VILLE DE PARIS

**Concours EXTERNE et 3ème CONCOURS**
pour l'accès au corps des
**ATTACHE·E·S D'ADMINISTRATIONS PARISIENNES**
ouverts à partir du 07 février 2022
**pour 26 postes (externe) et 1 poste (3ème concours)**

**1ère épreuve écrite**
**NOTE**

**Epreuve de rédaction d'une note** à partir d'un dossier relatif aux problèmes politiques, économiques, culturels et sociaux du monde contemporain permettant de vérifier les qualités de réflexion, d'analyse, de synthèse et de rédaction du·de la candidat·e.

**Coefficient : 4 - Durée 04h00**

**Le dossier comporte 35 pages et 11 documents**

**SUJET : En vous aidant des documents joints ainsi que de vos connaissances, vous rédigerez une note sur les enjeux auxquels sont confrontées les collectivités territoriales en matière de protection et de sécurité des données personnelles et les moyens d'y répondre.**

- **p. 2 à 7 (document 1)** : articles ou extraits d'articles du Règlement européen sur la protection des données (RGPD) – 6 pages
- **p. 8 (document 2)** : articles ou extraits d'article de la loi informatique et libertés – 1 page
- **p. 9 à 11 (document 3)** : fiche vidéoprotection - vidéosurveillance sur la voie publique – CNIL 03 décembre 2019 – 3 pages
- **p. 12 à 14 (document 4)** : fiche vidéoprotection - vidéosurveillance au travail – CNIL 27 novembre 2019 – 3 pages
- **p. 15 à 17 (document 5)** : extrait du rapport d'activité 2020 de la CNIL – 3 pages
- **p. 18 et 19 (document 6)** : extrait du site internet de la CNIL : sanction de 400 000 euros à l'encontre de la RATP – 04 novembre 2021 - 2 pages
- **p. 20 et 21 (document 7)** : extrait de « données personnelles info » - Secrétariat Général de la Ville de Paris (novembre 2018) - 2 pages
- **p.22 (document 8)** : extrait du site de l'Agence nationale de sécurité des systèmes d'information (ANSSI) : présentation du guide dédié aux collectivités territoriales – 1 page
- **p. 23 et 24 (document 9)** : extrait du site de l'ANSSI – présentation du guide « Anticiper et gérer sa communication de crise cyber » (décembre 2021) – 2 pages
- **p.25 à 27 (document 10)** : article de La Gazette des communes « cyberattaques : les collectivités de plus en plus transparentes » - 24 février 2021 – 3 pages
- **p. 28 à 35 (document 11)** : charte de la donnée de Nantes métropole – 8 pages

**RAPPEL : aucun nom, prénom, signature ou signe distinctif (supérieur hiérarchique, initiales quelles qu'elles soient, numéro de téléphone ou adresse de service, même fictifs,...) ne doivent figurer dans le corps (ou le timbre) de votre composition sous peine d'exclusion du concours.**

**Les feuilles de brouillon ne seront en aucun cas prises en compte.**

**Document 1 : articles ou extraits d'articles issus du règlement Union Européenne 2016/679 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 (RGPD).**

Article 5 - Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré (...) comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (...), pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Article 6 - Licéité du traitement (extraits)

1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

e) le traitement est nécessaire 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;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Article 13 - Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée

1. Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale (...) ;

2. En plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :

a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données;

c) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point a), ou sur l'article 9, paragraphe 2, point a), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci;

d) le droit d'introduire une réclamation auprès d'une autorité de contrôle;

e) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données;

f) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

3. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2.
4. Les paragraphes 1, 2 et 3 ne s'appliquent pas lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations.

Article 30 - Registre des activités de traitement

1. Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;

e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;

g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

2. Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.
4. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.
5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées (...).

Article 33 - Notification à l'autorité de contrôle d'une violation de données à caractère personnel

En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

La notification visée au paragraphe 1 doit, à tout le moins:

a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

Article 37 - Désignation du délégué à la protection des données

Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

(...)

Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

Dans les cas autres que ceux visés au paragraphe 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.

Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

Article 39 - Missions du délégué à la protection des données

Les missions du délégué à la protection des données sont au moins les suivantes:

a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;

b) contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;

c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35;

d) coopérer avec l'autorité de contrôle;

(...)

Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

**<u>Document 2</u> : articles ou extraits d'articles issus de la loi 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.**

Article 1 (extrait)
L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Article 8

I. - La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 du 27 avril 2016. Elle exerce les missions suivantes :

1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations et peut, à cette fin, apporter une information adaptée aux collectivités territoriales, à leurs groupements et aux petites et moyennes entreprises ;

2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France.

