisme est acteur de sa conformité, le délégué à la protection des données en est le chef d'orchestre, certes mais le responsable de la structure en est le responsable aux yeux de la loi.

8 Règles d'OR RGPD

- ✓ Licéité du traitement
- ✓ Finalité du traitement
- ✓ Minimisation des données
- ✓ Protection des données sensibles
- ✓ Conservation limitée des données
- ✓ Obligation de sécurité et confidentialité
- ✓ Transparence
- ✓ Respect des droits des personnes

Ce document est destiné à faciliter la prise en main de l'application **GestRGPD** de **Alsaperfo®**.

L'utilisation de l'application ainsi que du présent tutoriel sont strictement interdits sans autorisation expresse de l'auteur.

Ils demeurent la propriété exclusive de **Alsaperfo®**. Toute modification apportée à **GestRGPD**, outre de ne pas être autorisée, entraînerait un dysfonctionnement de cette dernière.

Document réalisé par André Schwenk, à usage exclusif des utilisateurs autorisés de **GestRGPD**

Le 02/07/2023