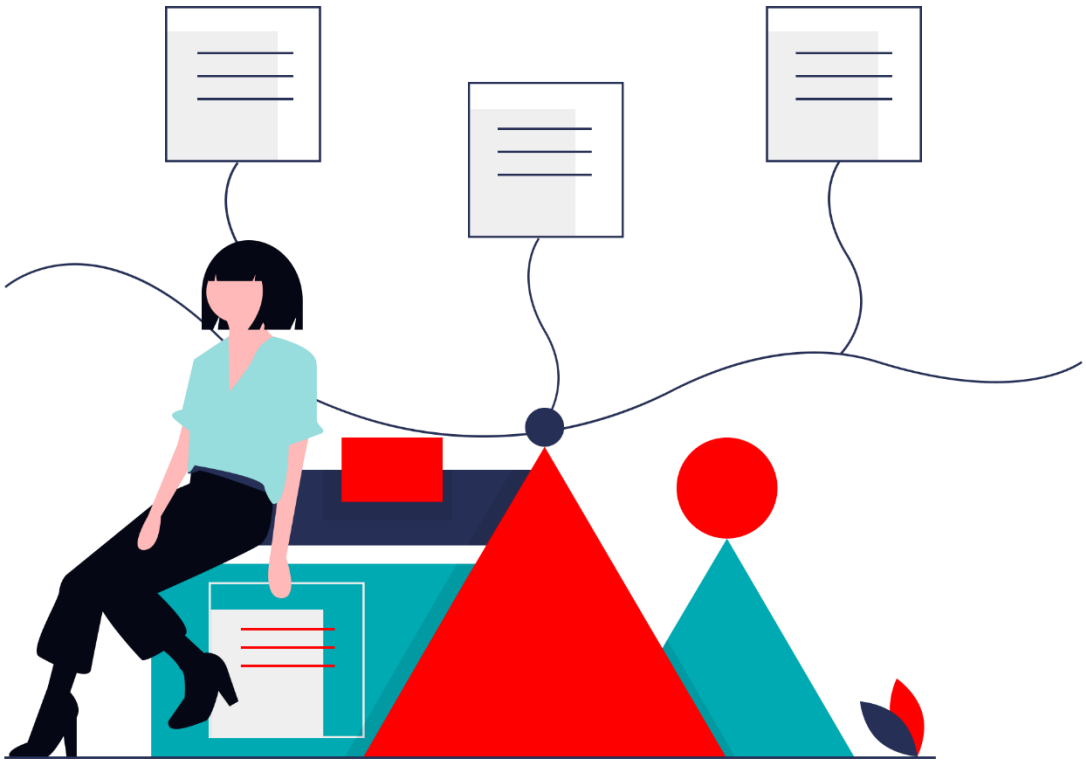
Mémoire technique

RGPD



Sommaire

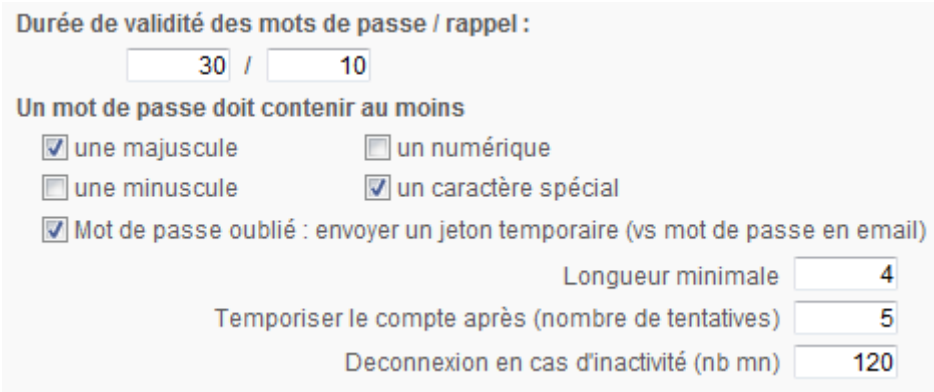
Afin d'accompagner les administrateurs de base documentaire Kentika, un programme de mise en conformité est proposé. Il est composé de différents volets :

- une session de sensibilisation au RGPD et de formation aux outils disponibles dans le kit ;
- une assistance à l'installation du kit ;
- l'utilisation de l'outil d'auto-diagnostic ;
- les éléments du registre.

1. Gestion des mots de passe

1.1. Contrôle à la saisie

Les options avancées de contrôle des mots de passe permettent de prendre en compte l'ensemble des recommandations de CNIL sur le sujet... l'administrateur de la base décide de les activer.



1.2. Gestion des connexions via SSO

Dans le cas où les utilisateurs se connectent à Kentika via SSO, le mot de passe Kentika n'est pas utilisé. Il est alors possible (et recommandé) d'affecter un mot de passe aléatoire (via un script : "Brouiller le mot de passe").

