Offre d'ingénierie territoriale ATESART : « Protection des données personnelles / mutualisation du Délégué prévu par le Règlement européen »

I) Contexte de la proposition

Les articles 37 à 39 du « Règlement Général pour la Protection des Données » (RGPD [*]) définissent le rôle et les compétences attendues du **« Délégué à la Protection des Données » [*]**, dont la nomination est **obligatoire** dans toutes les collectivités territoriales et autres organisations publiques (ainsi que pour la plupart des entreprises privées).

Cette nomination s'inscrit dans une volonté de responsabilisation de tous les « responsables de traitements » [*], qui sont tenus à partir du 25 mai 2018 de **formaliser et mettre en œuvre une politique pérenne de protection des données personnelles** qu'ils collectent auprès du public en général (usagers, clients, agents, employés, etc.).

Compte tenu de l'indépendance requise et des compétences relativement rares à mobiliser de façon discontinue mais permanente dans chaque collectivité ou établissement public, la **mutualisation du/des délégué(s)** – prévue par le RGPD et encouragée notamment par la CNIL et par le Parlement – doit permettre à l'ensemble de la sphère territoriale de mieux absorber l'impact de cette nouvelle réglementation.

Ce ou ces délégué(s) devront faire face, avec les responsables de traitements, à trois défis :

1. **D'ici le 25 mai 2021**, sensibiliser et former tous les agents territoriaux impliqués, engager l'inventaire et sa hiérarchisation, lancer les analyses d'impact éventuellement nécessaires, vérifier et au besoin réviser les contrats et conventions, revoir/adapter les procédures, [commencer à] assurer la formalisation et la traçabilité…
2. **Dans la durée**, assurer la veille et actualiser régulièrement les connaissances des agents concernés, tenir l'ensemble des dispositions et de la documentation à jour en fonction des évolutions et des nouveaux traitements, auditer régulièrement les pratiques et les outils utilisés…
3. **Répondre aux sollicitations aléatoires** : incidents, réagir à une attaque ou à une « fuite » de données, traiter les demandes d'usagers ou d'agents, etc.

➔ **Le Département de la Sarthe**

➔ Acteur « de confiance », par son expérience de la mutualisation numérique *(infrastructures de réseaux, plateformes de dématérialisation, données cadastrales et géographiques, etc.)*,

➔ Lui-même conscient des difficultés que peut entraîner le RGPD pour les collectivités territoriales et établissements sarthois,

➔ A pris l'initiative d'élaborer une offre d'ingénierie adaptée à la **mutualisation des « Délégués à la Protection des Données »**, qui sera portée par « l'Agence des Territoires » (ATESART).

II) Objectif de l'offre

L'offre ATESART vise à :