A ce titre :

(...)

b) Elle établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants. Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables de traitement et à leurs sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques, notamment des mineurs. Elle homologue et publie les méthodologies de référence destinées à favoriser la conformité des traitements de données de santé à caractère personnel. Elle prend en compte, dans tous les domaines de son action, la situation des personnes dépourvues de compétences numériques, et les besoins spécifiques des collectivités territoriales, de leurs groupements et des microentreprises, petites entreprises et moyennes entreprises ;

(...)

d) Elle traite les réclamations, pétitions et plaintes introduites par une personne concernée ou par un organisme, une organisation ou une association, examine ou enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire ;

(...)

g) Elle peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétaire général, dans les conditions prévues à l'article 19 de la présente loi, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions.

**Document 3 : La vidéosurveillance – vidéoprotection sur la voie publique – fiche publiée par la CNIL le 03 décembre 2019**

Le nombre de caméras filmant la voie publique a fortement augmenté ces dernières années, notamment sous l'impulsion des pouvoirs publics, pour lutter contre l'insécurité. Des textes spécifiques encadrent ces dispositifs soumis à une autorisation du préfet. Quelles sont les règles ? Quels sont les droits des personnes filmées ?

Des caméras peuvent être installées sur la voie publique pour prévenir des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants, des actes de terrorisme, dans les conditions prévues par l'article L.251-2 du code de la sécurité intérieure.

Ces dispositifs peuvent également permettre de constater des infractions aux règles de la circulation, réguler les flux de transport, protéger des bâtiments et installations publics et leurs abords, ou encore d'assurer la sécurité d'installations utiles à la défense nationale, prévenir des risques naturels ou technologiques, faciliter le secours aux personnes ou encore lutter contre les incendies et assurer la sécurité des installations accueillant du public dans les parcs d'attraction.

**Qui peut filmer la rue ?**

Seules les **autorités publiques** (les mairies notamment) peuvent filmer la voie publique.

Ni les entreprises, ni les établissements publics ne peuvent filmer la voie publique. Ils peuvent seulement filmer les **abords immédiats** de leurs bâtiments et installations (la façade extérieure par exemple mais pas la rue en tant que telle) dans les **lieux susceptibles d'être exposés à des actes de terrorisme.**

Les particuliers ne peuvent filmer que **l'intérieur de leur propriété.** Ils ne peuvent pas filmer la voie publique, y compris pour assurer la sécurité de leur véhicule garé devant leur domicile.

Quelles garanties pour la protection de la vie privée ?

Ces caméras ne doivent **pas permettre de visualiser l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées.** Des procédés de masquage irréversible de ces zones doivent être mis en œuvre.

**Qui peut consulter les images ?**

La mise en œuvre d'un système de vidéoprotection doit satisfaire à l'obligation de sécurisation des données, qui pèse sur les responsables de traitements. En conséquence, le visionnage des images ne peut être opéré que par les personnes spécifiquement et individuellement habilitées (par exemple : les agents du centre de supervision urbain d'une commune peuvent visionner les images enregistrées). Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un système de vidéoprotection.

L'article R.252-11 du CSI prévoit que le titulaire de l'autorisation tient un registre mentionnant notamment les enregistrements réalisés, la date de destruction des images, le cas échéant, la date de leur transmission au parquet.

**Pendant combien de temps conserver les images ?**

La durée de conservation des images doit être **proportionnée** et **correspondre à l'objectif pour lequel le système de vidéoprotection est installé**. En règle générale, quelques jours suffisent pour effectuer des vérifications, par exemple à la suite d'un incident.

La durée jugée proportionnée, dans chaque cas, est précisée dans l'arrêté préfectoral d'autorisation, et ne saurait excéder un mois (art. L.252-3 du CSI).

**Quelle information ?**

Les personnes filmées dans un espace public doivent en être informées, au moyen de panneaux affichés en permanence, de façon visible, dans les lieux concernés, et doivent être compréhensibles par tous les publics. Ils doivent a minima comporter, outre un pictogramme représentant une caméra qui indique que le lieu est placé sous vidéoprotection :

- les finalités du traitement installé ;
- la durée de conservation des images ;
- le nom ou la qualité et le numéro de téléphone du responsable/du délégué à la protection des données (DPO) ;
- l'existence de droits « Informatique et libertés » ;
- le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL), en précisant ses coordonnées.

Afin que les panneaux affichés restent lisibles, l'intégralité des informations qui doit être portée à la connaissance du public peut l'être par d'autres moyens, notamment par le biais d'un site internet. Ces autres informations sont, notamment :

- la base légale du traitement ;
- les destinataires des données personnelles, y compris ceux établis en dehors de l'UE ;
- enfin, s'il y en a, les informations complémentaires qui doivent être portées à l'attention de la personne (prise de décision automatisée, profilage, etc.).

