CHARTE INFORMATIQUE ET POLITIQUE DE CONFIDENTIALITÉ DE LA COMMUNAUTÉ DE COMMUNES ET DU CIAS DU PAYS DE CRAON

Table des matières

PARTIE 1 : APPLICATION ET MISE EN PLACE DE LA CHARTE INFORMATIQUE

1. Date d'entrée en vigueur

La présente charte informatique et politique de confidentialité est établie après consultation du Comité Social Territorial en date du 22/04/2025 est affiché au Centre Administratif Intercommunal (service informatique) et est disponible sur le serveur commun.

La présente charte est approuvée par le Conseil Communautaire en date du 28/04/2025 et le Conseil d'Administration en date du 14/05/2025.

Elle entrera en vigueur le 15/05/2025.

2. Modification

Toute modification ultérieure ou tout retrait sera soumis à l'avis du Comité Social Territorial et à la validation du Conseil Communautaire et du Conseil d'Administration.

Validation du Président le :

PARTIE 2 : INTRODUCTION

Le CIAS et la Communauté de Communes du Pays de Craon mettent en œuvre un système d'information et de communication nécessaire à l'exercice de son activité. Ces collectivités mettent ainsi à disposition de ses agents des outils informatiques et de communication.

La présente charte d'utilisation des ressources informatiques définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication du CIAS et de la Communauté de Communes du Pays de Craon. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet entraîner des conséquences graves de nature à engager sa responsabilité civile et / ou pénale ainsi que celle de nos collectivités.

1. Protection des données à caractère personnel

La loi n°78-17 du 6 janvier 1978 (modifiée) et la législation européenne RGPD définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elles ouvrent aux personnes concernées par les traitements des droits : opposition, accès, rectification, effacement, limitation et portabilité des données personnelles enregistrées sur leur compte.

Le CIAS et la Communauté de Communes du Pays de Craon ont désigné officiellement un délégué à la protection des données à caractère personnel qui peut être contacté via le secrétariat général. La Direction Générale des Services et la Direction du CIAS du Pays de Craon (délégué-e à la protection de données) assurent conjointement les missions liées à la protection des données personnelles et ont pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 (modifiée) et de la législation européenne RGPD. Dans ce cadre, la Direction Générale des Services et la Direction du CIAS du Pays de Craon doivent obligatoirement être consultées pour validation avant toute prise de décision et toute action concernant des données personnelles recueillies, manipulées ou stockées.

La Direction Générale des Services et la Direction du CIAS du Pays de Craon recensent dans un registre la liste de l'ensemble des traitements de données à caractère personnel au fur et à mesure de leurs mises en œuvre. Cette liste peut être tenue à disposition de tout agent en faisant la demande.

2. Le champ d'application de la charte

La présente charte s'applique à tout utilisateur du Système d'Information et de communication du CIAS et de la Communauté de Communes du Pays de Craon pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils n'est pas tolérée. La charte est diffusée à l'ensemble des utilisateurs par note de service. Elle est systématiquement remise pour signature à tout nouvel arrivant. Des actions de communication internes sont organisées régulièrement afin d'informer les utilisateurs des pratiques recommandées.

3. Quelques définitions

On désignera sous le terme « utilisateur » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication du CIAS et de la Communauté de Communes du Pays de Craon et à les utiliser : agents, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels, etc.

Les termes "outils informatiques et de communication" recouvrent tous les équipements informatiques, de télécommunications et de reprographie du CIAS et de la Communauté de Communes du Pays de Craon.

Les règles d'utilisation du système d'information.

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par le service informatique du CIAS et de la Communauté de Communes du Pays de Craon.

PARTIE 3 : LES MODALITES D'INTERVENTION DES ADMINISTRATEURS SYSTEMES INTERNES

Les administrateurs systèmes interne assurent le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication du CIAS et de la Communauté de Communes du Pays de Craon. Les agents de ce service disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Ils ont accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Ils s'engagent à enregistrer les interventions de maintenance dans une main courante informatisée pour aboutir à une traçabilité détaillée des interventions. Ils s'engagent aussi à effacer les données de tout matériel avant sa mise au rebut ou réattribution et à recueillir l'accord de l'utilisateur avant toute intervention sur un poste de travail.

