POLITIQUE GENERALE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Préambule

Le cadre légal en matière de protection des données à caractère personnel a considérablement évolué cette année avec l'adoption par le parlement européen (le 14 avril 2016) du nouveau Règlement Général de Protection des données à caractère personnel.

Ce nouveau règlement renforce notamment les droits des personnes concernées (administrés, salariés, …) et impose de nouvelles obligations pour l'organisme qui dispose d'un délai jusqu'au 25 mai 2018 pour se mettre en conformité (date d'entrée en vigueur du nouveau règlement).

Les actions engagées par le département du Doubs avec la nomination en 2017 d'un Délégué à la Protection des Données ont permis d'initier la mise en œuvre d'une partie des obligations mais des efforts supplémentaires doivent encore être consentis pour prendre en compte les nouvelles exigences légales.

Le présent document formalise la Politique Générale de Protection des Données à Caractère Personnel que la collectivité met en œuvre avec pour objectifs de :

- **Se mettre en conformité** avec les obligations légales françaises et notamment la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- **Se mettre en conformité** avec le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- **Décrire les rôles et les responsabilités** en matière de gestion et de protection des données à caractère personnel ;
- **Formaliser les principes** que l'e Département du Doubs entend mettre en application pour assurer la protection des données à caractère personnel.

Ce document de référence intitulé « **Politique Générale de Protection des Données à Caractère Personnel** » est destiné à être diffusé à l'ensemble des acteurs impliqués directement ou indirectement dans la protection du patrimoine informationnel et des systèmes d'information.

La politique n'a pas pour but de constituer un frein aux activités quotidiennes réalisées par les agents dans le cadre de l'exécution de leurs missions, mais de les aider à remplir ces missions dans le respect de la réglementation.

Rédigée le 15/02/2018	Validée le 24/04/2018	Approuvée le 24/04/2018
Le Délégué à la protection des données	Le Directeur général des services par interim	La Présidente
Jean-Marie ARCHIPOFF	Jean-Louis Guillet	Christine BOUQUIN

SOMMAIRE

1 Domaine d'application de la Politique

Les règles et les directives découlant de la présente politique s'appliquent à tous les **traitements de données à caractère personnel, automatisés en tout ou en partie, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un dossier papier** mis en œuvre par les services du Département du Doubs dans les cadres de ses missions.

Les différents acteurs concernés par cette politique sont :

- **Les agents cadres et non cadres** (salariés permanents temporaires, stagiaires, apprentis, etc.),
- **Les, personnels des partenaires, fournisseurs et intervenants externes** dès lors qu'ils utilisent les SI de la collectivité, s'y connectent, y hébergent ou y gèrent des ressources, des systèmes ou des données.

Sont exclus de la présente politique :

- **Les fichiers personnels des salariés dès lors qu'ils sont identifiés comme tel** (cf. Charte Informatique - principes et règles de bon usage et de sécurité -).

2 Définitions

Au titre de la présente Politique Générale de Protection des Données à Caractère Personnel, il est entendu par :

- **«Personne concernée»** (art.4 1) du Règlement n°2016/679): « (…) *personne physique identifiée ou personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à des identifiants en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »;*
- « **Données à caractère personnel** » (art.4 1) du Règlement n°2016/679) : « *toute information se rapportant à une personne concernée (…)* ».
- **« Données concernant la santé »** (art. 4 15) du Règlement n°2016/679) : « *Les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne » ;*
- **«Traitement de données à caractère personnel»** (art. 4 2) du Règlement n°2016/679): « *toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et appliquée(s) à des données à caractère personnel, telle(s) 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, ainsi que la limitation du traitement, l'effacement ou la destruction* »;
- « **Fichier** » (art. 4 6) du Règlement n°2016/679) : « *Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* » ;
- « **Responsable du traitement** » (art. 4 7) du Règlement n°2016/679) : « *Personne, autorité publique, service ou organisme qui détermine les finalités et les moyens de traitement de*

données à caractère personnel » ;

Le Responsable du traitement au sein du Département du Doubs est la Présidente.

- « **Sous-traitant** » (art. 4 8) du Règlement n°2016/679) : « *Personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* » ;
- « **Destinataire** » (art. 4 9) du Règlement n°2016/679) : « *La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un Etat membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement* » ;
- **« Tiers »** (art. 4 10) du Règlement n°2016/679) : « *Une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ».*

  Une liste des tiers autorisés à avoir communication des données à caractère personnel traitées par l'organisme est fournie en annexe II de ce document.
- **« Consentement de la personne concernée »** (art. 4 11) du Règlement n°2016/679) : « *Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement » ;*
- **« Violation de données à caractère personnel »** (art. 4 12) du Règlement n°2016/679) : « *Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données » ;*
- **« Limitation du traitement »** (art. 4 3) du Règlement n°2016/679) : « *Le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur » ;*
- **« Autorité de contrôle »** (art. 4 21) du Règlement n°2016/679) **:** *« Une autorité publique indépendante qui est instituée par un Etat membre en vertu de l'article 51 »* (du Règlement) ;

  En France, l'Autorité de contrôle est la Commission Nationale de l'Informatique et des Libertés (« CNIL »).
- **« Profilage »** (art. 4 4) du Règlement n°2016/679) : « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* » ;
- **Télé-service** (*ordonnance du 2005-1516 du 8/12/2005*) : tout système d'information permettant aux usagers de procéder par voie électronique à des démarches ou des formalités administratives *(échanges électroniques entre les usagers et les autorités administratives et entre autorités administratives).*

3 Rôles et responsabilités au titre de la protection des données à caractère personnel

3.1.1 La Présidente du Département du Doubs

Conformément aux obligations légales en vigueur[1], le Président de l'organisme est le Responsable des traitements mis en œuvre par l'organisme dans le cadre des missions.

Il est l'interlocuteur principal de l'autorité compétente (CNIL) et des personnes concernées en cas de litiges ou d'incidents relevant du cadre juridique en vigueur.

Pour la mise en œuvre opérationnelle des règles et des directives découlant de la présente politique, la Présidente de la collectivité délègue ses pouvoirs au Directeur Général des Services.

3.1.2 Le Directeur Général des Services

Au titre de la protection des données à caractère personnel, le Directeur Général des Services prend les mesures appropriées pour garantir que le traitement des données à caractère personnel est effectué dans le respect des dispositions adoptées conformément à la présente politique.