Ces informations sont prévues par l'article 13 du RGPD et l'article 104 de la loi « Informatique et Libertés ».

**Quelles formalités ?**

- Auprès de la préfecture du département

Le code de la sécurité intérieure prévoit que l'installation d'un système de vidéoprotection suppose de demander l'autorisation au préfet territorialement compétent (par ex. : à Paris, il s'agit du préfet de police), obligation maintenue par les textes européens et la loi du 20 juin 2018.

En conséquence, si les caméras filment la voie publique (rues), le dispositif doit être autorisé par le préfet (le préfet de police à Paris) après avis d'une commission départementale présidée par un magistrat. L'autorisation est valable 5 ans et renouvelable.

Le formulaire peut être retiré auprès des services de la préfecture du département ou téléchargé sur le site internet du ministère de l'Intérieur. Il peut également être rempli en ligne.

La demande d'autorisation doit être déposée par l'autorité décidant de la mise en oeuvre du dispositif, éventuellement accompagnée dans cette procédure par son prestataire technique.

En cas d'urgence et de risques particuliers d'actes de terrorisme, une procédure d'autorisation provisoire (4 mois) est prévue.

Cette procédure s'applique aussi lorsque les autorités sont informées de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens.

Enfin, le préfet peut demander à une commune d'installer un système de vidéoprotection pour prévenir des actes de terrorisme et pour protéger les abords d'établissements vitaux pour le pays (centrales nucléaires, réseaux d'eau potable, gares, aéroports...). Le conseil municipal doit en délibérer dans un délai de 3 mois

- Auprès de la CNIL

Effectuer une analyse d'impact sur la protection des données (AIPD) est une obligation nouvelle en droit français, qui découle directement des textes européens, si un traitement est susceptible d'engendrer « un risque élevé pour les droits et libertés des personnes physiques ».

Dès lors que la mise en œuvre d'un dispositif de vidéoprotection conduit à « la surveillance systématique à grande échelle d'une zone accessible au public », type de traitements expressément mentionné à l'article 35.1 du RGPD comme susceptible de présenter un tel risque élevé, une AIPD doit être effectuée. Par ce biais, une évaluation de la nécessité et de la proportionnalité du dispositif envisagé, au regard des finalités poursuivies, sera opérée.

**Quels recours ?**

Si un dispositif de vidéoprotection ne respecte pas ces règles, vous pouvez saisir :

- le service des plaintes de la Commission nationale de l'informatique et des libertés

La CNIL a en effet la faculté de s'assurer que les systèmes de vidéoprotection sont mis en oeuvre conformément au cadre légal applicable. Elle peut procéder à des contrôles. Les investigations de la Commission peuvent porter sur l'existence et la validité de l'autorisation préfectorale concernant le dispositif, sa finalité, son caractère proportionné, les modalités d'information et de droit d'accès des personnes filmées, la qualité des personnels autorisés à visualiser les images, les mesures permettant d'assurer la sécurité du traitement (notamment la nécessité de tenir un registre des consultations), la durée de conservation des images.

Le constat de manquements peut conduire la CNIL à adresser à l'organisme concerné une mise en demeure visant à ce que soient prises les mesures permettant au système de vidéoprotection d'être conforme aux règles de protection des données. En cas notamment de manquement grave ou persistant, ou d'organisme de mauvaise foi, la Commission peut également décider d'adopter une des sanctions prévues par les textes (rappel à l'ordre, limitation temporaire ou définitive du traitement, sanction pécuniaire, etc.).

- les services de la préfecture ;
- les services de police ou de gendarmerie ;
- le procureur de la République.

**Document 4 - La vidéosurveillance – vidéoprotection au travail – fiche publiée par la CNIL le 27 novembre 2019**

Les caméras de surveillance sont aujourd'hui largement utilisées sur les lieux de travail. Si ces outils sont légitimes pour assurer la sécurité des biens et des personnes, ils ne peuvent pas conduire à placer les employés sous surveillance constante et permanente. Quelles règles les employeurs doivent-ils respecter ? Quels sont les droits des employés ?

**À retenir**

Un employeur ne peut pas installer des caméras dans ses locaux sans définir un objectif, qui doit être légal et légitime. Par exemple, des caméras peuvent être installées sur un lieu de travail à des fins de sécurité des biens et des personnes, à titre dissuasif ou pour identifier les auteurs de vols, de dégradations ou d'agressions.

Quelles précautions prendre lors de l'installation du dispositif ?

Les caméras peuvent être installées au niveau des **entrées et sorties des bâtiments**, des **issues de secours** et des **voies de circulation**. Elles peuvent aussi filmer les zones où de la marchandise ou des biens de valeur sont entreposés.