PARTIE 4 : L'AUTHENTIFICATION

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte (« login » ou identifiant) fourni à l'utilisateur lors de son arrivée. Un mot de passe est associé à cet identifiant de connexion. Les moyens d'authentification sont personnels et confidentiels. Nous vous informons qu'une journalisation est ainsi réalisée pour aboutir à la mise en place d'un système de traçabilité systématique.

Tous les mots de passe utilisés doivent être complexes en étant composés de 8 caractères minimum combinant chiffres, minuscules, majuscules et caractères spéciaux. Ils ne doivent comporter ni nom ni prénom ni identifiant d'ouverture. Ils doivent être renouvelés tous les six mois.

Si un outil ou logiciel ne vous oblige pas technologiquement à utiliser un mot de passe complexe, vous vous engagez à choisir tout de même un mot de passe complexe tel que défini dans la présente charte informatique.

PARTIE 5 : LES REGLES DE SECURITE

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique à l'adresse : informatique@paysdecraon.fr toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement.
- Stocker les documents-papiers confidentiels ou contenant des informations personnelles dans des armoires ou des salles d'archive fermées à clé ou par digicode.
- Ne jamais confier son identifiant ou mot de passe.
- Ne jamais demander ou utiliser l'identifiant ou mot de passe d'un collègue (même en son absence).
- Ne jamais utiliser un identifiant ou mot de passe commun à plusieurs collègues ou commun à tout un service (sauf pour les messageries partagées).
- Ne jamais utiliser de mot de passe en rapport avec soi (date de naissance, prénom des enfants, nom de son entreprise, etc.).
- Pour rappel, toujours utiliser des mots de passe complexes de 8 caractères minimum mixant minuscules, majuscules, chiffres et caractères spéciaux même si l'outil utilisé permet l'utilisation d'un mot de passe simple.
- Ne pas masquer sa véritable identité et ne pas usurper l'identité d'autrui.
- Ne pas modifier les paramétrages du poste de travail sans autorisation.
- Ne pas installer de logiciels sans autorisation.
- Ne pas désinstaller ou désactiver les antivirus, anti-malware et firewall installés, ainsi que leurs processus de mise à jour continue.
- Ne pas désinstaller, désactiver ou modifier les procédures de verrouillage automatique de session.
- Ne pas copier, modifier, détruire les logiciels propriétés du CIAS et de la Communauté de Communes du Pays de Craon.
- Verrouiller son ordinateur dès que l'on quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas ou qui ne lui sont pas destinés.
- Demander l'accord de la Direction pour toute copie de données sur un support externe nomade ou potentiellement nomade (ordinateur portable, clés USB, disque dur externe, CD-R, DVD-RW, etc.) et utiliser un chiffrement du disque dur dans sa totalité lorsque le système d'exploitation le propose ou la création de conteneurs (dossiers susceptibles de contenir plusieurs fichiers) spécifiquement chiffrés.

- Le transfert de fichiers vers l'extérieur se fera via l'intermédiaire des outils déployés par le service informatique. En aucun cas il ne faudra utiliser des services tiers.
- Activer les options de chiffrement, verrouillage des sessions et mot de passe complexes de déverrouillage pour les smartphones ou tablettes qui accèdent à des données des collectivités.
- Activer dès que possible la sécurisation des échanges de données dans tous les outils (https, smtps, ftps, vpn ssl, imaps, pops, etc.).
- Dans le cadre de la maintenance, les échantillons de données éventuellement enregistrés doivent être détruits immédiatement après la fin de l'opération de maintenance.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information du CIAS et de la Communauté de Communes du Pays de Craon sans l'accord préalable de la Direction Générales des Services et / ou la Direction du CIAS du Pays de Craon.

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte à leurs propres salariés et éventuellement aussi aux salariés de leurs propres entreprises sous-traitantes. Dès lors, les contrats signés entre le CIAS ou la Communauté de Communes du Pays de Craon et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

PARTIE 6 : LES MOYENS INFORMATIQUES

1. Configuration du poste de travail

Le CIAS et la Communauté de Communes du Pays de Craon mettent à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions.

L'utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle.
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par la Direction.
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade »)
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires (logiciels de consultation de fichiers multimédia) est subordonnée à l'accord de la Direction.

2. Equipements nomades et procédures spécifiques aux matériels de prêt

Equipements nomades

On entend par « équipements nomades » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc…).

Pour rappel, quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker, notamment par cryptage.