Les responsabilités qui incombent au Directeur Général des Services sont les suivantes :

- Il veille à ce que les directions métiers associent le délégué à la protection des données [DPD] (cf. §3.1.3), d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.
- Il veille également à ce que le DPD soit doté des moyens d'accomplir les missions et obligations qui lui incombent de manière effective et en toute indépendance, et ne reçoive aucune instruction en ce qui concerne l'exercice de sa fonction.
- Il s'assure que les sous-traitants intervenant sur les traitements mis en œuvre par le Département du Doubs présentent des garanties suffisantes de mise en œuvre des mesures et procédures techniques et organisationnelles appropriées, de manière à ce que le traitement soit conforme aux dispositions adoptées conformément à la présente politique et garantisse la protection des droits de la personne concernée.
- Il homologue la sécurité de données et des systèmes d'information en conformité avec les obligations réglementaires en vigueur[2] (notamment au titre de l'ordonnance du 2005-1516 du 8/12/2005 relative à l'e-administration).

---

[1] L'article 34 de la Loi informatique et Libertés dispose que « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

L'article 24 1. du Règlement n°2016/679 précise que : « Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire ».

[2] L'article 25 du Règlement européen n°2016/679 prévoit que le responsable du traitement soit en mesure de démontrer qu'il respecte le principe de protection dès la conception et la protection par défaut.

L'article 25 1) du Règlement met en avant « **la protection des données dès la conception** » : « *1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données ».*

3.1.3 Le Délégué à la Protection des Données (DPD)

La Présidente du Département du Doubs a désigné, en mai 2017, un Délégué à la Protection des Données (DPD) chargé d'assurer, d'une manière indépendante, le respect des obligations pour l'ensemble des traitements sous sa responsabilité. Le DPD, dans le cadre de ses missions, est tenu au secret professionnel.

Le DPD est directement rattaché au Directeur Général des Services. Afin de faciliter les aspects opérationnels de sa mission, la Directrice des Usages du Numérique est désignée comme son interlocuteur privilégié.

Pour s'acquitter de sa tâche (réf. Art. 38 du Règlement n°2016/679), le DPD dispose de la liberté d'action et des moyens qui lui permettent de recommander des solutions organisationnelles ou techniques adaptées. Il exerce pleinement ses missions, en dehors de toute pression, et joue son rôle auprès du responsable des traitements.

Il est tenu d'informer le Directeur Général des Services en cas de risques majeurs pouvant impacter la vie privée des administrés ou des salariés afin de déterminer les mesures nécessaires à la préservation de la vie privée.

En outre, le DPD est reçu formellement a minima une fois par trimestre par le Directeur Général des Services afin de rendre compte de ses activités. Ces réunions ont un ordre du jour et donnent lieu à un compte rendu annexé au bilan.

Dans le cadre de ses missions définies par la loi, le DPD rédige chaque année un bilan de ses activités qu'il présente ou remet à la Présidente du Département du Doubs et qu'il tient à la disposition de la CNIL (article 49 du décret de 2005). La rédaction du bilan est obligatoire et constitue une des missions principales du Délégué à la Protection des Données.

Le DPD a en charge les actions suivantes (réf. Art. 39 du Règlement n°2016/679) :

- **Le conseil et les recommandations** dans la mise en œuvre des traitements ;
- La construction et la diffusion de la culture de la maîtrise des risques liées à la gestion des données à caractère personnel ;
- L'établissement, la mise à jour et la publication de la liste des traitements automatisés des données à caractère personnel (tenue du registre) ;
- **Le suivi des formalités préalables** à toute mise en œuvre de traitements de données à caractère personnel ;
- **L'alerte du responsable des traitements** en cas de manquement grave à la loi ;
- **L'interface et la médiation avec les usagers** lors de leur demande d'exercer leurs droits ;
- L'établissement et le maintien d'une relation privilégiée de collaboration avec la CNIL ;
- **L'établissement d'un bilan annuel d'activités** en relation avec la gestion des données à caractère personnel ;
- **L'élaboration et l'actualisation** des principes et des règles d'application de la politique de conformité des données à caractère personnel ; **l'autorité** pour les faire respecter.

Dans le cadre de ses fonctions, le DPD doit pouvoir s'appuyer sur l'expertise et les compétences :

- Des Archives départementales pour :
  - s'assurer de la bonne conservation des documents quand ils sont encore dans les services ou chez des hébergeurs ;

- déterminer leur durée de conservation ;
- sélectionner les documents d'intérêt historique et juridique à conserver définitivement ;
- autoriser les destructions ;

- Des directions métiers et notamment sur les Relais Informatique et Libertés (RIL) désignés ;
- D'un interlocuteur privilégié au sein de la Direction de la Modernisation de l'Action Publique (Service Juridique-Assemblées-Deontologie) ;
- Du Responsable de Sécurité des Systèmes d'Information (RSSI) en matière de sécurité des données ;
- D'experts en protection de la vie privée ;
- **De réseaux professionnels** dédiés à la protection de la vie privée ;
- De la CNIL.

La fin de la mission du DPD peut intervenir pour différentes raisons (réf. Art. 52, 53 et 54 du Décret de 2005). L'organisme s'engage à remplacer le DPD et maintenir son remplaçant dans les mêmes conditions de désignation, de lui assurer les mêmes missions et les mêmes fonctions (Cf chapitres précédents).

3.1.4 Le Responsable de la Sécurité des Systèmes d'Information (RSSI)

Au titre de la protection des données à caractère personnel, le Responsable de la Sécurité des Système d'Information définit, fait approuver et assure le suivi de la mise en œuvre des règles et des directives de la politique des sécurité des Si de l'organisme (PSSI).

Afin de préserver la cohérence et l'efficacité des actions de protection relative à la vie privée, le RSSI et le DPD travaillent en étroite collaboration et de façon coordonnée.

Conformément à la PSSI de l'organisme, les missions du RSSI sont réparties comme suit :

- Les missions relevant du domaine « pilotage » : missions qui visent à organiser puis contrôler le déploiement de la PSSI, à s'assurer que les risques majeurs pour la protection de la vie privée sont sous contrôle et à évaluer l'efficacité de l'action SSI ;
- Les missions relevant du domaine « opérationnel » : missions qui visent à accompagner les acteurs en charge de la mise en œuvre des mesures de sécurité préventives, dissuasives et réactives ;
- Les missions relevant du domaine « support » : missions qui visent à permettre aux intervenants en charge de la définition, de la mise en œuvre et du contrôle de la PSSI de réaliser les actions qui leur incombent.

3.1.5 Responsable de la Sécurité des biens et des personnes

Placé sous la responsabilité de la Direction du Patrimoine et de la Logistique il est le maître d'œuvre des mesures de sécurité physique des données à caractère personnel placés sous la responsabilité de l'organisme.

A ce titre, il veille à la mise en place des meilleures pratiques en matière de sécurité physique des données à caractère personnel (broyeur, contrôle d'accès physique, destruction des papiers, vidéo-surveillance, lutte contre les incendies, …) et assure leur maintien en condition opérationnelle.