Elles ne doivent **pas filmer les employés sur leur poste de travail**, sauf circonstances particulières (employé manipulant de l'argent par exemple, mais la caméra doit davantage filmer la caisse que le caissier ; entrepôt stockant des biens de valeurs au sein duquel travaillent des manutentionnaires).

En effet, sur le lieu de travail comme ailleurs, les employés ont **droit au respect de leur vie privée**.

Les caméras ne doivent **pas non plus filmer les zones de pause ou de repos des employés, ni les toilettes**. Si des dégradations sont commises sur les distributeurs alimentaires par exemple, les caméras ne doivent filmer que les distributeurs et pas toute la pièce.

Enfin, elles ne doivent pas **filmer les locaux syndicaux** ou des représentants du personnel, ni leur accès lorsqu'il ne mène qu'à ces seuls locaux.

Si les images sont accessibles à distance, depuis internet sur son téléphone mobile par exemple, il faut sécuriser cet accès.

**La possibilité de regarder les images sur tablette ou téléphone ne doit pas conduire à surveiller ses employés pour leur faire des remarques sur la qualité du travail.** L'accès à distance doit être sécurisé (mot de passe robuste, connexion https, etc). Enfin, l'enregistrement du son, en plus des images, est réservé à des situations particulières et ne doit pouvoir être déclenché qu'à l'initiative d'un l'employé en cas d'événement le justifiant (en cas d'agression par exemple).

**Qui peut consulter les images ?**

Seules les personnes habilitées par l'employeur, dans le cadre de leurs fonctions, peuvent visionner les images enregistrées (par exemple : le responsable de la sécurité de l'organisme). Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un système de vidéosurveillance. L'accès aux images doit être sécurisé pour éviter que tout le monde ne puisse les visionner.

**Pendant combien de temps conserver les images ?**

L'employeur doit définir la durée de conservation des images issues des caméras.

Cette durée doit être en lien avec l'objectif poursuivi par les caméras. En principe, cette durée n'excède pas un mois. En règle générale, conserver les images quelques jours suffit, sauf circonstances exceptionnelles à effectuer les vérifications nécessaires en cas d'incident et permet d'enclencher d'éventuelles procédures disciplinaires ou pénales. Si de telles procédures sont engagées, les images sont alors extraites du dispositif (après consignation de cette opération dans un cahier spécifique) et conservées pour la durée de la procédure.

La durée maximale de conservation des images ne doit pas être fixée en fonction de la seule capacité technique de stockage de l'enregistreur.

Quelle information ?

Les personnes concernées (employés et visiteurs) doivent être informées, au moyen de panneaux affichés en permanence, de façon visible, dans les lieux concernés, qui comportent a minima, outre le pictogramme d'une caméra indiquant que le lieu est placé sous vidéoprotection :

- les finalités du traitement installé ;
- la durée de conservation des images ;
- le nom ou la qualité et le numéro de téléphone du responsable/du délégué à la protection des données (DPO) ;
- l'existence de droits « Informatique et Libertés » ;
- le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL), en précisant ses coordonnées.

Afin que les panneaux affichés restent lisibles, l'intégralité des informations qui doit être portée à la connaissance du public peut l'être par d'autres moyens, notamment par le biais d'un site internet. Ces autres informations sont, notamment :

- la base légale du traitement ;
- les destinataires des données personnelles, y compris ceux établis en dehors de l'UE ;
- enfin, s'il y en a, les informations complémentaires qui doivent être portées à l'attention de la personne (prise de décision automatisée, profilage, etc.).

Quelles formalités ?

Les formalités à accomplir peuvent varier en fonction des lieux qui sont filmés.

- Lieu non ouvert au public

Si les caméras filment un lieu non ouvert au public (lieux de stockage, réserves, zones dédiées au personnel comme le fournil d'une boulangerie), aucune formalité auprès de la CNIL n'est nécessaire.

Si l'organisme qui a mis en place des caméras a désigné un délégué à la protection des données (DPO), ce dernier doit être associé à la mise en œuvre des caméras. Si le dispositif doit faire l'objet d'une analyse d'impact (AIPD), le DPO doit y être associé.

L'employeur doit inscrire ce dispositif de vidéosurveillance dans le registre des traitements de données qu'il doit tenir.

- Lieu ouvert au public

Si les caméras filment un lieu ouvert au public (espaces d'entrée et de sortie du public, zones marchandes, comptoirs, caisses), le dispositif doit être autorisé par le préfet du département (le préfet de police à Paris). Le formulaire peut être retiré auprès des services de la préfecture du

département ou téléchargé sur le site du ministère de l'Intérieur. Il peut également être rempli en ligne sur le site via un formulaire dédié.