L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Pour rappel, quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

Procédures spécifiques aux matériels de prêt

L'utilisateur doit renseigner et signer un registre, tenu par le service informatique et dont une copie figurera dans le dossier individuel de l'agent, actant la remise de l'équipement nomade ou encore la mise à disposition d'un matériel spécifique pour la tenue d'une réunion (vidéoprojecteur par exemple). Il en assure la garde et la responsabilité et doit informer la Direction en cas d'incident (perte, vol, dégradation) afin qu'il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements. Le retour du matériel est consigné dans le registre.

3. Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu'ils soient.

Toutefois, une utilisation pour un motif personnel n'est pas autorisée.

4. Messagerie électronique et instantanée

Conditions d'utilisation

La messagerie (courriel ou instantanée) mise à disposition des utilisateurs est destinée à un usage strictement professionnel. L'utilisation de la messagerie à des fins personnelles n'est pas tolérée.

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

Le CIAS et la Communauté de Communes du Pays de Craon s'interdisent d'accéder aux dossiers et aux messages identifiés comme « personnel » dans l'objet de la messagerie de l'utilisateur.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par la Direction :

- Volumétrie de la messagerie,
- Taille maximale de l'envoi et de la réception d'un message,
- Nombre limité de destinataires simultanés lors de l'envoi d'un message,
- Gestion de l'archivage de la messagerie.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes nomades ou potentiellement nomades.

Les utilisateurs peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (Webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'utilisateur dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

Consultation de la messagerie

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, la Direction peut ponctuellement désigner une personne pour consulter cette boite mail et transmettre un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur.

Le supérieur hiérarchique n'a pas accès aux autres messages de l'agent. L'agent concerné est informé dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée d'un agent (longue maladie par exemple), la direction peut demander le transfert des messages reçus.

Courriel non sollicité

Le CIAS et la Communauté de Communes du Pays de Craon disposent d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

5. Téléphone

Le CIAS et la Communauté de Communes du Pays de Craon mettent à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes ou mobiles.

L'utilisation du téléphone à titre privé n'est pas admise.

Des restrictions d'utilisation des téléphones peuvent être mises en place en tenant compte des missions des utilisateurs. A titre d'exemple, certains postes peuvent être limités aux appels nationaux.

Le CIAS et la Communauté de Communes du Pays de Craon peuvent mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elles permettent de vérifier que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

Le CIAS et la Communauté de Communes du Pays de Craon s'interdisent d'accéder à l'intégralité des numéros appelés. Toutefois, en cas d'utilisation manifestement anormale, la Direction se réserve le droit d'accéder aux numéros complets des relevés individuels.

6. L’utilisation des outils informatiques par les représentants du personnel

Les représentants du personnel utilisent, dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l’exercice de leur activité professionnelle. Ils disposent d’une adresse électronique dédiée et d’une liste de diffusion : representants-personnels@paysdecraon.fr .

Afin de surveiller le fonctionnement et de garantir la sécurité du système d’information, différents dispositifs sont mis en place.

7. Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information du CIAS et de la Communauté de Communes du Pays de Craon et d’assurer la sécurité et la confidentialité des données qui sont mis en œuvre. Il s’agit notamment du filtrage des sites Internet, de l’élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée…).

8. Les systèmes automatiques de traçabilité

Les administrateurs du CIAS et de la Communauté de Communes du Pays de Craon opèrent sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Ils s’appuient pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, identifiants ou adresse IP et objet de l’évènement. Les administrateurs sont les seuls destinataires habilités de ces informations qui sont effacées à l’expiration d’un délai de 12 mois maximum.

La base juridique de la traçabilité opérée est l’intérêt légitime de sécurisation et l’obligation légale de journalisation liée à la législation européenne RGPD qui prévoit de pouvoir détecter les intrusions informatiques éventuelles. Vous pouvez exercer vos droits (accès, rectification, suppression, opposition, limitation et portabilité le cas échéant) en contactant le DPO à l’adresse : dpo@paysdecraon.fr . Vous disposez par ailleurs, du droit d’introduire une réclamation auprès de la Commission Nationale de l’Informatique et des Libertés (CNIL), notamment sur son site internet www.cnil.fr .

9. Gestion du poste de travail

A des fins de maintenance informatique, les administrateurs du CIAS et de la Communauté de Communes du Pays de Craon peuvent accéder à distance à l'ensemble des postes de travail. Pour rappel, cette intervention s'effectue avec l'autorisation de l'utilisateur.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service de maintenance informatique peut être amené à intervenir sur l'environnement technique des postes de travail. Il s'interdit d'accéder aux contenus.