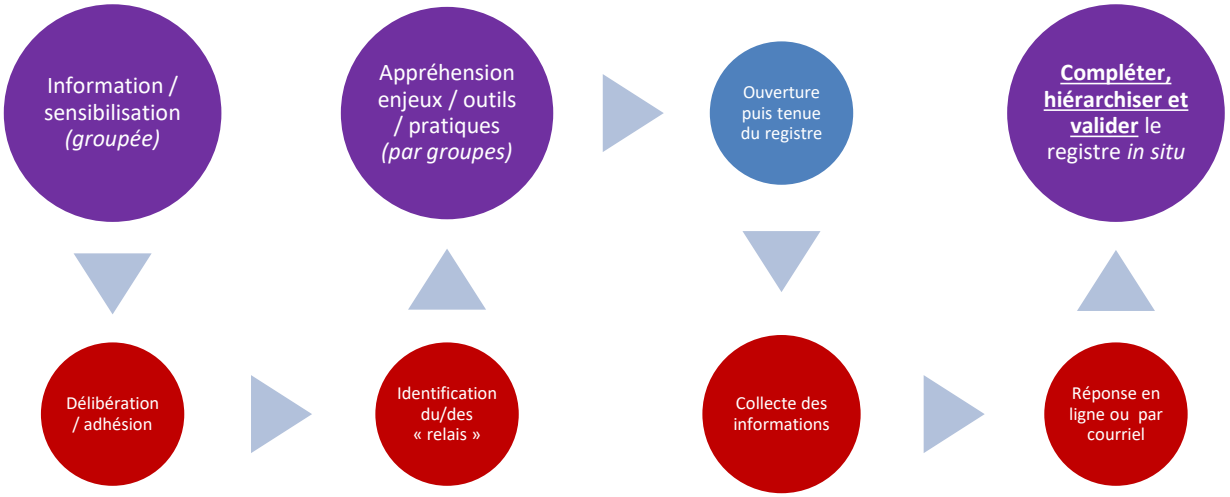
- **Accompagner les collectivités petites et moyennes** dans leur « conformité au RGPD, **en leur proposant de désigner un Délégué mutualisé, dans le respect de leurs spécificités et de leurs contraintes** (cette offre s'adresse aussi aux EPCI et syndicats[1]),
- Assurer une prestation de service adaptée, portée par **une équipe dédiée et spécifiquement qualifiée,**
- Faire bénéficier les adhérents d'**une offre péréquée au plus juste**, grâce notamment :
    - à la prise en compte de la taille des collectivités/EPCI, étroitement corrélée avec le nombre de traitements et la complexité de l'organisation (mais aussi aux compétences internes mobilisables),
    - à la mise à profit du délai d'adaptation au RGPD de trois ans accordé par la CNIL, soit jusqu'au 24 mai 2021,
    - au distinguo tarifaire entre la mise en œuvre (les deux premières années, plus chargées) et un régime de croisière (les années suivantes, une fois le rattrapage effectué),
    - à trois niveaux et modalités d'intervention :
        - information/sensibilisation/appréhension des outils en regroupement (par « bassins » géographiques ou au Mans, selon le public visé),
        - échanges et travail majoritairement à distance (par messagerie et autres plateformes à définir),
        - et quelques interventions *in situ* pour auditer, discuter et valider les constats et les préconisations, etc.
    - à un forfait particulièrement bas, assorti de la possibilité de tenir compte d'événements ou de besoins exceptionnels qui seront chiffrés en toute transparence « sur devis »,
    - à un « droit de tirage » forfaitisé (nombre de jours *in situ*, nombre d'études d'impact) pouvant éventuellement être reporté sur l'année suivante si non totalement consommé,
    - et enfin à la mutualisation des outils et des pratiques, ainsi qu'à la capitalisation des connaissances et « l'industrialisation » rendues possibles par les similitudes inévitables à une certaine échelle (même éditeur, traitements et/ou configurations matérielles similaires…).

[1] **Les CCAS ou CIAS** ne peuvent statutairement pas adhérer à l'Agence. Toutefois, si – comme c'est le plus souvent le cas – ils dépendent pour l'informatique de leur mairie ou intercommunalité de rattachement, il suffira que le CCAS et la mairie (ou le CIAS et la communauté de communes) passent une convention décrivant la nature et les conditions de traitement définies par chacune des deux parties pour protéger les données personnelles, et qu'ils y insèrent une clause de prise en charge du Délégué par la collectivité.
Indépendamment du choix du Délégué, dans tous les cas de figure le RGPD imposera cette contractualisation explicite CCAS/CIAS – Commune/Communauté, du fait des personnalités juridiques distinctes.
Par ailleurs, même si les moyens sont apportés par les collectivités, **les écoles, juridiquement indépendantes de l'autorité territoriale, ne rentrent pas dans le champ d'intervention direct** de votre futur Délégué. Néanmoins, s'il y a transmission ou accès à des données personnelles, des conventions de co-traitance ou de sous-traitance devront être élaborées conjointement avec le DASEN (qui est le « Responsable de traitement « pour toutes les écoles du département) ou son représentant/Délégué.

