- RGPD & KinTPV -

Version	Date	Auteur	Objet
1	13/06/18	BBA	Création du document

Ce document explique comment KinTPV répond techniquement aux exigences de la RGPD.

ATTENTION, ce document ne se substitue pas aux différentes démarches que vous devez effectuer.
Entres autres :

- nommer un responsable de traitement,
- lister les utilisations des données personnelles (registre des activités),
- mettre en place une procédure de demande de consentement,
- ...

Liens vers des documents de la cnil :

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

TABLE DES MATIERES :

Informations relevant des données personnelles

Dans la fiche d'un client :

- la photo
- le titre
- la civilité
- le nom
- le prénom
- les lignes d'adresses
- la date de naissance
- l'email
- le site web
- le fax
- les téléphones
- l'information libre
- le commentaire
- l'empreinte de la Carte Bancaire

Dans les adresses de livraison :

- le libellé
- la civilité
- le nom
- le prénom
- la société
- les lignes d'adresses
- le téléphone
- le code porte

Dans les destinataires de mailing papier ou emailing :

- la civilité
- le titre
- le nom
- le prénom
- l'email
- les lignes d'adresses

Dans la blacklist emailing :

- l'email

Dans un ticket de caisse :

les informations de livraison

- la civilité
- le nom
- le prénom
- la société
- les lignes d'adresses
- le téléphone
- le code porte
- information

les informations de billetterie / abonnement / ...

- le nom du caissier
- le nom du vendeur

- le nom du client
- la photo du client

Dans les ventes externes (ecommerce,...) :

les informations du client
- le code client
- le numéro du client
- la civilité
- le nom
- le prénom
- les lignes d'adresses
- la date de naissance
- l'email
- les téléphones

les informations de livraison
- le libellé
- le nom
- le prénom
- les lignes d'adresses
- les téléphones
- le code porte
- le complément d'information

Informations sensibles sécurisées

Sécurisé par CRYPTAGE :
Données qui doivent être relues par une personne autorisée et qui possède la clé de décryptage.

- CLIENT.EmpreinteNum
- CLIENT.EmpreinteCode
- CLIENT.EmpreinteDate

Gestions utilisant les données personnelles

Gestion dans le logiciel KinTPV :

- Carte d'abonnement
- Fidélité client
- Offre promotionnelle selon la date d'anniversaire
- Mailing / eMailing
- Livraison d'article au client
- Contacter le client suite à une commande fournisseur spécifique
- Facturation client
- Statistique de vente par client
- Import des clients
- Export des clients (liste, vente, ...)
- Impression des clients (liste, vente, grand livre, …)
- Gestion des utilisateurs (administrateur, gestionnaire, caissier, vendeur)

FLUX en sortie :

- Vers AppMobile (location et panier d'article)
- Vers site eCommerce
- Vers dossier FTP
- Vers le cloud
- Par WebService
- Par Mail (gestion Multi-magasins)
- Vers dossier distant (gestion Multi-magasins)
- Par réseau local client/serveur (gestion Multi-postes)

FLUX en entrée :

- Depuis site eCommerce
- Depuis le cloud
- Par Mail (gestion Multi-magasins)
- Depuis dossier distant (gestion Multi-magasins)
- Par réseau local client/serveur (gestion Multi-postes)

Consentements des clients

Dans la fiche de chaque client le consentement se fait par cochage des cases.

Autorise d'être contacté par :

- Mailing papier + date
- eMailing + date
- SMS + date
- Téléphone + date

Anonymisation des données

Le logiciel KinTPV permet d'effectuer différentes statistiques pour aider le commerçant dans la prise de décisions.

Pour ne pas perdre certaines statistiques les clients seront anonymisés, c'est à dire qu'il ne sera pas possible de remonter jusqu'à la personne physique avec les données conservées dans le logiciel.

Lien vers les documents de la cnil pour avoir les préconisations de temps avant anonymisation :

https://www.cnil.fr/fr/limiter-la-conservation-des-donnees
https://www.cnil.fr/fr/le-paiement-distance-par-carte-bancaire

- 30 jours : photo
- 13 mois : redemander le consentement.
- 36 mois (3ans) : prospect inactif.
- 60 mois (5ans) : relation contractuelle.
- tps de transac. : empreinte CB et autres données sensibles.