3.1.6 Le Directeur des archives

Le directeur des Archives départementales assiste les directeurs dans la définition de la durée de conservation, s'assure de sa mise en œuvre et peut décider de la conservation de données présentant un intérêt historique au-delà de la durée de conservation liée à la finalité initiale (art. 89 du RGPD).

3.1.7 Les Directeurs

Chaque directeur est considéré comme responsable de la mise en œuvre des traitements au sein de sa direction. A ce titre, il détermine clairement les finalités et les moyens de chacun des traitements de données à caractère personnel et il s'assure de la conformité du traitement avant sa mise en œuvre.

Le Directeur est l'interlocuteur privilégié du DPD pour tout ce qui relève des traitements mis en œuvre au sein de ses services. En superviseur des administrateurs fonctionnels [AFONDs] et des facilitateurs des usages numériques [FUN] dans sa Direction, Il agit en tant que Relais Informatique et Libertés (RIL) afin d'apporter un support opérationnel aux missions du DPD.

Le Directeur, RIL par défaut, peut, tout en en conservant les obligations, déléguer cette mission à un agent cadre de sa direction. Le Relais informatique et libertés est un maillon essentiel de la mission Informatique et Libertés au sein de l'organisme.

Il incombe au Directeur de s'assurer que chaque agent placé sous sa responsabilité applique les règles et les directives de la présente politique qui leur incombe, notamment en matière de création de nouveau fichier, d'utilisation des données à caractère personnel et d'alerte en cas de violation sur les données.

Dans le cadre des contrats passés avec des tiers (convention, marché etc.), il incombe au Directeur, dès lors que des données à caractère personnel sont traitées, de s'assurer que les clauses spécifiques relatives à la protection des données à caractère personnel et à la responsabilité du tiers et de l'organisme dans le domaine sont prévues.

3.1.8 Les agents

Avant toute mise en œuvre d'un nouveau traitement, les agents doivent en référer au Relais Informatique et Libertés de leurs directions respectives.

Il incombe à chaque agent, cadre et non cadre, de respecter et de faire respecter l'ensemble des directives de la présente politique pour les traitements qu'ils sont amenés à mettre en œuvre et à exploiter au sein de leurs services et de reporter tout incident ou violation sur les données constaté.

3.1.9 Le Directeur des systèmes d'Information

Le Directeur des Systèmes d'Information est le maitre d'œuvre des mesures de sécurité des données à caractère personnel traitées dans les moyens informatiques placés sous la responsabilité de l'organisme.

A ce titre :

- Il veille à la mise en place des meilleures pratiques en matière de sécurité de données dans le respect des directives des autorités compétentes (ANSSI, CNIL etc.) et assure leur maintien en condition opérationnelle. Les règles de sécurité des données sont définies dans la politique de sécurité des SI (PSSI) formalisée et suivie par le RSSI (Responsable de la Sécurité du SI).

- Il s'assure que les chefs de projet informatique intègrent dans leurs démarches la prise en compte de la protection des données à caractère personnel dès les phases amont d'un projet tel qu'imposé par le règlement européen. Dans ce cadre, le DPD apporte son assistance pour mettre en conformité les nouveaux traitements avec la réglementation en vigueur.
- Il s'assure que tout contrat avec des tiers (éditeurs, hébergeurs, fournisseurs, etc.), dès lors que des données à caractère personnel sont traitées, inclue des clauses spécifiques relatives à la protection des données à caractère personnel et à la responsabilité du tiers et de l'organisme dans le domaine.
- Il s'assure que tout incident de sécurité identifié par un agent de la DUN impactant des données à caractère personnel fasse l'objet d'une notification sans délai auprès du DPD et du RSSI qui déclencheront, si nécessaire les procédures relatives à la violation de données à caractère personnel.

3.1.10 Destinataires et tiers autorisés

Dès lors que les données à caractère sont transmises à des tiers autorisés (cf. Annexe II) ou à des destinataires externes, la sécurité et l'usage de ces données leur incombent et la responsabilité de l'organisme n'est plus engagée.

Cependant, la direction responsable du traitement doit s'assurer que la sécurité de transmission des données est assurée.

3.1.11 Les sous-traitant externes

Dans le cadre des missions confiées contractuellement à un sous-traitant, la responsabilité de celui-ci se limite aux respects des clauses contractuelles. L'organisme reste responsable juridiquement du traitement des DCP.

Il incombe aux directions métiers et/ou aux maitrises d'œuvre, dès les phases de contractualisation de préciser les conditions de collecte, d'usage et de conservation des données à caractère personnel.

Les contrats signés avec les sous-traitants précisent les obligations qui leur incombent au titre de la protection des données à caractère personnel et leurs responsabilités en cas de violation de données.

En matière de sécurité des données, les directives de la PSSI (politique de sécurité des SI) doivent être appliquées par les sous-traitants qui définissent les modalités techniques pour les appliquer.

4 Directives relatives à la protection des données à caractère personnel

Chaque responsable du service en charge de la mise en œuvre des traitements de données à caractère personnel doit s'assurer que les principes énoncés ci-dessous sont appliqués par les personnels placés sous sa responsabilité.

Il doit être en mesure de démontrer que tous les moyens sont mis en œuvre par son service pour respecter les principes énoncés.

Il incombe au DPD de contrôler l'application de ces règles et d'alerter le responsable des traitements de toute non-conformité constatée.

La Présidente du Département est tenue informée annuellement par le DPD des actions engagées pour se mettre en conformité avec les obligations légales en vigueur.

4.1 Directives relatives au registre des traitements de données

Objectif : Tenir à jour la liste de tous les traitements mis en œuvre au sein de l'organisme et la mettre à disposition des personnes concernées qui en feraient la demande.

Directive REG_01 : Mettre à jour le registre des traitements

Un registre des traitements de données à caractère personnel est tenu à jour au sein de la collectivité.

Sa création et sa mise à jour sont confiées au Délégué à la Protection des Données qui définit les procédures appliquées au sein du Département pour son maintien en condition opérationnelle.

Ce registre contient a minima les informations légales imposées par la législation en vigueur.

Le DPD peut intégrer des informations complémentaires qu'il juge nécessaires à l'accomplissement de ses missions.

Directive REG_02 : Déclarer tous les traitements au DPD

Il est de la responsabilité des Directeurs de s'assurer que tous les traitements de données à caractère personnel mis en œuvre au sein de leurs services soient inscrits au registre des traitements.

Tout nouveau traitement doit faire l'objet d'une déclaration auprès du DPD afin qu'il puisse instruire la demande de création d'un traitement et inscrire celui-ci dans le registre du Département.

