SERENITICY

~

RGPD

Version 1.00

Jeudi 31 Mai 2018

SERENICITY
54 boulevard Thiers BP 80072 F-42002 Saint-Etienne Cedex 1
http://www.serenicity.fr contact@serenicity.fr

TABLE DES MATIERES

INTRODUCTION

Ce document présente les processus de protection de données à caractère personnel conformément au Règlement Général sur la Protection des Données (RGPD) mis en place dans notre société.

Ce chapitre présente un résumé du règlement divisé en cinq parties.

Quoi ?

Le règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
On définit par donnée à caractère personnel, toute information se rapportant à une personne physique identifiée ou identifiable. Cela concerne tous les interlocuteurs d'une entreprise qu'il s'agisse de ses salariés, clients ou encore partenaires et fournisseurs.
Certaines données personnelles ont un statut particulier : les données sensibles qui sont par principe interdites de traitement sauf exceptions prévues par le règlement. Il s'agit des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, des données génétiques, biométriques, ou encore celles concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Le traitement d'une donnée à caractère personnel est l'ensemble des opérations ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés sur la donnée (collecte, enregistrement, organisation, structuration, conservation, modification, communication… jusqu'à sa destruction).
Un traitement est licite dès lors qu'il répond à au moins une condition de l'article 6 du règlement: consentement de la personne physique, nécessité à l'application d'un contrat auquel la personne a souscrit, obligation légale, intérêts vitaux de la personne concernée ou d'une autre personne physique, nécessité d'ordre public.

Quand ?

Après de longs mois de discussions et d'amendements, le texte a finalement été adopté le 14 avril 2016. Il remplacera en France la Loi Informatique et Libertés à compter du 25 mai 2018, sans passer par une transposition nationale. Néanmoins, des décrets définiront les points laissés à l'appréciation de chaque pays membre.

Comment ?

La mise en conformité passe par la mise en place de mesures organisationnelles et techniques. Le règlement rappelle l'importance des certifications notamment dans le choix des sous-traitants. Le responsable de traitement a la possibilité de se faire aider par l'autorité locale qui explicitera les bonnes pratiques en fonction de son secteur d'activité. Si la nomination d'un DPD (Délégué à la Protection des données), qui remplacera la fonction du CIL actuel (Correspondant Informatique et Libertés), est encouragée, elle est obligatoire pour certaines organisations :

- les autorités ou les organismes publics ;
- les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;

- les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Son rôle est de centraliser et de coordonner en interne la gestion des traitements, notamment par de la sensibilisation. Il sera également le point de contact avec l'autorité locale pour remplir les formalités et coopérer en cas d'audit ou de litige.

Qui ?

Les entreprises et les administrations, ainsi que leurs sous-traitants, effectuant un traitement de données à caractère personnel relatives à des ressortissants de l'Union européenne. La nouveauté du RGPD réside dans une responsabilisation accrue des sous-traitants, avec qui la responsabilité peut être partagée par voie contractuelle avec la notion de cotraitance.

Où ?

La territorialité s'étend désormais à l'international : les entreprises, responsables de traitement ou sous-traitants, hors de l'Union européenne sont concernées dès lors que le traitement s'applique à l'offre de biens ou de services s'adressant à des personnes dans l'U.E. ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'U.E.

En cas de traitement transfrontalier, le responsable de traitement peut définir quelle sera l'autorité locale référente (la CNIL en France) qui coopérera avec les autres autorités européennes. Cette notion de « guichet unique » s'adresse aussi aux personnes physiques qui souhaitent effectuer des réclamations : elles pourront passer par l'autorité locale de leur pays.

Les chapitres de ce document suivent le plan en six étapes définis par la CNIL (https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes).

Le tableau suivant défini plusieurs termes utilisés dans les chapitres de ce document.

TERME	**DEFINITION**
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

TERME	DEFINITION
Traitement	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.
Personne concernée	Toute personne qui peut être identifiée, directement ou indirectement, par le biais d'un identifiant (par exemple, un nom, un numéro d'identification ou des données de localisation) ou d'un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. En d'autres termes, une personne concernée est un utilisateur final dont les données à caractère personnel peuvent être recueillies.
Responsable du traitement	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.
Sous-traitant	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Autorité de protection des données	Une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51. En France, cette autorité est la CNIL.