Données concernées :

Chaque donnée concernée sera (H)achée ou (V)idée ou (S)upprimée

- (S) Photo
- (H) Nom
- (H) Prénom
- (H) eMail
- (V) Titre
- (V) Civilité
- (V) Les lignes d'adresses
- (V) N° de compte comptable
- (V) Date de naissance
- (V) Les n° de téléphone
- (V) Libellé d'adresse de livraison
- (V) Complément de livraison
- (V) Code porte pour la livraison
- (V) Empreinte CB

Règles de recherche des données obsolètes pour les clients :

Principe :

- Client contractuel (achat, loc, …): 60 mois.
- Client inactif ..... : 36 mois.
- Empreinte de carte bancaire ..... : début de mois suivant (date règlement).
- Code porte et complément ..... : début de mois suivant (date livraison).
- Photo client ..... : début de mois suivant (date prise +30jrs).

Définition d'un client inactif :

Que le client n'ait pas répondu aux sollicitations, au moins par un devis.
Car la finalité est que le client fasse au moins un devis.

Gestion :

Mettre une date de prévision d'anonymisation (DatePrevueAno) dans la fiche client qui est remise à jour selon les actions du client :

/! = Toujours garder la date la plus lointaine dans la date de prévision d'anonymisation.

- Création du client : Date de création + 36 mois => DatePrevueAno
- Devis .....: Date du devis + 36 mois => DatePrevueAno **/!**
- Clic consentement : Date de consentement + 36 mois => DatePrevueAno **/!**
- Achat .....: Date d'achat + 60 mois => DatePrevueAno
- Location .....: Date fin de location + 60 mois => DatePrevueAno

Procédure automatique de recherche des données obsolètes :

1 fois par mois lors de l'ouverture du logiciel.
Affichage du rapport des anonymisations à faire avec demande de confirmation.

Droit à l'oubli

Le droit à l'oubli permet au client d'être "supprimé", dans notre cas devenir anonyme, dans le logiciel.

La demande doit être effectuée par le client, alors le responsable lancera la procédure d'anonymisation pour ce client.

Droit à la portabilité des données

Le droit à la portabilité des données permet au client de recevoir un fichier
dans un format structuré des données personnelles se trouvant dans le logiciel.

La demande doit être effectuée par le client, alors le responsable lancera la procédure
de portabilité des données pour ce client.

Accès aux données personnelles des clients

Les écrans :

- la gestion clients : recherche, visualisation, création, modification
- la caisse : recherche, visualisation, création, modification
- les tickets : recherche, visualisation, création, modification
- les devis : recherche, visualisation, création, modification
- les locations : recherche, visualisation, création, modification
- les Résa/Cmd/Fab : visualisation
- les ventes eCommerce : visualisation
- les articles : statistiques

Autorisations pour les utilisateurs :

Visualisation de l'empreinte CB :

Demande de l'utilisateur, du mot de passe et de la clé de cryptage.

Caisse/Devis/Location/Ticket :

Modification de la fiche d'un client.

Gestion des clients :

Accéder à la liste des clients.
Accéder à la fiche d'un client.
Accéder aux fonctionnalités (Par lot, Fusionner, exporter, …)
Ajouter et supprimer des clients.

Traçabilité :

https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents

Gestion d'un "Log"

- Gérer un accès aux logs seulement en mode visualisation aux utilisateurs autorisés.
- Sur 6 mois glissants (1 fichier par jour)
- LOG : Requêtes non abouties (HTTP) ou rejetées (SQL, Web, 4D Mobile).
- LOG : Accès utilisateurs aux données personnelles des clients (id, nom, prenom, horodatage, action).

Sécurité des connexions au logiciel

Pour éviter les connexions non prévues à la base de données on rejette par défaut les requêtes entrantes :

- Sur authentification SQL
- Sur authentification Web
- Sur authentification 4D Mobile

Connexion HTTP :

Lors d'une connexion autorisée par requête HTTP (WebService ou AppMobile), la requête est sécurisée par vérification de l'IP de connexion et vérification de l'URI de la requête.

Il n'est donc pas possible d'executer une requête HTTP dans le logiciel si :

- l'IP du demandeur n'est pas autorisée dans le logiciel.
- la requête n'est pas définie dans le logiciel.