Pour chaque nouveau traitement, le RIL de la direction concernée par le nouveau traitement renseigne le formulaire idoine, en précisant en langage clair et facilement compréhensible, la finalité du traitement, les données traitées, des destinataires et la durée de conservation. Celui-ci doit être daté et signé du Directeur.

Ce formulaire est transmis au DPD, qui tient à jour le registre des traitements mis en œuvre par la collectivité. A cette étape, il transmet le formulaire au directeur des Archives départementales, pour validation de la durée de conservation et mise en œuvre éventuelle à terme de traitements archivistiques (art.89). Tout traitement mis en œuvre sans respecter la procédure définie par le DPD est considérée comme illicite.

Pour les traitements opérationnels, le responsable du traitement ou son sous-traitant doit s'assurer que le traitement reste dans le cadre du but (finalité) défini. Tout traitement de données qui va au-delà des buts spécifiés initialement représente un détournement de finalité.

Directive REG_03 : Rendre accessible le registre des traitements

Le registre des traitements est rendu accessible aux agents du département par le DPD au travers des moyens de communications mis en œuvre par la collectivité. Le registre est accessible directement depuis « I-DOO » dans l'espace collaboratif dédié.

Une procédure interne permet aux personnes externes (usagers, tiers, ..) de prendre connaissance du contenu du registre des traitements. Il est communicable à toute personne qui en fait la demande.

La Présidente du Département reçoit annuellement une copie du registre des traitements au travers du bilan annuel du DPD.

Sur demande, le registre peut être rendu disponible à la CNIL lors de sa démarche de contrôle notamment.

Directive REG_04 : Vérifier régulièrement le registre des traitements

Le DPD peut être amené à faire vérifier la conformité du registre des traitements avec les obligations légales en vigueur et les directives de la CNIL.

Dans ce cadre, le DPD définit les modalités de vérification du registre, qui peut être réalisée par un expert externe ou interne.

En outre, une revue périodique de conformité du traitement est réalisée par le DPD en collaboration avec les directions métiers et les non-conformités constatées font l'objet d'un plan d'actions.

4.2 Directives relatives à la garantie de licéité des traitements

Objectif : L'organisme s'engage à mettre en œuvre tous les moyens pour garantir la licéité des traitements en conformité avec les obligations légales en vigueur (art. 5 et 6 du Règlement n°2016/679).

Directive LIC_01 : **Agir avec loyauté et transparence lors de la collecte des données** (art. 5.1 a) du Règlement n°2016/679)

Les agents ne doivent pas collecter des données à caractère personnel à l'insu des personnes concernées ou lorsque les personnes s'y opposent légitimement. En outre, et conformément aux obligations légales en vigueur, ils s'engagent :

- à ne collecter que des données **adéquates, pertinentes et non excessives** (art. 5.1 c) du Règlement n°2016/679) au regard de la finalité du traitement (cf. Règle LIC_03).
- à ne collecter des données que pour des finalités déterminées, légitimes et explicites (art. 5.1 b) du Règlement n°2016/679)

Les traitements sont justifiés par le consentement des personnes concernées (cf. Règle LIC_02) ou par l'un des cas suivants :

- Le respect d'une obligation légale, (par exemple, les traitements imposés par les obligations déclaratives pesant sur les employeurs en matière fiscale et sociale, aide sociale à l'enfance, etc.) ;
- L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
- La réalisation de l'intérêt légitime tout en respectant les intérêts et les droits et libertés fondamentaux de la personne concernée ;

- L'exécution d'une mission (par exemple les fichiers de police ou de justice, à l'exception de données sensibles portant sur un autre régime) ;
- La sauvegarde des intérêts vitaux.

Dans toutes ses relations avec les personnes concernées, les agents de la collectivité s'engagent sur une transparence totale relative au(x) traitement(s) effectué(s) sur les données recueillies et ils s'engagent à fournir toutes les explications dans un langage adapté nécessaire à la compréhension du traitement et des données collectées.

Directive LIC_02 : Démontrer que le consentement des personnes concernées est respecté (art. 7 du Règlement n°2016/679)

Pour les traitements soumis au consentement des personnes concernés, la direction en charge de la mise en œuvre du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement. Pour les mineurs ou majeurs sous tutelle, le consentement est obtenu auprès de l'autorité parentale ou par l'autorité de tutelle.

La demande de consentement est présentée de façon distincte, claire et compréhensible dans un langage approprié. Par exemple, un encart dédié dans le formulaire de collecte, document de consentement dédié avec indication de la finalité du traitement et la possibilité de retrait de ce consentement, case à cocher dans le cadre des télé-services.

Les modalités de recueil et de conservation de ce consentement doivent être définies avant la collecte des données et la mise en œuvre du traitement.

Les traces permettant de démontrer le consentement des personnes concernées sont conservées dans les services en charge de la mise en œuvre des traitements et mises à disposition lors des demandes de justification ou de contrôle.

Le consentement peut être retiré à tout moment par la personne concernée sans que cela remette en cause la licéité du traitement. Cependant, si la finalité repose sur le traitement de la donnée consentie, le retrait du consentement entraîne la fin du traitement, il sera nécessaire d'en informer la personne concernée. Dans ce cas, le service en charge du traitement s'engage sauf indication légale contraire à détruire ou faire détruire les données concernées.

Directive LIC_03 : **Respecter les finalités déterminées lors de la collecte des données**

Les données collectées pour des finalités déterminées, légitimes et explicites ne peuvent être traitées pour d'autres finalités sans en informer la personne concernée et obtenir son consentement.

Directive LIC_04 : Limiter les informations collectées dans les formulaires papiers ou numériques au strict nécessaire

Les formulaires papiers ou numériques conçus par les Directions métiers pour recueillir les données à caractère personnel ne doivent contenir que les champs d'informations strictement nécessaires à la finalité du traitement afin d'éviter de collecter des données non justifiées par le traitement.

Le DPD apporte le conseil nécessaire à la réalisation de ces documents.

Les formulaires doivent être suffisamment explicites pour identifier les champs obligatoires au travers notamment d'un symbole clair.

Directive LIC_05 : Limiter la conservation des données au strict nécessaire (art. 5.1 e) du Règlement n°2016/679)

Les données collectées par les agents ne peuvent pas être conservées au-delà des besoins définis dans le cadre de la finalité du traitement. Les durées de conservation infinies ou

indéterminées sont proscrites sauf décision contraire du directeur des Archives, motivée par l'une des fins prévues à l'article 89 du RGPD.

Avant la mise en œuvre du traitement, le responsable de traitement ou son sous-traitant précise, dans le cadre des dossiers de formalités préalables et dans la fiche signalétique du traitement, la durée de conservation des données.