Dès lors qu'un dispositif de vidéoprotection conduit à la « surveillance systématique à grande échelle d'une zone accessible au public », une AIPD doit être effectuée. Elle permettra notamment d'évaluer la nécessité et la proportionnalité du dispositif envisagé, au regard des finalités poursuivies.

- Auprès des instances représentatives du personnel

**Les instances représentatives du personnel doivent être informées et consultées** avant toute décision d'installer des caméras.

## COVID-19 : la protection des libertés et des données personnelles au cœur des débats publics

Dans le contexte de la crise sanitaire, l'utilisation des technologies de communication à distance et de dispositifs de surveillance pour essayer de ralentir l'épidémie ou pour s'adapter aux mesures de distanciation physique n'a cessé d'augmenter. Face à la multitude d'initiatives, la CNIL a su mobiliser ses deux piliers, l'accompagnement et la chaîne répressive, tout en restant à l'écoute de ses publics.

Tout au long de l'année, la CNIL a ainsi conseillé activement les pouvoirs publics afin de contribuer à garantir que la mise en œuvre des systèmes d'information sanitaires (StopCovid-TousAntiCovid, SI-DEP, Contact Covid, Vaccin Covid) soit respectueuse des droits des personnes concernées. La participation de la CNIL à la coopération européenne a également permis d'apporter des positions communes importantes, notamment sur les applications de suivi de contact ou le traitement de données de santé à des fins de recherche scientifique dans la lutte contre le virus.

Afin de répondre à un grand nombre d'interrogations des particuliers et des professionnels, la CNIL a su proposer sur son site des contenus inédits tels que ceux publiés sur la continuité pédagogique, le télétravail, la distribution de masques par les collectivités ou encore TousAntiCovid.

Par ailleurs, la CNIL a priorisé le traitement des plaintes liées à la COVID-19 ainsi que les contrôles des dispositifs mis en œuvre, et a mené des contrôles sur des sujets aussi différents que les cahiers de rappels ou l'usage des drones équipés de caméras pour surveiller le respect des mesures de confinement.

## Nouvelles règles pour les cookies : un tournant pour les internautes et le secteur de la publicité en ligne

En publiant ses lignes directrices modificatives et sa recommandation le 1er octobre 2020, la CNIL a rappelé deux règles fondamentales : l'internaute doit être informé, de façon claire et synthétique de ce à quoi servent les traceurs et il doit pouvoir refuser les cookies aussi facilement que les accepter.

Cette évolution des règles applicables a été accompagnée de la publication de nombreuses fiches pour les professionnels (mettre son site en conformité, les solutions pour outils de mesure d'audience, questions-réponses, etc.) et pour les particuliers (les changements au quotidien, les conseils pour maîtriser son navigateur, le logiciel CookieViz, etc.)

Le délai d'adaptation aux lignes directrices étant arrivé à son terme le 31 mars 2021, la CNIL s'assure désormais du respect de ces règles chez l'ensemble des acteurs publics et privés.

## Une protection toujours plus forte des personnes dans leur quotidien numérique

La CNIL a également reçu 13 585 plaintes soit 62,5 % d'augmentation depuis la mise en œuvre du RGPD. Ce chiffre, toujours élevé et constant par rapport à 2019, confirme une prise

de conscience conséquente des Français vis-à-vis de leurs droits. Parmi ces plaintes, 4 528 ont été suivies d'une réponse rapide et 9 057 ont nécessité une étude plus approfondie.

## La sécurité des données, une thématique prioritaire de contrôle pour la CNIL

La CNIL a reçu, en 2020, 2 825 notifications de violation de données personnelles soit 24 % de plus qu'en 2019. Pour plus de 500 d'entre elles, l'origine est une attaque par rançongiciel, dont la CNIL a pu constater l'augmentation en 2020 et notoirement en 2021 pour des établissements de santé.

La CNIL sera particulièrement attentive, en 2021 et au-delà, au respect des règles de sécurité concernant les données de santé et dont la perte, l'altération ou l'accès non autorisé peuvent avoir des conséquences particulièrement importantes pour les personnes concernées.

## Un renforcement de l'accompagnement et du conseil des professionnels et des pouvoirs publics

Si chaque organisme est responsable de sa conformité au RGPD et à la loi, la CNIL propose une boîte à outils complète pour les aider à comprendre et à appliquer les différentes règles. L'accompagnement des professionnels a été conduit à deux niveaux, avec des outils généraux et sectoriels.