CHAPITRE 1 : DESIGNER UN RESPONSABLE DU TRAITEMENT DES DONNEES

Pour piloter la gouvernance des données personnelles de notre société, nous avons décidé de nommé un responsable du traitement de données.

Ce responsable exerce une mission d'information, de conseil et de contrôle en interne. Il est référent et responsable du traitement des données à caractère personnel. Il tient et rend accessible un registre et est garant des obligations liées à la loi. Il assure la sécurité informatique et simplifie les formalités auprès de la CNIL.

Il informe les responsables de traitement et les sous-traitants.

Il a l'appui total de la direction de notre entreprise pour mener à bien ses missions.

Voici les coordonnées du responsable du traitement des données de notre société :

Thierry Veyre

Directeur général

rgpd@serenitycy.fr

CHAPITRE 2 : CARTOGRAPHIER

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que nous traitons, notre société a recensé de façon précise les traitements de données personnelles. Nous avons élaboré un registre des traitements répondant aux questions suivantes.

Qui ?

Le registre contient le nom et les coordonnées du responsable du traitement (et de son représentant légal).
Les responsables des services opérationnels traitant les données au sein de notre société sont identifiés.
La liste des sous-traitants est établie.

Quoi ?

Les catégories de données traitées sont identifiées.
Les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé ou les infractions) sont identifiées.

Pourquoi ?

La ou les finalités pour lesquelles nous collectons ou traitons des données (exemple : gestion de la relation commerciale, gestion RH…) sont identifiées.

Où ?

Le lieu où les données sont hébergées sont définis.
Les pays où les données sont éventuellement transférées sont identifiés.

Jusqu'à quand ?

Pour chaque catégorie de données, le temps de conservation des données est défini.

Comment ?

Les mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées sont en place.

Nous avons décidé de mettre en forme l'ensemble de ces informations dans un registre construit à partir du modèle de registre du règlement européen mis à la disposition par la CNIL :
https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

Liste des traitements de notre registre

Identification du traitement				**Acteurs**	**Finalité du traitement**	**Transfert hors UE ?**	**Données sensibles ?**
Nom	Référence	Date de création	Date de dernière mise à jour	Responsable du traitement	Finalité principale	Oui/Non	Oui/Non
Gérer les processus commerciaux	RGPD-REF0001	31 mai 2018	31 mai 2018	Thierry Veyre	Gérer les processus commerciaux	Non	Non
Gérer le personnel	RGPD-REF0002	31 mai 2018	31 mai 2018	Thierry Veyre	Gérer le personnel	Non	Non

Fiche de registre

Fiche de registre	
Description du traitement	Gérer les processus commerciaux
Nom	Gérer les processus commerciaux
Référence	RGPD-REF-0001
Date de création	31 mai 2018
Date de mise à jour	31 mai 2018
Acteurs	
Responsable du traitement	Thierry Veyre
Finalité(s) du traitement effectué	
Finalité principale	Gérer les processus commerciaux
Sous-finalité 1	Etablir des documents commerciaux à destination des clients de Serenicity(devis, commande, facture, bon de livraison, courrier de relance, …).
Sous-finalité 2	Etablir des documents commerciaux à destination des fournisseurs et des sous-traitants de Serenicity (devis, commande, facture, bon de livraison, courrier de relance, …).
Sous-finalité 3	Envoyer des documents commerciaux à destination des clients de Serenicity (devis, commande, facture, bon de livraison, courrier de relance, …).
Sous-finalité 4	Envoyer des documents commerciaux à destination des fournisseurs et des sous-traitants de Serenicity (devis, commande, facture, bon de livraison, courrier de relance, …).
Sous-finalité 5	Réaliser toutes les tâches courantes d'administration sur les documents commerciaux à destination des clients de Serenicity (relance, règlement, recouvrement, …).
Sous-finalité 6	Réaliser toutes les tâches courantes d'administration sur les documents commerciaux à destination des fournisseurs et des sous-traitants de Serenicity (relance, règlement, recouvrement, …).