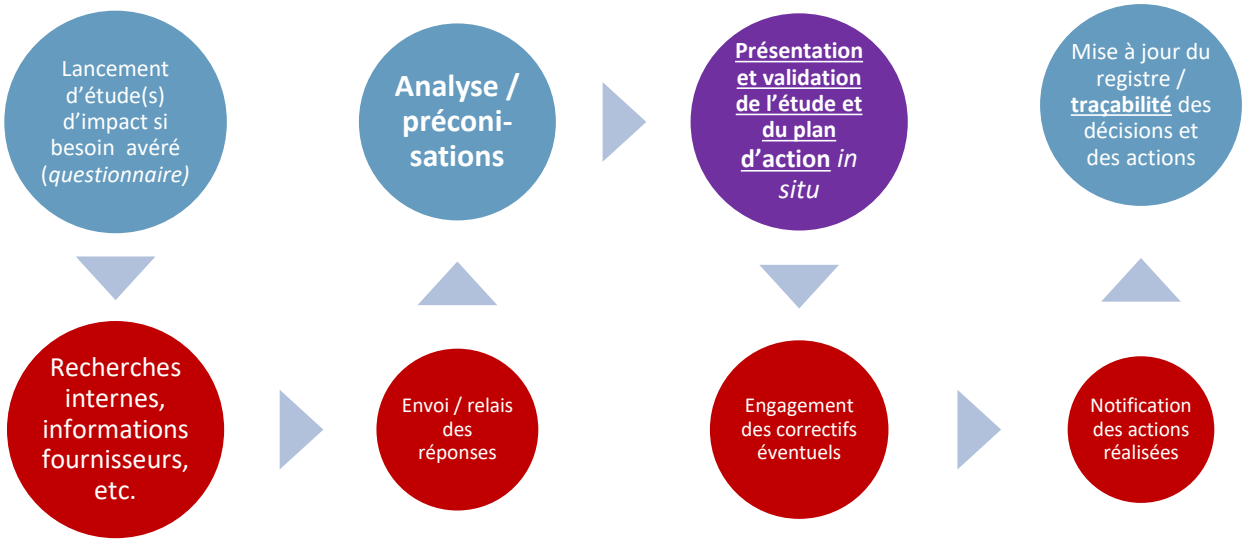
III) « Comment cela va se passer ? » : aperçu du mode opératoire

Mise en oeuvre

Première étape : *information, adhésion, appréhension des enjeux et des outils, ouverture du « registre »…*



Deuxième étape facultative *(uniquement si données sensibles) : étude d'impact et mesures correctives*