Si la table des personnes est alimentée via une synchronisation avec une source extérieure (exemple : annuaire LDAP, fichier csv...), le filtre d'import comportera un brouillage du mot de passe lors de la création d'un nouveau compte.

2. Recevoir ses données personnelles

Chaque utilisateur peut demander à recevoir l'intégralité de ses données personnelles.

NB : Il s'agit des données personnelles d'historique d'utilisation identifiables comme telles dans le logiciel à l'exclusion des données contenues spécifiquement dans les bases clientes dans les champs de métadonnées personnalisés, les champs de format libre ou encore les documents de Geide qui devront faire l'objet d'une attention et d'un traitement spécifique par le gestionnaire de la base de données.

2.1. Contenu des données personnelles

Le mail produit comporte les sections suivantes :

- les données de la fiche personne ;
- les recherches enregistrées ;
- les emprunts et réservations en cours ;
- l'historique des emprunts ;
- les demandes d'achat ;
- les revues sur lesquelles la personne figure en circulation ;
- les kentapps personnelles ;
- les sélections (ou paniers) ;
- les contributions (notes et commentaires) ;
- les actions lancées ;
- les actions qui ont été attribuées ;
- le log (saisies, modifications, suppressions, consultations, recherches...)

NB : un mécanisme de pseudonymisation des logs et historiques d'emprunts au-delà de six mois (valeur par défaut) fait que ces données anciennes n'apparaîtront pas.

2.2. Le droit à l'oubli

Tout utilisateur peut exercer son droit à l'oubli au travers du portail / mes préférences. Un email est adressé à l'administrateur qui prendra ensuite les dispositions.

A noter : un message d'alerte au cas où des emprunts seraient toujours en cours.

Dans le cas d'un oubli définitif, l'utilisateur ne pourra plus bénéficier des ressources qui lui sont propres et services qui nécessitent une identification.

Attention : si une synchronisation est effectuée avec l'annuaire LDAP, sa fiche pourrait être recréée automatiquement (sans son historique). Il sera alors nécessaire de prévoir une adaptation du filtre d'import pour éviter que ce cas ne se produise.

2.2.1. Traitement de l'oubli définitif par l'administrateur

L'administrateur qui reçoit une telle demande, procède aux vérifications éventuelles et procède à la pseudonymisation de tout ce qui concerne la personne.

NB : l'oubli définitif peut être décidé par l'administrateur. Exemple : lorsque l'une personne quitte la société.

Lorsqu'une personne est "oubliée", les données suivantes sont concernées :

- fiche signalétique : nom, prénom, adresse email, identifiant, type ;
- log ;
- historique d'emprunts ;
- circulation des revues ;
- demandes d'achat ;
- sélections (paniers) ;
- contributions (post) ;
- mail.

Dans le cas d'informations de gestion, l'identifiant de l'utilisateur apparaît sous la forme : $FORGET$$$ suivi d'un numéro. Ceci permet de savoir que, par exemple, une demande d'achat avait été réalisée pour une personne maintenant "oubliée".

3. Audit et auto-diagnostic

3.1. Préambule et avertissement

Le kit RGPD fournit un outil d'assistance à la mise en conformité de son application documentaire : "l'auditeur".

L'auditeur ne vérifie que ce qui est accessible et identifié nativement comme une donnée personnelle.

3.2. Points de contrôles

Ils concernent :

- qui fait quoi ;
- les mots de passe des utilisateurs ;
- le paramétrage des mots de passe ;
- la pseudonymisation.

3.3. Ce qui ne peut pas être contrôlé via l'auditeur

Architecture et production : les données sont-elles bien sauvegardées en Europe ? qui a un accès au contenu du disque dur du serveur ?
Contenu des champs : la fiche signalétique comporte des champs libres : comment sont-ils renseignés (ex : comportent-t-il des informations relatives à la santé, à la religion, les opinions politiques) ?
Les fichiers GED : comportent-ils des données personnelles ?

3.4. Avertissements fournis par l'auditeur

- Une personne ayant pour identifiant "admin" et mot de passe "admin" existe dans la base
- Nombre de personnes ayant accès en consultation à la table des personnes
- Nombre de personnes ayant accès en saisie / modification à la table des personnes
- Nombre de personnes n'ayant pas signé le formulaire de confidentialité
- Aucune règle de construction de mot de passe n'est en place
- Aucun délai de déconnexion en cas d'inactivité
- L'envoi d'un mot de passe par messagerie n'est pas recommandé
- Une longueur minimale de 8 pour les mots de passe est recommandée
- Aucun délai de validité des mots de passe n'est déterminé
- Aucun superviseur n'est désigné
- Mentions légales complémentaires du site non renseignées
- Nombre de personnes enregistrées sans adresse email
- Les connexions au serveur web ne sont pas sécurisées (TLS/SSL)
- Nombre d'historiques d'emprunts de plus d'un an non pseudonymisés
- Nombre de logs de plus d'un an non pseudonymisés
- Liste des personnes dont le mot de passe présente une anomalie.
    - Personne sans mot de passe ;
    - Personne ayant un mot de passe non conforme.