Mesures de sécurité		
Mesures de sécurité techniques	Voir chapitre 4.	
Mesures de sécurité organisationnelles	Voir chapitre 4.	
Catégories des données personnelles concernées	**Description**	**Délai d'effacement**
Etat civil, identité, données d'identification, images…	Prénom, nom, adresse de messagerie professionnelle, numéro de téléphone professionnelle	5 ans
Vie personnelle (habitudes de vie, situation familiale, etc.)	/	
Informations d'ordre économique et financier	/	
Données de connexion (adresse IP, logs, etc.)	/	5 ans
Données de localisation (déplacements, données GPS, GSM, etc.)	/	5 ans
Données sensibles	**Description**	**Délai d'effacement**
Données révélant l'origine raciale ou ethnique	/	
Données révélant les opinions politiques	/	
Données révélant les convictions religieuses ou philosophiques	/	
Données révélant l'appartenance syndicale	/	
Données génétiques	/	
Données biométriques aux fins d'identifier une personne physique	/	
Données concernant la santé	/	
Données concernant la vie sexuelle ou l'orientation sexuelle	/	
Données relatives à des condamnations pénales ou infractions	/	
Numéro d'identification national unique (NIR pour la France)	/	

Destinataires	
Destinataire 1	KPMG
Destinataire 2	/
Destinataire 3	/
Destinataire 4	/
Destinataires hors UE	
Destinataire 1	/
Destinataire 2	/
Destinataire 3	/

Fiche de registre	
Description du traitement	Gérer le personnel
Nom	Gérer le personnel
Référence	RGPD-REF-0002
Date de création	31 mai 2018
Date de mise à jour	31 mai 2018
Acteurs	
Responsable du traitement	Thierry Veyre
Finalité(s) du traitement effectué	
Finalité principale	Gérer le personnel
Sous-finalité 1	Tenir le registre du personnel
Sous-finalité 2	Effectuer les déclarations légales inhérentes au contrat de travail
Sous-finalité 3	Editer les bulletins de salaire et les déclarations correspondantes
Sous-finalité 4	Payer les salaires
Sous-finalité 5	Gérer la fin de contrat
Sous-finalité 6	Gérer les institutions et les représentants du personnel (adhésion d'un employé à une représentation syndicale et gestion des élections des représentants du personnel).
Mesures de sécurité	
Mesures de sécurité techniques	Voir chapitre 4.
Mesures de sécurité organisationnelles	Voir chapitre 4.

Catégories des données personnelles concernées	**Description**	**Délai d'effacement**
Etat civil, identité, données d'identification, images…	Prénom, nom, adresse postale personnelle, adresse de messagerie personnelle, date de naissance, lieu de naissance, pays de naissance, numéro de sécurité social, photographie, pièce d'identité, permis de conduire, carte Sesam Vitale	5 ans
Vie personnelle (habitudes de vie, situation familiale, etc.)	Situation familiale, coordonnées de la personne à contacter en cas d'urgence (prénom, nom, numéro de téléphone personnelle)	5 ans
Informations d'ordre économique et financier	Relevé d'identité bancaire	5 ans
Données de connexion (adresse IP, logs, etc.)	/	
Données de localisation (déplacements, données GPS, GSM, etc.)	/	
Données sensibles	**Description**	**Délai d'effacement**
Données révélant l'origine raciale ou ethnique	/	
Données révélant les opinions politiques	/	
Données révélant les convictions religieuses ou philosophiques	/	
Données révélant l'appartenance syndicale	Prénom, nom, étiquette syndicale et fonction. Ces données sont collectées sans traitement à haute fréquence. Nous ne nommons donc pas un délégué à la protection des données (DPD) pour ces données sensibles et nous ne mettons pas en place une analyse d'impact (PIA).	5 ans
Données génétiques	/	
Données biométriques aux fins d'identifier une personne physique	/	
Données concernant la santé	/	
Données concernant la vie sexuelle ou l'orientation sexuelle	/	
Données relatives à des condamnations pénales ou infractions	/	
Numéro d'identification national unique (NIR pour la France)	/	

Destinataires	
Destinataire 1	KPMG
Destinataire 2	/
Destinataire 3	/
Destinataires hors UE	
Destinataire 1	/
Destinataire 2	/
Destinataire 3	/

CHAPITRE 3 : PRIORISER

Sur la base de notre registre, nous avons identifié les actions à mener pour nous conformer aux obligations actuelles et à venir.