Interne ATESART

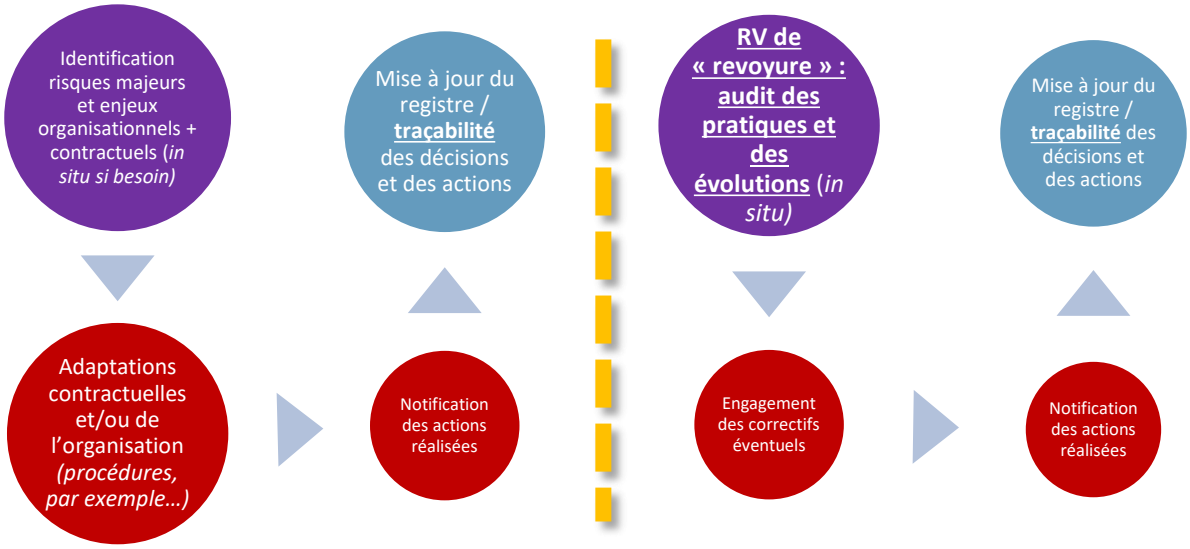
Travail en commun

- *soit en regroupement*
- *soit in situ*

Interne collectivité

Mise en œuvre (suite et fin)

Troisième étape : *revue procédures et contrats*



Travaux récurrents a minima

Ultérieurement : *« revoyure » et audit annuel*

IV) Nature et tarif des prestations prévues par l'offre ATESART[2]

	Années 1 et 2 ***Vous bénéficiez de :***	**Années suivantes** ***Vous bénéficiez de :***
Dans tous les cas de figure	1. Accès à la veille, et à toutes les réunions en regroupement 2. Ouverture et tenue à jour du registre et des éléments de traçabilité requis par le RGPD et/ou la CNIL / révision des contrats et des mentions légales 3. Accès aux outils/plateformes qui seront mis en place (registre, traçabilité, informations partagées…) 4. Centralisation et suivi des contacts : usagers, autorités compétentes, etc. 5. Conseil, traitement à distance (messagerie, etc.) de questions courantes	1. Accès, tenue à jour, centralisation et suivi des contacts, conseil, traitement à distance : idem années 1 et 2 2. « Revoyure » : revue des évolutions, audit des pratiques, préconisations, prise en compte de nouveaux traitements, transfert de compétences/connaissances envers les nouveaux agents, etc.
PLUS, si population < 1000 habitants	1. Maximum **1 jour *in situ*** (fractionnable par ½ journée de 3h, ou ¼ journée d'1h30 hors déplacement) 2. Maximum **1 étude d'impact** selon nécessité/ sensibilité des données.	1. Maximum **0,5 jour *in situ*** (fractionnable par ¼ journée d'1h30 hors déplacement)
OU BIEN, si population ≥ 1000 habitants	1. Maximum **2 jours *in situ*** (fractionnable par ½ journée de 3h, ou ¼ journée d'1h30 hors déplacement) 2. Maximum **2 études d'impact** selon nécessité / sensibilité des données.	1. Maximum **1 jour *in situ*** (fractionnable par ½ journée de 3h, ou ¼ journée d'1h30 hors déplacement) 2. Maximum **1 étude d'impact** supplémentaire, selon nécessité.
Forfait annuel (quelle que soit la population, si < 40 000 habitants)	**100 € minimum** **< 0,90 €/habitant** **< 2500 € maximum**	**75 € minimum** **< 0,50 €/habitant** **< 1500 € maximum**
Dépassement, CCAS/CIAS…[3]	**Sur devis.** Pour info, la journée (fractionnable ½ et ¼) est facturée **365 €**	

[2] Descriptif et tarif basés sur « l'état de l'art » connu à la date de rédaction du présent document. Ils restent susceptibles d'évoluer en fonction d'obligations nouvelles, ou encore du fait d'évolutions sociétales, comportementales ou techniques à ce jour imprévisibles.

[3] Les forfaits prévoient les opérations de mise à niveau RGPD « normales », mais ils excluent un éventuel rattrapage dû à la méconnaissance de la Loi de 1978 modifiée (absence de déclarations), ou encore le rôle de délégué pour le compte d'un établissement juridiquement distinct.