Parmi les outils d'accompagnement généraux, la CNIL a notamment publié un guide des tiers autorisés et un guide pour aider les professionnels à définir des durées de conservation, ainsi que de nombreux de contenus sur les cookies et autres traceurs. D'autres contenus, sur des outils de conformité prévus par le RGPD, ont également été mis à disposition des professionnels. De nouvelles fiches explicatives pour comprendre et maîtriser les codes de conduite (pour harmoniser des pratiques au niveau d'un secteur d'activité) ou des règles d'entreprise contraignantes (politique de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne), mais également la certification (d'un produit, service, processus ou système de données) sont ainsi disponibles sur cnil.fr.

La CNIL a également renforcé son accompagnement sectoriel en publiant de nouveaux référentiels, prenant en compte les exigences du RGPD, pour la gestion des cabinets médicaux et paramédicaux, pour la gestion des ressources humaines ainsi qu'une consultation sur un projet de référentiel pour la gestion locative.

Concernant les pouvoirs publics, la CNIL a participé à **20 auditions parlementaires et a répondu à 8 questionnaires adressés aux parlementaires.** En 2020, elle a adopté 96 avis sur des projets de texte, notamment en lien avec la crise sanitaire ou concernant les fichiers PASP, GIPASP et EASP. Sans constituer une « autorisation » ou un « refus », ces avis permettent d'éclairer les pouvoirs publics sur des enjeux Informatique et Libertés.

## De nombreux contrôles et des sanctions d'un montant total de 138 millions d'euros

En 2020, la CNIL a conduit **247 contrôles** :

82 en ligne, 74 sur pièces, 72 sur place et 19 sur audition.

Ces contrôles font suite à des plaintes ou des signalements (40 % des cas), sont effectués à l'initiative de la CNIL selon l'actualité (32 %) ou en lien avec les thématiques prioritaires annuelles (15 %) ou font suite à des mises en demeure ou des sanctions (3 %).

**En 2020, la formation restreinte de la CNIL a prononcé 14 sanctions**, dont 11 amendes d'un montant total de **138 489 300 euros** (parfois accompagnées d'une injonction sous astreinte), 2 rappels à l'ordre et une injonction sous astreinte non associée à une amende. Un seul non-lieu a été prononcé.

Ces sanctions concernent des acteurs, des secteurs d'activités et des manquements très variés, et font notamment suite à une sécurité insuffisante des données ou à l'absence d'information et de consentement des personnes, en particulier concernant l'utilisation des cookies.

L'année aura également été marquée par une première sanction décidée en coopération avec les autres autorités de protection des données européennes dans le cadre de la procédure dite de « guichet unique ».

La présidente de la CNIL a par ailleurs prononcé **49 mises en demeure** de se mettre en conformité, dont 3 publiques et 4 en coopération avec d'autres autorités de protection des données européennes. Elle a également prononcé **38 rappels à l'ordre** et **2 avertissements**, notamment suite à des plaintes.

## Une coopération européenne intensifiée en 2020 :

- plus de 1 000 dossiers de coopération européenne concernaient des plaintes ou des contrôles. La CNIL a été autorité chef de file (quand l'établissement principal de l'organisme concerné se situe en France) dans une centaine de cas et autorité concernée dans près de 400 cas.
- 14 projets de sanctions européens ont été examinés par la CNIL, dont 6 décisions adoptées par la formation restreinte contenant des objections pertinentes et motivées ou des commentaires.

**Document 6 : (extrait du site de la CNIL) - Fichiers d'évaluation des agents : sanction de 400 000 euros à l'encontre de la RATP - 04 novembre 2021**

La CNIL a sanctionné la RATP d'une amende de 400 000 euros après avoir constaté que plusieurs centres de bus avaient intégré le nombre de jours de grève des agents dans des fichiers d'évaluation qui servaient à préparer les choix de promotion. Elle a également relevé une durée de conservation excessive des données et des manquements relatifs à la sécurité des données.

## Les contrôles et la sanction en bref

En mai 2020, la CNIL a été saisie par une organisation syndicale d'une plainte concernant la présence du nombre de jours de grève exercés par les agents dans les fichiers utilisés lors des procédures d'avancement de carrière. À la suite de cette plainte, la RATP a déclaré à la CNIL que quatre centres de bus étaient concernés par cette pratique, qu'elle estimait elle-même illégale.

La CNIL a alors effectué des contrôles dans plusieurs centres de bus de la RATP. Ils ont permis de confirmer cette pratique dans trois centres de bus de la RATP (un parmi les quatre signalés par la RATP et deux autres centres). Lors de ses vérifications, la CNIL a également constaté des manquements relatifs à la durée de conservation et à la sécurité des données.