Dans les archives courantes et intermédiaires (informatisées ou papier), les données ne sont conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées, sauf si le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Les Archives départementales en collaboration avec les directions métiers établissent la politique et les procédures aptes à gérer les durées de conservation (tableau de gestion).

A cet égard, les directions métiers s'engagent à respecter la politique en matière d'archivage. Pour rappel :

- Les fichiers papiers contenant des données à caractère personnel sont versés aux Archives ou éliminés.
- Aucune élimination de documents ne peut être réalisée sans le bordereau idoine signé des archives.
- Les copies numériques des documents conservés dans les dossiers papier ne doivent en aucun cas être conservées plus longtemps que le délai prévu dans le registre des traitements pour le document papier correspondant.
- Les fichiers bureautiques « à éliminer » sont purgés par les Directions métiers.
- Les fichiers informatiques centralisés (applications métiers) contenant des données à caractère personnel et identifiées par les Archives départementales comme « à éliminer » sont détruites par la DUN sur sollicitation des directions métiers.
- Les fichiers informatiques centralisés (applications métiers) contenant des données à caractère personnel et identifiées par la Direction des archives comme « à conserver » sont archivés par la DUN sur sollicitation des directions métiers dans le système d'archivage électronique du Département, géré par les Archives départementales.

4.3 Directives relatives aux traitements de données sensibles ou perçues comme sensibles

Objectif : L'organisme s'engage à appliquer des procédures et des moyens spécifiques aux traitements des données sensibles ou perçues comme sensibles afin de limiter les risques pour les personnes concernées et de respecter les obligations légales concernant leurs traitements.

Directive DPS_01 : **Respecter le cadre légal relatif au traitement des données sensibles** (art. 9 du Règlement n°2016/679)

Les traitements des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique **sont interdits sauf** dans les cas suivants :

- La personne concernée a donné son consentement explicite au traitement de ces données ;
- Obligation légale à traiter ce type de données ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- Données rendues publiques par la personne concernée ;
- Gestion et suivi de la médecine préventive ou de la médecine du travail.

Les directions métiers s'engagent à respecter ces principes et alertent sans délai le DPD de toutes non-conformités constatées ou de toute violation sur ces données.

Directive DPS_02 : **Interdire le traitement des données relatives aux condamnations pénales et aux infractions** (art. 10 du Règlement n°2016/679)

Les directeurs métiers doivent s'assurer que les documents relatifs aux condamnations pénales et aux infractions que les agents sont amenés à recueillir dans le cadre de leurs missions ne peuvent en aucun cas faire l'objet d'un traitement interne à la collectivité.

Seuls sont autorisés :

- La conservation de ces pièces selon la politique d'archivage en vigueur ;
- La transmission de ces documents à des destinataires ou prestataires externes dès lors qu'un cadre légal le justifie.

Directive DPS_03 : **Limiter l'accès aux données de santé aux seuls professionnels habilités** (art. 9 du Règlement n°2016/679)

Les données de santé collectées par la collectivité (médecine préventive, médecine du travail, action sociale, etc.) sont placées sous la responsabilité d'un professionnel soumis à une obligation de secret professionnel conformément au droit en vigueur.

Il incombe au responsable du traitement de s'assurer que seules les personnes habilitées puissent y avoir accès (papier ou numérique) et que les règles définies par les autorités compétentes sont appliquées (ASIP santé – Ministère de l'action sociale et de la santé).

Directive DPS_04 : **Interdire l'usage du NIR comme identifiant unique**

En aucun cas le Numéro de sécurité sociale ne peut être utilisé au sein des services comme identifiant unique d'un usager.

Les systèmes informatiques ne doivent pas permettre l'usage du NIR comme identifiant unique des personnes.

Directive DPS_05 : **Limiter l'accès et l'usage des données bancaires au strict nécessaire**

Les données bancaires collectées par l'organisme (RH, action sociale etc.) sont placées sous la responsabilité de la direction métier en charge du traitement concerné.

Il lui incombe de s'assurer que seules les personnes habilitées puissent y avoir accès (papier ou numérique) et que les règles définies par les autorités compétentes sont appliquées.

Directive DPS_06 : Limiter l'accès aux données sur les difficultés sociales des personnes aux seules personnes habilitées

Seuls les professionnels assujettis au secret professionnel sont habilités à collecter et à traiter des données sur les difficultés sociales des personnes.

Il leur incombe de s'assurer que la protection des données est bien assurée (notamment lors de leur stockage et de leur transfert) et d'alerter le DPD ou le RIL en cas de violation sur ces données.

Directive DPS_07 : Réaliser des évaluations d'impact sur la vie privée des personnes concernées par les traitements de données sensibles.

Dans le cas où la licéité du traitement est avérée, il incombe à la direction concernée de s'assurer préalablement à la mise en œuvre du traitement **qu'une étude d'impact sur la vie privée** des personnes concernées a été réalisée par l'équipe projet et a été validée par le DPD (art. 35 du Règlement n°2016/679).

L'analyse d'impact sur la vie privée (AIVP) doit être menée par le responsable du service en charge de la mise en œuvre du traitement en collaboration avec le DPD, le RSSI, les chefs de projet et les personnels impliqués dans le traitement (Utilisateur, équipe informatique, etc.).

Le DPD se charge de vérifier les résultats de l'analyse d'impact au regard notamment des obligations légales et des risques internes ou externes associés au traitement des DCP.

Le Responsable des traitements approuve et valide les résultats des analyses d'impacts sur la vie privée, prend les décisions pour réduire les risques identifiés et accepte les risques résiduels.

La démarche méthodologique adoptée pour évaluer les impacts sur la vie privée des personnes concernées s'appuie sur les guides méthodologiques de la CNIL.

Il incombe au responsable du service en charge de la mise en œuvre des traitements de DCP de s'assurer que les principes énoncés précédemment sont appliqués par les personnels placés sous sa responsabilité.

Il incombe au DPD de contrôler l'application de ces règles et d'alerter le responsable des traitements de toute non-conformité constatée.

Directive DPS_08 : **Limiter l'usage des zones de commentaires à des informations d'ordre général**

L'usage des zones commentaires dans les logiciels professionnels, les bases de données ou les fichiers mis à la disposition par l'organisme (exemple : ASTRE RH, ASTRE GF, IODAS, fichiers XLS, …) ainsi que sur les formulaires est strictement réservé aux informations d'ordre général et ne pouvant en aucun cas porter atteinte aux droits des personnes concernées.

Certains commentaires pouvant être désobligeants, discriminants, voire injurieux, ou encore faire apparaitre des données dites « sensibles » telles que des données relatives à la santé, il convient d'utiliser des termes neutres et objectifs.