Attention !

1. Obligatoire dans les collectivités et EPCI ou autres établissements, **la nomination d'un Délégué n'entraîne pas de transfert de responsabilités** : si celui-ci conseille et émet des préconisations, c'est l'organisme qui agit en toute souveraineté et encadre ses agents, demeurant donc seul « Responsable de traitement » [*].
2. **Le Délégué ne peut rien faire tout seul** : l'identification et la réduction des risques impliquent, avec le soutien des élus, la contribution et l'implication de tous les services, responsables et agents concernés (ainsi que, via la collectivité, des sous-traitants et prestataires éventuels). Élus, responsables, agents et tous autres intervenants peuvent aussi solliciter/alerter spontanément le Délégué qui DOIT centraliser ces contacts.

[*] Glossaire

- Commission Nationale Informatique et Libertés (CNIL) : autorité française chargée de faire respecter et de contrôler la protection des données personnelles traitées par les entités publiques et privées – en capacité, le cas échéant, de sanctionner les écarts : non-respect du droit, « fuites », etc. Elle émet également des prescriptions et des conseils en direction des « Responsables de traitement », et propose différents outils et modèles indicatifs adaptés aux différents acteurs.
- Délégué à la Protection des Données personnelles (DPD ou DPO) : personne physique ou morale désignée par le Responsable de traitement, « à l'abri des conflits d'intérêts » *[donc non impliquée dans la mise en œuvre des traitements soumis à son contrôle, ni hiérarchiquement rattachée au(x) responsable(s) de cette mise en œuvre]*, disposant d'un niveau d'expertise et de moyens suffisants pour exercer ses missions.
- Données à caractère personnel (ou « données personnelles ») : toute information permettant d'identifier, directement ou indirectement (même par croisement), des personnes physiques.
- Étude d'impact : pour les traitements les plus « sensibles » (de par la nature des données recueillies/conservées), il est nécessaire d'analyser en détail les risques encourus et de définir les palliatifs adoptés en conséquence (outils et démarche de sécurité spécifiques par exemple). Le tout doit être formalisé et conservé, en s'inspirant si possible de normes/méthodes reconnues (ISO, NF…).
- Loi « Informatique et Libertés » : adoptée le 6 janvier 1978 puis plusieurs fois révisée et complétée, cette réglementation pionnière connaît un « toilettage » important pour s'adapter au Règlement européen, dont elle doit préciser certaines modalités. À date, la révision votée le 14 mai 2018 et non encore publiée contient 19 renvois à de futurs décrets.
- Règlement européen sur la protection des données personnelles (RGPD) : publié le 27 avril 2016, ce Règlement est entré en vigueur le **25 mai 2018.** La CNIL a concédé un **délai d'adaptation maximum de 3 ans**.
- Registre : inventaire des « traitements » et de leurs caractéristiques tenu à jour par le Responsable de traitement (ou par son Délégué lorsqu'il existe). C'est le principal – mais pas le seul ! – moyen de traçabilité prévu par le Règlement : sa forme et son contenu sont libres, mais la CNIL propose un modèle indicatif dont une version simplifiée s'adresse aux PME et aux « petites » collectivités.
- Responsable de traitement : toute personne morale qui collecte et/ou traite des données à caractère personnel. Dans notre cas, il s'agit donc de **la collectivité territoriale ou l'établissement public « représenté(e) par » son Maire/Président** (aucune délégation possible).
- Traitement : toute collecte, manipulation ou conservation de données est susceptible de constituer un « traitement ». Dans notre cas, **seuls les traitements de données personnelles, informatisés ou non, sont pris en compte**, en s'attachant aux finalités poursuivies : « gestion du service périscolaire », « facturation de l'assainissement », « tenue du fichier électoral »… *(plutôt que « logiciel XXX », « module web YYY », etc.)*.