Sur la base de ces éléments et après avoir entendu la RATP, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – a considéré que la RATP avait manqué à ses obligations, en particulier car seules des données strictement nécessaires à l'évaluation des agents auraient dû figurer dans ces fichiers. L'indication du nombre de jours d'absence suffisait ici, sans qu'il soit nécessaire de préciser le motif d'absence lié à l'exercice du droit de grève.

La CNIL a ainsi prononcé une amende de 400 000 euros et a décidé de rendre publique sa décision.

## Les manquements constatés

Une collecte de données non nécessaires (article 5.1.c et 5.2 du RGPD)

La RATP organise chaque année, dans chaque centre de bus, une réunion d'arbitrage dont l'objectif est d'établir la liste des agents proposés à l'avancement par la direction. À cette occasion, un fichier d'aide à la décision est créé par les personnels affectés aux services des ressources humaines. En principe, ce fichier contient seulement les données nécessaires à l'évaluation des agents.

Toutefois, la CNIL a constaté que dans les fichiers des centres de bus qu'elle a contrôlés, figuraient des colonnes relatives au nombre de jours de grève exercés par les agents pour chaque année évaluée.

Au cours de la procédure, la RATP a reconnu le caractère illicite de ces fichiers et a fait valoir qu'une telle pratique était contraire à sa politique générale.

La CNIL a retenu que l'utilisation de données relatives au nombre de jours de grève des agents n'était pas nécessaire pour atteindre les objectifs visés dans le cadre de la préparation des commissions de classement. En particulier, l'indication du nombre total de jours d'absence suffisait, sans qu'il soit nécessaire de rentrer dans le détail en distinguant les jours liés à l'exercice du droit de grève (principe de minimisation des données).

Un manquement à l'obligation de limiter la durée de conservation des données (article 5.1.e du RGPD)

Dans le cadre de fichiers de ressources humaines, la RATP utilise une application qui permet le suivi d'activité des agents, par des fonctionnalités de visualisation et d'extraction de nombreuses données principalement issues des systèmes d'information de ressources humaines de la RATP.

Les contrôles ont permis d'établir que la RATP conservait l'ensemble de ces données dans la base active de l'application, accessible à un grand nombre d'agents, pour une durée qui excède celle qui est nécessaire pour accomplir les finalités recherchées.

Par ailleurs, la RATP a également conservé des fichiers d'évaluation des agents pendant plus de 3 ans après la commission d'avancement pour lesquels ils sont établis, alors que leur conservation n'était nécessaire que 18 mois après la tenue de ces commissions.

La société a toutefois pris les mesures requises au cours de la procédure concernant ce point.

Un manquement à la sécurité des données (article 32 du RGPD)

La CNIL a constaté que la RATP ne différenciait pas suffisamment les différents niveaux d'habilitation des agents. En effet :

- les agents habilités accédaient à l'ensemble des catégories de données contenues dans l'outil (notamment, l'ensemble des données relatives aux ressources humaines) sans distinction des fonctions ou des missions des agents ;
- ces agents accédaient aux données relatives aux agents du centre de bus dans lequel ils exercent leurs fonctions mais également à celles des agents de tous les autres centres de bus ;
- tous les agents habilités pouvaient extraire l'ensemble des données contenues dans l'outil.

Une telle configuration ne permettait pas de prévenir une éventuelle mauvaise utilisation des données et donc de garantir leur confidentialité.

Lors de la procédure, la RATP a fait part de mesures prises pour mettre fin aux manquements relevés par la CNIL.

**Document 7 – Extrait de « Données personnelles info » - Secrétariat Général de la Ville de Paris - Novembre 2018**

# PROTECTION DES DONNÉES: ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

Deux délibérations de la CNIL d'octobre 2018 précisent le périmètre des analyses d'impact sur la vie privée rendues obligatoires et présentent, à titre d'exemple, une liste des traitements pour lesquels une analyse d'impact est requise

## Traitements soumis à la réalisation d'une AIPD

Le RGPD prévoit que le responsable doit effectuer une AIPD lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques
**Le règlement lui-même** donne trois types de traitements susceptibles de présenter un risque élevé :

☐ l'évaluation systématique et approfondie d'aspects personnels fondée sur un traitement automatisé et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;

☐ le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et des infractions ;

☐ la surveillance systématique à grande échelle d'une zone accessible au public.

Dans ce cadre, le Comité européen de protection des données personnelles (CEPD) a identifié **neuf critères** permettant de caractériser un traitement susceptible d'engendrer un risque élevé :

1. données traitées à grande échelle ;
2. données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou de santé, données biométriques et données concernant la vie ou l'orientation sexuelle) ou données à caractère hautement personnel (données relatives à des communications électroniques, données de localisation, données financières, etc.) ;
3. données concernant des personnes vulnérables (patients, personnes âgées, enfants, etc.)
4. croisement ou combinaison de données ;
5. évaluation/scoring (y compris le profilage) ;
6. prise de décision automatisée avec un effet juridique ou similaire ;
7. surveillance systématique de personnes ;
8. traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat ;
9. utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles.