4.4 Directives relatives au respect des droits des personnes

Objectif : Le Département du Doubs s'engage à informer les personnes concernées des droits dont elles disposent légalement et à mettre en œuvre tous les moyens leur permettant de les exercer.

Directive DRO_01 : S'assurer que les mentions légales sont conformes aux obligations (art. 13 du Règlement n°2016/679)

Toute collecte de données doit être réalisée en s'assurant que la personne concernée a été informée de ses droits.

Il incombe aux directions métiers de s'assurer que les mentions légales présentes sur les formulaires papier ou numériques comportent les informations nécessaires à l'exercice des droits

des personnes concernées.

Le DPD peut être sollicité pour conseiller ou vérifier la conformité des mentions d'informations aux obligations légales qui s'imposent.

Outre les informations relatives aux respects des droits, les mentions légales doivent également préciser les informations nécessaires permettant à la personne concernée de donner son consentement au traitement de ses données ou d'être informée sur la nature des traitements visés.

Ainsi selon la nature du traitement, les informations suivantes doivent (ou peuvent) être présentes sur les mentions légales d'information :

- L'identité et les coordonnées du responsable du traitement ;
- Les coordonnées du DPD ;
- Les finalités du traitement pour lequel les données sont collectées ;
- Les intérêts légitimes poursuivis par le responsable du traitement si le traitement n''impose pas le consentement de la personne concernée ;
- Les catégories de destinataires des données si la communication des données est envisagée ;
- L'intention du responsable du traitement d'effectuer un transfert de données à caractère personnel hors UE le cas échéant ;
- La durée de conservation des données à caractère personnel ;
- L'existence du droit de demander au responsable du traitement la rectification ou l'effacement de ces données, ou la limitation de leur traitement ;
- L'existence du droit de retirer son consentement lorsque le traitement est fondé sur l'article 6 paragraphe 1 a) ou sur l'article 9 paragraphe 2 a),
- Le droit d'introduire une réclamation auprès de la CNIL et les coordonnées de ladite CNIL,
- Le caractère contractuel ou réglementaire de la collecte de données à caractère personnel,
- L'existence d'une prise de décision automatisée y compris le profilage ;
- Si les données ne sont pas collectées auprès de la personne concernée, le responsable du traitement ou son sous-traitant doit l'informer au plus tard lors de leur enregistrement ou, en l'absence d'un enregistrement, lors de leur première communication à un.

Directive DRO_02 : Permettre aux personnes concernées d'exercer leurs droits d'accès (art. 15 du Règlement n°2016/679)

Il incombe aux directions métiers de mettre en œuvre tous les moyens pour permettre aux personnes qui en font la demande d'exercer leurs droits dans les délais légaux en vigueur, deux mois actuellement (un mois à compter de 2018).

Dans le cadre d'une demande relative à un dossier médical ce délai est réduit à huit jours (deux mois si dossier antérieur à cinq ans).

Bien qu'étant un droit fondamental, la collectivité peut refuser de donner suite à la demande dans les cas suivants :

- Demande manifestement infondée ou excessive : dans ces cas-là, il appartient alors directeur concerné de démontrer le caractère excessif ;
- Demande formulée alors qu'une action de justice est en cours.

La réponse apportée doit être claire, précise et facilement compréhensible par tous. En cas de codes ou sigles, la liste des abréviations et des correspondances devra être fournie. Attention, il convient de préciser toutefois que la direction métier concernée ne peut en aucun cas modifier ou occulter une information.

Aucun paiement ne peut être exigé pour répondre aux requêtes des personnes concernées.

Afin de se conformer aux obligations légales en vigueur, le DPD assure le suivi de toutes les demandes de droit d'accès, rectification, suppression, opposition selon une procédure validée par le Directeur Général des Services.

Le responsable des traitements est tenu informé annuellement des demandes exprimées par les agents et les usagers, ainsi que des suites données à ces demandes. Le DPD tient un registre « de suivi ».

Directive DRO_03 : Permettre aux personnes concernées d'exercer leurs droits de rectification (art. 16 du Règlement n°2016/679)

Il incombe à la direction métier en charge de la mise en œuvre du traitement concerné par la demande de rectifier ou de compléter les données à caractère personnel qui sont inexactes, dans les meilleurs délais selon les procédures en vigueur au sein de l'organisme.

La direction métier est tenue également d'apporter les preuves des rectifications ou modifications demandées lors de la constitution du dossier de réponse à fournir au demandeur.

Toute difficulté ou impossibilité (technique ou juridique) ne permettant de répondre favorablement à la demande doit être justifiée.

Le DPD est sollicité dès que nécessaire pour traiter les éventuels risques de litiges avec le demandeur.

Directive DRO_04 : Permettre aux personnes concernées d'exercer leurs droits d'opposition (art. 20 du Règlement n°2016/679)

Il incombe à la direction métier de stopper le traitement des données d'une personne concernée qui en fait la demande, à moins de démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Le DPD est sollicité dès que nécessaire pour traiter les éventuels risques de litiges avec le demandeur.

Directive DRO_05 : Permettre aux personnes concernées d'exercer leurs droits à l'oubli (art. 17 du Règlement n°2016/679)

L'organisme a l'obligation d'effacer les données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

- Les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ;
- La personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ;
- La personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement;
- Les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- Les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit français;

Exception à ce droit : pour tout traitemnent nécessaire :

- Au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- A des motifs d'intérêt public dans le domaine de la santé publique :
- A des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
- A la constatation, à l'exercice ou à la défense de droits en justice.

Directive DRO_06 : Permettre aux personnes concernées d'exercer leurs droits à la limitation du traitement de leurs données (art. 18 du Règlement n°2016/679)

Il incombe aux directions métiers de limiter le traitement de données pour les personnes qui en font la demande lorsque l'un des éléments suivants s'applique :

- L'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;
- Le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;
- Le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
- La personne concernée s'est opposée au traitement, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

Lorsque le traitement a été limité, ces données ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre.

La personne qui a obtenu la limitation du traitement est informée par le DPD avant que la limitation du traitement ne soit levée.

Directive DRO_07 : Notifier aux destinataires les modifications apportées aux données suite aux demandes des personnes concernées (art. 19 du Règlement n°2016/679)

La Direction métier concernée, avec l'appui du DPD notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

Elle fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.

Directive DRO_08 : Interdire le profilage ou les décisions individuelles automatisées d'une personne (art. 22 du Règlement n°2016/679)

Aucune direction métier n'est autorisée à mettre en œuvre des fichiers permettant de faire du profilage des salariés ou des usagers sans avoir une validation formelle de la Direction Générale des Services après avis consultatif du DPD.

4.5 Directive relative à la sécurité des données

Objectif : Le Département du Doubs s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles permettant la protection des données à caractère personnel contre les risques liés à l'usage des systèmes d'information.