Nous collectons seulement les données personnelles strictement nécessaires et nos traitements des données personnelles se fondent sur une base juridique légitime en totale adéquation avec l'activité de notre entreprise.

Ce document est accessible :

Soit sur simple demande à notre responsable du traitement (son adresse de messagerie pour les questions sur le RGPD est présentée ci-dessus).

Soit par téléchargement sur notre site Internet à adresse : http://www.serenicity.fr

Nous avons informé nos sous-traitants de leurs obligations et de leurs responsabilités. Notre responsable du traitement s'est assuré de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées. La traçabilité des données personnelles confiées à nos sous-traitants est opérationnelle.

Les modalités d'exercice des droits des personnes concernées sont présentées dans la tableau ci-dessous.

Consentement	Le consentement est obtenu lors de la signature de nos documents commerciaux.
Droit d'accès	Le droit d'accès est activable par la personne concernée sur simple demande à notre responsable du traitement (ses coordonnées sont présentées ci-dessus). Ce droit est possible dans la limite de quatre fois par an.
Droit de rectification	Le droit de rectification des données personnelles est activable par la personne concernée sur simple demande à notre responsable du traitement (ses coordonnées sont présentées ci-dessus).
Droit à la portabilité	Le droit à la portabilité est activable par la personne concernée sur simple demande à notre responsable du traitement (ses coordonnées sont présentées ci-dessus). Les données seront restitués à l'aide d'un fichier informatique type…
Retrait du consentement	Le retrait du consentement est activable par la personne concernée sur simple demande à notre responsable du traitement (ses coordonnées sont présentées ci-dessus).
Droit à l'oubli	Le droit à l'oubli est activable par la personne concernée sur simple demande à notre responsable du traitement (ses coordonnées sont présentées ci-dessus).

NOTA : notre entreprise présente des exemples de formulaire d'exercice des droits des personnes concernées dans le chapitre 6.

La sécurité de notre système d'information repose une politique de sécurité du système d'information (PSSI) qui inclut, entre autres, les mesures de sécurité mises en place pour la protection des données à caractère personnel. Elle comporte les mesures suivantes :

- Authentification de nos utilisateurs avec des mots de passe complexes via un protocole hautement sécurisé bloquant automatiquement les sessions après plusieurs tentatives infructueuses de connexion. Nos utilisateurs ne sont pas administrateurs de leurs sessions.
- Définition des droits d'accès pour l'accès aux données et aux applications par appartenance des utilisateurs à des groupes de sécurité.
- Antivirus, pare feu et bouclier intelligent supervisés.
- Installation des correctifs de sécurité à jour et automatisation des tâches courantes d'administration.
- Sauvegarde supervisée complétée par un plan de reprise d'activité.
- Les unités de disque de nos ordinateurs sont chiffrées par la solution Microsoft bitlocker.
- …

La durée de conservation des données à caractère personnel est de 5 ans.

CHAPITRE 4 : GERER LES RISQUES

Nous n'avons pas identifié de traitement de données personnelles susceptibles d'engendrer des risques élevés pour les droits et les libertés des personnes concernées.

Si un nouveau traitement devait être mis en place alors nous avons prévu de mener une analyse d'impact sur la protection des données (PIA).

Ce PIA permettra de créer un traitement conforme au RGPD et respectueux de la vie privée. Il sera réalisé avant la mise en œuvre du traitement et sera basé sur un processus itératif. Des analyses régulières permettront de corriger le traitement notamment lors de changements majeurs de ses modalités.

Ce PIA respectera les 9 critères suivant :

- Evaluation ou notation.
- Décision automatisée avec effet juridique ou effet similaire significatif.
- Surveillance systématique.
- Données sensibles ou données à caractère hautement personnel.
- Données personnelles traitées à grande échelle.
- Croisement d'ensembles de données.
- Données concernant des personnes vulnérables.
- Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles.
- Exclusion du bénéfice d'un droit, d'un service ou de contrat.