4. Acceptation des conditions générales

Kentika - RGPD permet de suivre l'acceptation des conditions générales d'accès au portail et permettant de bénéficier des services proposés par la base documentaire.

4.1. Signature manuelle

Pour les responsables des traitements sur les données personnelles : il est recommandé de recueillir une signature formelle de leur part. Pour cela, il suffit d'imprimer le formulaire (voir ci-dessus).

4.2. Acceptation électronique

Lorsqu'un utilisateur demande à visualiser les "Mentions légales", une page présentant les conditions générales est affichée.

4.3. Les conditions générales

Une page listant les conditions générales est incluse dans le kit RGPD (RGPD_infoslegales.htm).

Ces conditions sont complétées automatiquement à partir du paramétrage de la base. Des conditions complémentaires peuvent être ajoutées.

4.3.1. Bibliothéconomie

Si le module est installé, une section spécifique aux emprunts, revues et demandes d'achat est incluse.

5. Pseudonymisation des historiques

Le droit à l'oubli provoque de fait une pseudonymisation de l'historique de la personne.
Le log des actions et l'historique des emprunts est également automatiquement pseudonymisé passé un délai de six mois. Ce délai peut être modifié. Les actions pseudonymisées sont celles qui concernent les recherches et consultations.

5.1. Pseudonymisation versus suppression

Kentika comporte un automate de suppression sélective des logs passé un certain délai. Il est conseillé de conserver les logs pendant un an afin de répondre à une éventuelle réquisition judiciaire ou administrative. Pendant la période de pseudonymisation, la personne à l'origine d'une action ne sera plus identifiable sans outil spécifique. Les logs seront cependant toujours exploitables à des fins de statistiques.

5.2. Pseudonymisation versus anonymisation

Une anonymisation interdit tout lien possible entre une information donnée (exemple : un log) et la personne qui en était à l'origine. Un pseudonyme autorise des traitements statistiques par le logiciel.

6. Processus de conformité

La conformité est un processus permanent. La mise en place également. En effet, s'il est difficilement envisageable d'être 100 % conforme dès le premier jour, il est important d'entreprendre les actions qui vont permettre d'y tendre progressivement. L'Auditeur (cf. ci-dessus) vous assistera dans toute la première phase, et au-delà.

6.1. Elaboration du registre des traitements

6.1.1. Le registre automatique

Les traitements génériques du logiciel sont clairement identifiés. Une fonction permet d'obtenir, pour chacun d'eux :

- l'intitulé ;
- la description ;
- les personnes autorisées à les exécuter ;
- les données mises en jeu.

Toute personne autorisée figure sur le registre. En cas d'erreur d'affectation, il est suggéré de corriger l'erreur puis de redemander le calcul du registre.
Le registre ne fonctionne pas en "annule et remplace" mais en versions successives que vous devez conserver. Lorsque de nouvelles personnes intègre l'équipe, que

des interventions sont réalisées sur les autorisations, que des traitements nouveaux sont identifiés : une nouvelle version du registre doit être élaborée.

6.1.2. Traitements identifiés

Kentika est en mesure d'identifier quels sont les traitements potentiellement effectués.

- Maintenance de la table des personnes : les gestionnaires ayant accès en saisie et modification des personnes.
- Préparation et envoi des produits presse : si le module KPress est installé
- Diffusion sélective des informations : les personnes ayant l'autorisation "DSI" et si des centres d'intérêt sont déclarés.
- Emprunts, retours et réservations : les personnes ayant l'autorisation "emprunt, saisie des opérations" et si le module de bibliothéconomie est installé.
- Relance des emprunteurs en retard : les personnes ayant l'autorisation "emprunt, relance" et si le module de bibliothéconomie est installé.
- Circulation des revues : les personnes ayant l'autorisation "réception des numéros" et si des listes de circulation existent.
- Prévenir des destinataires de commande : les personnes ayant l'autorisation "saisie des livraisons" et si des demandes d'achat ont été enregistrées avec un destinataire.

Il se peut que d'autres traitements soient effectués sur les données personnelles gérées dans Kentika. Il appartient alors à l'administrateur de les définir et de les documenter.

6.1.3. Registre sous-traitant

Si des traitements sont confiés à un sous-traitant, un registre dédié doit alors être tenu (ce cas est très rare en ce qui concerne Kentika).

6.1.4. Registre des notifications de violations de données personnelles

Le logiciel gère de manière stricte les accès aux informations de manière générale. Il ne peut cependant pas décider s'il est légitime que telle ou telle personne a bien un accès à la table des personnes. Il vous appartient donc d'établir si, par erreur, un tel accès aurait été fourni à une personne qui aurait pu se montrer indélicate et de le mentionner dans le registre des notifications de violations, réelles ou potentielles.