Directive SSI_01 : Appliquer les mesures de sécurité définies dans la Politique de Sécurité des SI (PSSI) de la collectivité (art.24 et 32 du Règlement n°2016/679)

Les directions métiers définissent avec le RSSI les mesures techniques et organisationnelles appropriées afin de garantir, compte tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, un niveau de sécurité adapté aux risques présentés par le traitement et à la sensibilité des données à caractère personnel à protéger.

Ces mesures permettant de limiter les risques de violation de données à caractère personnel sont formalisées dans la PSSI.

L'organisme exige de ses sous-traitants qu'ils présentent des garanties suffisantes pour assurer la sécurité et la confidentialité des données à caractère personnel conformément à la politique de sécurité de l'organisme.

Pour tout nouveau projet, un dossier de sécurité est formalisé par l'équipe projet en concertation avec le RSSI et le DPD afin de déterminer les mesures de sécurité à appliquer au regard de la nature des données traitées et des risques encourus.

Pour les traitements opérationnels, des audits sont réalisés par le RSSI et le DPD selon un plan d'audit défini annuellement et un plan de correction des non-conformités constatées est mis en œuvre avec les directions concernées.

Le DPD informe le Directeur Général des Services et la Présidente du Département au travers du bilan annuel de ces activités des mesures prises pour protéger les données et les éventuelles failles de sécurité constatées lors des échanges planifiés.

4.6 Directives en cas de violation de données

Objectif : Le Département du Doubs s'engage à traiter toute violation de données à caractère personnel pour limiter son impact pour les personnes concernées et éviter que cela puisse se reproduire.

Directive VIO_01 : Formaliser la notification de violation de données à caractère personnel (art. 33 du Règlement n°2016/679)

Toute violation de données à caractère personnel doit faire l'objet d'une analyse précise de l'incident selon la procédure en vigueur au sein de l'organisme.

Cette procédure prévoit la formalisation d'un dossier de notification de la violation impliquant le RSSI, le DPD et les services impliqués dans la mise en œuvre du traitement concerné.

Le formulaire de notification de la violation est compléter dans un délai de 72h00 après identification de l'incident. La notification doit, à tout le moins :

- Décrire la nature de la violation de données à caractère personnel, y compris les catégories et le nombre de personnes concernées par la violation et les catégories et le nombre d'enregistrements de données concernées ;
- Communiquer l'identité et les coordonnées du DPD ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

- Recommander des mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données à caractère personnel ;
- Décrire les conséquences éventuelles de la violation de données à caractère personnel ;
- Décrire les mesures proposées ou prises par le responsable du traitement pour remédier à la violation de données à caractère personnel.

Le DPD conserve une trace documentaire de toute violation de données à caractère personnel, en indiquant son contexte, ses effets et les mesures prises pour y remédier.

Avant juin 2018, le Directeur Général des services pourra décider de transmettre ou non ce formulaire de notification d'une violation à la CNIL. Après juin 2018, cette notification à la CNIL est obligatoire.

Directive VIO_02 : Communiquer à la personne concernée la violation de ses données à caractère personnel (art. 34 du Règlement n°2016/679)

Lorsque la violation de données à caractère personnel porte atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée, le Directeur Général des Services, après avoir procédé à la notification prévue, communique la violation sans retard indu à la personne concernée.

La communication à la personne concernée décrit la nature de la violation des données à caractère personnel et contient au moins les informations et recommandations prévues.

La communication à la personne concernée d'une violation de ses données à caractère personnel n'est pas nécessaire si le responsable du traitement prouve, auprès de la CNIL, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données à caractère personnel concernées par ladite violation. De telles mesures de protection technologiques doivent rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

La communication à la personne concernée ne peut être retardée, limitée ou omise que pour des motifs explicitement énoncés par la CNIL ou par une loi.

5 Directives relatives au renforcement de la culture protection de la vie privée au sein de l'organisme

Objectif : Le Département du Doubs s'engage à renforcer la culture informatique et libertés au sein de tous les services de l'organisme. Elle s'engage également à s'assurer que les compétences internes soient adaptées aux enjeux réglementaires et que chaque agent soit impliqué dans la protection des données à caractère personnel.

Directive CUL_01 : Sensibiliser les agents et les élus à la culture Informatique et Libertés

Tous les agents et les élus doivent être sensibilisés sur leurs rôles et responsabilités en matière de protection des données à caractère personnel. Cette sensibilisation vise à renforcer la culture informatique et libertés au sein du Département du Doubs.

Le DPD définit le programme annuel de sensibilisation et le fait approuver par le Directeur Général des Services.

Il définit également les moyens les plus adaptés pour mettre en œuvre ce programme de sensibilisation (interventions d'experts, mise à disposition d'outils pédagogiques, ….).

Concernant les nouveaux arrivants, plusieurs réunions d'information, de sensibilisation à la Loi Informatique et Libertés et au nouveau Règlement européen n°2016/679 sont organisées dans l'année.

Le Délégué à la Protection des Données, au titre de ses missions, intervient au cours de cette journée pour présenter les fondamentaux de la protection des données à caractères personnel.

Directive CUL_02 : Former les agents et les élus sur la mise en œuvre de la politique de protection des données à caractère personnel

Le DPD définit, en accord avec le Directeur Général des Services et la direction des ressources humaines, les formations qui sont nécessaires à la mise en œuvre des directives de la présente politique.

Ces formations peuvent être de nature technique ou juridique et visent à renforcer l'appropriation des sujets informatiques et libertés par les agents et les élus de la collectivité.

Le DPD peut faire appel à des organismes spécialisés en formation pour le soutenir dans sa démarche et organiser un transfert de compétences.

6 Directives relatives à l'évolution de la politique

Objectif : Le Département du Doubs s'engage à faire évoluer la politique de protection des données à caractère personnel afin qu'elle puisse prendre en compte les évolutions réglementaires ou technologiques ainsi que les contraintes internes des services. Il s'engage également à s'assurer que les dispositifs et les procédures découlant de cette politique soient appliqués.

Directive SUI_01 : Assurer une veille juridique et technologique sur le domaine informatique et libertés

Le DPD effectue une veille tant auprès de l'autorité de contrôle qu'auprès des réseaux de professionnels de la protection des données afin de s'assurer que la politique prenne en compte les évolutions réglementaires et techniques.

La Direction de la Modernisation de l'Action Publique est également chargée de la veille notamment par le biais du service Pilotage-Evaluation-Prospective.

Le RSSI assure une veille technologique sur tous les sujets relatifs à la sécurité des systèmes d'information.

Le responsable de la sécurité des biens et des personnes s'enquiert de l'évolution des normes et règlements relatifs à son domaine d'action.