CHAPITRE 5 : ORGANISER

Nous avons mis en place les procédures internes suivantes pour prendre en compte la protection des données à tout moment.

PROCEDURE	DETAIL DE LA PROCEDURE
Anticiper les violations de données	En cas de violation de données personnelles sous notre responsabilité, notre responsable du traitement fera une notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais. Cette notification sera faite à l'aide du « formulaire de notification de violation de données personnelles » (https://www.cnil.fr/fr/organiser-les-processusinternes).
Prendre en compte la protection des données personnelles dès la conception	La protection des données personnelles dès la conception d'une application ou d'un traitement est systématiquement prise en compte dans notre entreprise. Ce processus est géré par notre responsable du traitement. Chaque nouveau traitement est étudié et renseigné dans notre registre. Si un traitement traite des données sensibles alors un PIA est mis en place. NOTA : les données inutiles ont été supprimés de nos traitements.
Gérer les demandes des personnes concernées	Les demandes suivantes sont traitées par notre responsable du traitement : - Demande de droit d'accès. - Demande de rectification. - Demande de droit à la portabilité. - Demande de retrait du consentement. - Droit de droit à l'oubli. Ces demandes et les réponses apportées sont faites par voie électronique.
Gérer le changement de sous-traitant	En cas de changement de sous-traitant, notre responsable du traitement s'assure que le nouveau sous-traitant est en conformité avec le RGPD. Si ce sous-traitant remplace un autre, notre responsable du traitement s'assure que ce dernier détruira la totalité des données personnelles en sa possession.

Sensibiliser les collaborateurs	Une sensibilisation sur la protection des données personnelles à destination de l'ensemble des collaborateurs de notre entreprise est faite par notre responsable du traitement des données une fois par trimestre par voie électronique.

CHAPITRE 6 : DOCUMENTER

L'ensemble de la documentation de la mise en conformité de notre entreprise au RGPD est présente dans ce document qui est révisé annuellement. Le chapitre « VERSION DU DOCUMENT » présente un tableau résumant les numéros de version, les dates et commentaires correspondants et l'auteur de la modification.

Les commandes des sous-traitants concernés par le RGPD sont stockés dans l'ERP Clipper. Les conditions générales d'achat de notre société s'appliquent systématiquement.

Exemples de formulaire d'exercice des droits des personnes concernées :

Consentement	Par la présente, Je, Prénom Nom fonction (au sein de l'entreprise), accepte que la société, - nom de l'entreprise -, collecte mes données personnelles – nommer les données – pour les traitements – nommer les traitements – ayant comme finalité – nommer les finalités -.
Droit d'accès	Par la présente Je, Prénom Nom fonction (au sein de l'entreprise), demande que la société, - nom de l'entreprise -, me fournisse l'intégralité des données personnelles qui me concernent dans une copie d'un fichier structuré, couramment utilisé et lisible par machine.
Droit de rectification	Par la présente Je, Prénom Nom fonction (au sein de l'entreprise), demande que la société, - nom de l'entreprise -, - rectifie, complète, actualise, verrouille ou efface – mes données personnelles ci-dessous : - - lister les données personnelles - Je vous remercie de me faire parvenir une copie des données ainsi modifiées.
Droit à la portabilité	Par la présente Je, Prénom Nom fonction (au sein de l'entreprise), demande à la société, - nom de l'entreprise -, de recevoir mes données à caractère personnel dans un fichier structuré, couramment utilisé et lisible par machine, et de les transmettre au responsable de traitement de - nom de l'entreprise – sans y faire obstacle.
Retrait du consentement	Par la présente Je, Prénom Nom fonction (au sein de l'entreprise), retire mon consentement à la société, - nom de l'entreprise -, de traiter mes données personnelles.
Droit à l'oublie	Par la présente Je, Prénom Nom fonction (au sein de l'entreprise), demande à la société, - nom de l'entreprise -, de supprimer mes données personnelles de tous ses traitements informatiques.

REFERENCES

https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

https://www.designations.cnil.fr/designations/designation/designation.new.action

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

https://www.cnil.fr/fr/documenter-la-conformite

VERSION DU DOCUMENT

Numéro	Date	Commentaire	Auteur
1.00	31 mai 2018	Création du document	TV