Procédure applicable lors du départ de l'utilisateur

Lors de son départ, l'utilisateur doit restituer à la Direction les matériels mis à sa disposition.

Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par la Direction.

Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ (hors contrainte légale de conservation des données).

Toute donnée professionnelle reste propriété de la Communauté de Communes et du CIAS du Pays de Craon.

PARTIE 7 : RESPONSABILITES ET SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Tout agent qui ne se conformera pas aux dispositions du présent règlement, s'exposera à des sanctions disciplinaires de la part de l'autorité territoriale.

Agents titulaires :

- ✓ 1er groupe : l'avertissement, le blâme, l'exclusion temporaire de fonction pour une durée maximale de trois jours ;
- ✓ 2ème groupe : l'abaissement d'échelon, l'exclusion temporaire de fonction pour une durée maximale de 4 à 15 jours ;
- ✓ 3ème groupe : la rétrogradation, l'exclusion temporaire de fonction pour une durée de 16 jours à 6 mois ;
- ✓ 4ème groupe : la mise à la retraite d'office, la révocation.

La sanction retenue sera en adéquation avec la faute commise et répétitive.

Agents stagiaires :

Liste des sanctions disciplinaires par ordre d'importance :

- ✓ l'avertissement ;
- ✓ le blâme ;
- ✓ l'exclusion temporaire de fonction pour une durée maximale de trois jours ;
- ✓ l'exclusion temporaire de fonction pour une durée maximale de 4 à 15 jours ;
- ✓ l'exclusion définitive du service.

L'autorité ayant le pouvoir disciplinaire choisit parmi les sanctions précitées celle qu'elle estime en rapport avec la gravité des faits reprochés.

Agents contractuels :

- ✓ l'avertissement ;
- ✓ le blâme ;
- ✓ l'exclusion temporaire de fonction pour une durée maximale de trois jours ;

- ✓ l'exclusion temporaire de fonction pour une durée de 4 jours à 6 mois (CDD) ou 4 jours à 1 an (CDI) ;
- ✓ licenciement, sans préavis ni indemnité de licenciement.

L'autorité ayant le pouvoir disciplinaire choisit parmi les sanctions précitées celle qu'elle estime en rapport avec la gravité des faits reprochés.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'informations est susceptible de sanctions pénales prévues par la loi.

PARTIE 8 : DROIT A LA DEFENSE

Quelle que soit la sanction disciplinaire, l'agent dispose d'un délai suffisant pendant lequel il prend connaissance de son dossier individuel et peut organiser sa défense.

Les sanctions appartenant aux 2ème, 3ème ou 4ème groupe nécessitent l'intervention du Conseil de Discipline.

PARTIE 9 : DIFFUSION ET AFFICHAGE

Le règlement formation sera diffusé auprès de l'ensemble des agents pour qu'ils en prennent connaissance. Il sera également affiché afin qu'il soit lisible par tous.

PARTIE 10 : POLITIQUE DE CONFIDENTIALITE

À la suite de l'entrée en vigueur de la législation européenne RGPD, le CIAS et la Communauté de Communes du Pays de Craon vous informe de manière transparente sur l'utilisation qui est faite de vos données personnelles.

En vue :

- ➢ De la gestion administrative des personnels sur la base légale de notre intérêt légitime d'employeur ;
- ➢ De la gestion des rémunérations et accomplissement des formalités administratives afférentes sur la base légale de nos obligations juridiques ;
- ➢ De la mise à disposition du personnel d'outils professionnels sur la base légale de notre intérêt légitime d'employeur ;
- ➢ De l'organisation du travail sur la base légale de l'exécution du contrat de travail ;
- ➢ Du suivi des carrières et de la mobilité sur la base légale de notre intérêt légitime d'employeur ;
- ➢ De l'organisation de formation sur la base légale de notre intérêt légitime d'employeur ;
- ➢ De la tenue des registres obligatoires, rapports avec les instances représentatives du personnel sur la base légale de nos obligations juridiques ;
- ➢ De la gestion des communications internes sur la base légale de notre intérêt légitime d'employeur ;
- ➢ De la gestion des aides sociales sur la base légale de notre intérêt légitime d'employeur