Le Directeur des Archives départementales fait connaître au DPD toute évolution pouvant conduire à des changements dans les durées de conservation des données à caractère personnel.

Toutes les évolutions de nature réglementaire ou technologique identifiées dans le cadre des activités de veille doivent faire l'objet d'une analyse d'impact sur la politique.

Le DPD se charge de proposer les ajustements nécessaires pour prendre en compte des évolutions et les fait valider par le Directeur Général des Services.

Directive SUI_02 : Contrôler régulièrement la mise en œuvre des directives de la politique

Un programme annuel d'audits de conformité à la Loi Informatique et Libertés et le cas échéant au Règlement européen n°2016/679 est planifié en tenant compte de l'état et de l'importance des processus et des traitements à auditer, ainsi que des résultats des audits précédents.

Ce programme est défini par le DPD et validé par le Directeur Général des Services et porte principalement sur :

- Le contrôle de la conformité aux exigences légales et à la Politique Générale de Protection des Données à Caractère Personnel :

- Le contrôle de l'efficacité des dispositifs de protection mis en œuvre pour assurer la protection des données à caractère personnel.

Les responsabilités et les exigences pour planifier, mener les audits, rendre compte des résultats et conserver des enregistrements sont définies dans une procédure documentée.

Le Directeur responsable du domaine audité doit assurer que des actions sont entreprises sans délai indu pour éliminer les non-conformités détectées et leurs causes.

Les résultats des audits sont signalés au directeur concerné ou au sous-traitant ainsi qu'au DPD, qui prendront les décisions qui s'imposent en fonction de la gravité des non-conformités constatées.

Directive SUI_03 : Réviser régulièrement la politique

La Politique Générale de Protection des Données à Caractère Personnel est revue périodiquement et de façon systématique en cas de changement des obligations en vigueur ou d'évolutions technologiques significatives.

Le DPD propose au Directeur Général des Services, qui décide et les valide, les modifications apportées à cette politique et aux procédures associées.

Dès que les modifications sont approuvées, l'ensemble de la documentation associée est mise à jour et ces amendements sont mis en évidence.

7 Annexe I : Glossaire

ANSSI	**Agence Nationale de la Sécurité des Systèmes d'Information**
ASIP	**Agence des Systèmes d'Information Partagés**
CIL	**Correspondant Informatique et Libertés**
CNIL	**Commission Nationale de l'Informatique et des Libertés**
DUN	**Direction des usages du Numérique**
DPD	**Délégué à la protection des données**
UE	**Union européenne**
NIR	**Numéro d'Inscription au Répertoire**
PSSI	**Politique des Systèmes de Sécurité de l'Information**
RSSI	**Responsable des Systèmes de Sécurité de l'Information**
RT	**Responsable du Traitement**
SI	**Système d'Information**
SSI	**Système de Sécurité de l'Information**

8 Annexe II : Liste des tiers autorisés

Les tiers autorisés à avoir communications de données à caractère personnel traités au sein des services du Département du Doubs sont les suivants :

- **L'administration fiscale**

  Le Trésor public (direction générale de la comptabilité publique uniquement dans les conditions fixées par les articles L.81 à L.95 du Livre des Procédures fiscales pour le recouvrement de créances fiscales ou des amendes et condamnations pécuniaires - article 90 de la loi de finances pour 1987). L'article L 1617-5 du code des collectivités territoriales a, en outre, étendu le droit de communication des comptables du Trésor pour le recouvrement des créances des collectivités locales et de leurs établissements publics.

  La direction générale des impôts ou la direction générale des douanes en vue de l'établissement de l'assiette, du contrôle, du recouvrement des impôts (articles L. 81 à L. 95 du Livre des procédures fiscales) et pour le recouvrement des créances domaniales (article L. 79 du code du domaine de l'État).

- **Les organismes sociaux**

  Les organismes débiteurs de prestations familiales ou en charge du versement du RSA dans les conditions prévues par l'article L.583-3 du code de la sécurité sociale.

  Les organismes débiteurs de prestations familiales ou les huissiers de justice au titre de leur mission de recouvrement des créances alimentaires impayées (article 7 de la loi 73-5 du 2 janvier 1973).

- **Les administrations de la justice, de la police et de la gendarmerie**

  Les magistrats, dans le cadre des dispositions des codes de procédure pénale et de procédure civile (notamment les articles 56, 57, 92 à 97 du code de procédure pénale).

  Le procureur de la République, à la demande de l'huissier de justice porteur d'un titre exécutoire et au vu d'un relevé certifié sincère des recherches infructueuses qu'il a tentées pour l'exécution (article 40 de la loi n° 91-650 du 9 juillet 1991).

  Les officiers de police judiciaire de la police et de la gendarmerie nationale agissant en flagrant délit, sur commission rogatoire ou dans le cadre d'une enquête préliminaire (articles 57-1, 60-1 et 76-3 du code de procédure pénale) y compris par voie informatique ou télématique (article 60-2 du même code).

  Les bureaux d'aide judiciaire afin de demander la vérification des ressources en vue de l'attribution de l'aide judiciaire (loi n° 72-11 du 3 janvier 1972 modifiée par la loi du 31 décembre 1982 relative à l'aide judiciaire).

- **Les autres administrations bénéficiant d'un droit de communication**

  Les services extérieurs du travail et de l'emploi dans le cadre du contrôle de la recherche d'emploi (ordonnance n°86-1286 du 20 décembre 1986, articles L. 351-1 et R. 351-32 du code du travail).

  Les services en charge de la gestion des allocations supplémentaires prévues aux articles L 815-2 et 3 du code de la sécurité sociale (fonds de solidarité vieillesse et fonds spécial d'invalidité) pour le recouvrement sur la succession des héritiers (articles L. 815-12 et L. 815-15 du code de la sécurité sociale).

9 Annexe III : Catégories de données

La Commission Nationale Informatique et Libertés (CNIL) propose de classer les données à caractère personnel en trois catégories :

- Les données dites « courantes »,
- Les données « sensibles »,
- Les données considérées comme « sensibles au sens de la Loi Informatique et Libertés » (art. 8 de la Loi).

Le tableau ci-dessous précise les types de données par catégorie :

Types de DCP	Catégories de DCP
DCP courantes	Etat civil, identité, données d'identification
	Vie personnelle (habitude de vie, situation familiale, hors données sensibles, très sensibles ou dangereuses, …)
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, ..)
	Données de connexion (adresses IP, journaux d'évènements, …)
	Données de localisation, (déplacements, données GPS, GSM, …)
DCP sensibles	Numéro de sécurité sociale (NIR) Données biométriques
	Données bancaires
DCP très sensibles au sens de la loi	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou la vie sexuelle.