DOSSIER DE CONFORMITÉ RGPD ET SÉCURITÉ DES SYSTÈMES D'INFORMATION

I. TRAITEMENT « SÉCURITÉ DES SYSTÈMES D'INFORMATION »

1. Identification du traitement

Responsable de traitement : La Cité d'Or

Intitulé du traitement : Sécurité des systèmes d'information

Finalité principale : assurer la sécurité, l'intégrité, la disponibilité et la confidentialité des systèmes d'information et des données traitées.

2. Finalités du traitement

Le traitement poursuit les finalités suivantes :

- prévention des intrusions et accès non autorisés ;
- détection des comportements anormaux ou frauduleux ;
- surveillance et sécurisation des systèmes informatiques ;
- protection des données à caractère personnel ;
- gestion des incidents de sécurité ;
- traçabilité des accès et actions effectuées sur les systèmes ;
- maintien de la disponibilité des services numériques.

3. Base légale

Le traitement est fondé sur l'intérêt légitime du responsable de traitement conformément à l'article 6 §1 f) du Règlement (UE) 2016/679.

Le responsable de traitement considère, après mise en balance des intérêts en présence, que ce traitement est nécessaire à la sécurisation des systèmes d'information et ne porte pas une atteinte disproportionnée aux droits et libertés des personnes concernées.

4. Catégories de données traitées

Les données traitées sont strictement limitées à ce qui est nécessaire à la sécurité des systèmes :

- adresses IP ;
- identifiants techniques ;
- journaux de connexion ;
- journaux d'activité ;
- horodatage des opérations ;

- informations relatives aux incidents techniques ;
- données de sécurité et de supervision.

Aucune donnée relevant des catégories particulières de données visées à l'article 9 du RGPD n'est collectée dans le cadre de ce traitement.

5. Catégories de personnes concernées

- utilisateurs du site internet ;
- salariés et collaborateurs habilités ;
- administrateurs système ;
- prestataires techniques autorisés.

6. Destinataires

Les données sont accessibles uniquement :
- aux personnes habilitées en charge de l'administration des systèmes ;
- aux prestataires techniques agissant en qualité de sous-traitants ;
- aux autorités légalement habilitées lorsque la réglementation l'impose.

L'accès est limité selon le principe du moindre privilège.

7. Durées de conservation

Les données sont conservées pour une durée adaptée aux finalités poursuivies :
- journaux techniques : six mois maximum ;
- données relatives à un incident de sécurité : douze mois maximum lorsque leur conservation est nécessaire à l'analyse ou à la gestion de l'incident.

À l'issue de ces délais, les données sont supprimées ou anonymisées.

8. Mesures de sécurité

Le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées comprenant notamment :
- journalisation des accès ;
- gestion des habilitations ;
- restriction des accès aux données ;
- chiffrement des flux ;
- sauvegardes régulières ;
- surveillance des systèmes ;
- mécanismes d'alerte et de détection des incidents.

9. Transferts internationaux

Aucun transfert de données hors de l'Union européenne n'est réalisé dans le cadre de ce traitement, sauf mise en œuvre de garanties appropriées conformément aux dispositions du RGPD.

II. PROCÉDURE D'EXERCICE DES DROITS DES PERSONNES CONCERNÉES

1. Réception des demandes

Toute demande d'exercice des droits prévus par le RGPD est reçue par courrier, courrier électronique ou tout autre canal officiellement mis à disposition des personnes concernées. Chaque demande fait l'objet d'un enregistrement permettant d'assurer sa traçabilité.

2. Accusé de réception

Un accusé de réception est adressé au demandeur dans les meilleurs délais lorsque cela apparaît nécessaire.

3. Vérification de l'identité

Le responsable de traitement procède aux vérifications nécessaires afin de s'assurer de l'identité du demandeur.
En cas de doute raisonnable, un justificatif d'identité peut être sollicité.

4. Analyse de la demande

La demande est examinée afin :
- d'identifier le droit invoqué ;
- de vérifier sa recevabilité ;
- de déterminer les traitements concernés ;
- d'identifier les données à traiter.

5. Mise en œuvre

Le responsable de traitement procède, selon le cas :
- à la communication des données ;
- à leur rectification ;
- à leur effacement ;
- à la limitation du traitement ;
- à l'opposition au traitement ;
- à leur portabilité lorsque ce droit est applicable.

L'ensemble des opérations réalisées est documenté.

6. Délais de traitement

Conformément à l'article 12 du RGPD :

- délai de réponse : un mois maximum ;
- prolongation possible de deux mois supplémentaires en cas de demande complexe ou multiple.

Toute prolongation est motivée et portée à la connaissance du demandeur.

7. Réponse

La réponse adressée à la personne concernée est rédigée de manière claire, compréhensible et juridiquement motivée.

Elle précise, le cas échéant :
- les actions réalisées ;
- les données concernées ;
- les voies de recours disponibles.

8. Archivage

Les demandes et les réponses apportées sont conservées à titre de preuve de conformité pendant une durée adaptée aux obligations légales applicables.

III. PROCÉDURE DE GESTION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

1. Détection et signalement

Tout incident susceptible d'affecter la confidentialité, l'intégrité ou la disponibilité des données à caractère personnel est immédiatement signalé au responsable de traitement.
Chaque incident fait l'objet d'un enregistrement dans un registre dédié.

2. Qualification

Une analyse est réalisée afin de déterminer :
- la nature de l'incident ;
- les catégories de données concernées ;
- le nombre approximatif de personnes impactées ;
- les conséquences potentielles de l'incident.

3. Mesures immédiates

Les mesures nécessaires sont prises sans délai afin :
- de contenir l'incident ;
- de corriger la faille identifiée ;
- de limiter les conséquences potentielles ;
- de rétablir la sécurité des systèmes.

4. Évaluation du risque

Le responsable de traitement évalue le niveau de risque présenté pour les droits et libertés des personnes concernées en tenant compte notamment :

- de la nature des données ;
- du volume des données concernées ;
- de la sensibilité des informations ;
- de la probabilité et de la gravité des conséquences.

5. Notification à la CNIL

Lorsqu'une violation est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, une notification est adressée à la CNIL dans les meilleurs délais et, si possible, dans les soixante-douze heures suivant sa découverte, conformément à l'article 33 du RGPD.

6. Information des personnes concernées

Lorsqu'une violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, celles-ci sont informées dans les conditions prévues à l'article 34 du RGPD.

7. Registre des violations

Le responsable de traitement documente toute violation de données à caractère personnel, y compris lorsque celle-ci ne donne lieu à aucune notification.

Le registre comporte notamment :

- la date de l'incident ;
- sa description ;
- les conséquences constatées ;
- les mesures correctives mises en œuvre ;
- les décisions prises.

8. Mesures postérieures à l'incident

À l'issue de chaque incident significatif, une analyse est réalisée afin :

- d'identifier les causes de l'incident ;
- d'améliorer les mesures de sécurité existantes ;
- de prévenir la réitération d'incidents similaires ;
- d'actualiser les procédures internes lorsque cela est nécessaire.