- De la réalisation des audits, gestion du contentieux et du précontentieux sur la base légale de notre intérêt légitime d'employeur ;
- De la gestion de la paie, du personnel et des déclarations sociales sur la base légale de nos obligations juridiques ;

Votre dossier individuel et les documents de gestion du personnel associés seront conservés par le CIAS et la Communauté de Communes du Pays de Craon qui est le responsable de traitement en base active, le temps de la durée du contrat de travail. La nature des données traitées inclut des informations d'identité, de situation professionnelle, de preuves d'autorisation de travail, de gestion de carrière, d'évaluation professionnelle, de formation, de suivi administratif, de rémunération, de gestion de déclaration éventuellement médicale, d'outils et matériel mis à la disposition de l'agent, d'activité élective voire syndicale ou sociales. Seuls la Direction, le personnel de la Direction des ressources humaines et le personnel interne ou externalisé en charge de la comptabilité et de la paie sont habilités à avoir accès aux données conservées. Les délais de conservation des données sont fixés par les délais légaux en la matière.

Des informations vous concernant sont aussi susceptibles d'être enregistrées dans les données ou documents suivants :

Finalité/Documents Destinataire habilité Durée de conservation

- Traçabilité des appels téléphoniques et des usages de la téléphonie et d'internet en vue de sécurisation et de contrôle des dépenses sur la base de notre intérêt légitime d'employeur
  Direction en cas de problématique, Managers concernés 1 an
- Traçabilité technique des outils informatiques en vue de sécurisation sur la base de notre intérêt légitime d'employeur
  Direction en cas de problématique, techniciens concernés, managers concernés 6 mois
- Vidéosurveillance en vue de sécurisation sur la base de notre intérêt légitime d'employeur
  Pour le temps réel, seuls la Direction et le personnel en charge de la sécurité ont accès aux images. Pour les données archivées, la Direction ou son délégataire en son absence ont accès aux données. 1 mois
- Traçabilité du contrôle d'accès à l'entrée du siège (horaire d'entrée-sortie, N° de matricule, identité) en vue de contrôle d'accès sur la base légale de notre intérêt légitime de sécurisation
  Direction en cas de problématique, managers concernés 3 mois

Nous vous informons que des informations sur nos collaborateurs sont susceptibles d'être transférées à des partenaires, notamment de contrôle, de santé, institutionnels ou de résolution de litige (avocat externalisé, organismes sociaux, médecine du travail, OPCO, mutuelles, prévoyances, commissaire aux comptes, cabinets comptables, prestataire-paie, etc.).

Après la cessation du contrat de travail, les données concernant nos agents seront archivées le temps des délais légaux de prescription des litiges (ou d'obligation par l'Etat en vue de reconstitution de votre carrière lors de votre départ en retraite). Seuls la Direction et le personnel RH missionné pour des problématiques juridiques ainsi que le personnel juridique externalisé éventuel sont habilités à avoir accès aux données archivées.

En application des lois européennes et de la loi du 6 janvier 1978 (relative à l'informatique, aux fichiers et aux libertés), vous disposez des droits d'accès, de rectification, de limitation, de portabilité et de suppression de vos données personnelles ainsi que du droit d'opposition à leurs traitements pour des motifs légitimes. Vous pouvez exercer l'ensemble de ces droits par email à l'adresse dpo@paysdecraon.fr , ou courrier postal adressé à au délégué à la protection des données – 1 rue Buchenberg 53400 CRAON. Vous disposez par ailleurs, des droits de retirer à tout moment vos consentements et d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), notamment sur son site internet www.cnil.fr

ANNEXES

Dispositions légales applicables

Règlement n° 2016/679 de l'Union européenne, dit « règlement général sur la protection des données » (R.G.P.D.), qui constitue le texte de référence en matière de protection des données à caractère personnel.

La loi n° 2018-493 du 20 juin 2018 promulguée le 21 juin 2018 qui a modifié la loi Informatique et Libertés du 6 janvier 1978 afin d'exercer certaines des « marges de manœuvre nationales » autorisées par le Règlement général sur la protection des données et de modifier certaines dispositions de la loi Informatique et Libertés pour les rapprocher de législation RGPD.

Dispositions Pénales :

- Code Pénal (partie législative) : art 226-16 à 226-24
- Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. Dispositions pénales : art 323-1 à 323-3 du Code pénal.

Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)

Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels.

Disposition pénale : art L.335-2 du Code pénal.