## Rappel: le contenu minimal d'une AIPD

1. une description des opérations de traitement envisagées et de ses finalités
2. l'évaluation de la proportionnalité des opérations de traitement au regard de la finalité ;
3. une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face aux risques.

## Cas de transmission obligatoire d'une AIPD à la CNIL

En ce qui nous concerne deux cas de transmission obligatoire et préalable peuvent exister dans nos procédures :

1/ Lorsqu'après analyse, une AIPD fait apparaître des risques résiduels qui demeurent élevés malgré les mesures correctrices envisagées par le responsable de traitement, celle –ci doit être transmise à la CNIL au préalable de la mise en oeuvre du traitement. Dans ce cas la CNIL, en lien avec le responsable de traitement estime les mesures à prendre et les conditions dans lesquelles le traitement concerné peut être mis en oeuvre.

2/ S'agissant des traitements de données de santé, ils ne peuvent être mis en oeuvre qu'avec la garantie de normes élevées de sécurité. Pour ce raisons, la quasi totalité de ceux-ci devront effectuer une AIPD.

## Type de traitements soumis à AIPD

La CNIL a adopté en octobre 2018, en complément, une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.
Pour chacun de ces traitements la CNIL indique les critères issus des lignes directrices du Comité européen qui sous-tendent l'obligation du recours à un AIPD.
Cette liste a un caractère non-exhaustif.

☐ traitements de données de santé mis en oeuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes (*collecte de données sensibles, personnes dites « vulnérables »)*

☐ Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines *( évaluation ou notation, personnes « vulnérables »)*

☐ Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés *(personnes dites « vulnérables, surveillance systématique)*

☐ Traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire et en matière professionnelle *(personnes vulnérables, évaluation ou notation, collecte de données sensibles)*

☐ Traitements ayant pour finalité la gestion des alertes et des signalements (personnes « vulnérables », *évaluation ou notation, collecte de données sensibles)*

☐ traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre (collecte de données sensibles, personnes « vulnérables »)

☐ Traitements impliquant le profilage des personnes et de manquements contractuels constatés pouvant aboutir à leur exclusion du bénéfice d'un contrat ou à la suspension voire à la rupture de celui-ci (évaluation ou notation, croisement ou combinaison d'ensembles de données, prise de décision automatisée avec effet juridique)

☐ traitements de profilage faisant appel à des données provenant de sources externes (évaluation ou notation, croisement ou combinaison d'ensembles de données)

☐ Traitements de données biométriques aux fins de reconnaissance des personnes parmi lesquelles figurent des personnes dites « vulnérables » (élèves, personnes âgées, patients, demandeurs d'asile, etc.) (collecte de données sensibles, personnes vulnérables)

☐ Instruction des demandes et gestion des logements sociaux (collecte de données sensibles, évaluation ou notation)

☐ Traitements ayant pour finalité l'accompagnement social ou médico-social des personnes *(collecte de données sensible, évaluation ou notation, personnes « vulnérables »)*

**Document 8 – site de l'Agence nationale de sécurité des systèmes d'information – extrait du guide dédié aux collectivités territoriales**

## 04 – SÉCURITÉ NUMÉRIQUE DES COLLECTIVITÉS TERRITORIALES

Les collectivités territoriales (CT) sont engagées dans une transformation numérique profonde, autant pour répondre à des obligations règlementaires qu'à un souci de rendre un meilleur service aux citoyens. Cette dépendance de plus en plus forte aux systèmes d'information (SI), couplée à l'hétérogénéité de la taille des communes, crée une fragilité, soulignée dans la Revue stratégique de cyberdéfense (RSC) de 2018. Au même titre que les SI de l'État, des opérateurs d'importance vitale (OIV) ou des opérateurs de services essentiels (OSE), la protection des SI des collectivités territoriales fait partie des champs prioritaires définis par la RSC pour consolider le modèle national de cyberdéfense. Au-delà de l'application de mesures, qu'elles soient d'hygiène ou techniques, de gouvernance, organisationnelles et humaines, la dimension règlementaire et juridique est essentielle pour assurer une meilleure prise en compte des risques numériques. Pour répondre au défi de la sécurité du numérique des collectivités territoriales, la France, soit directement par son droit national, soit via les règlements et directives pris au niveau de l'Union Européenne, s'est dotée d'un cadre règlementaire. Ce dernier participe à la protection de ces systèmes d'information et a pour objectifs :

- le renforcement de la confiance des usagers dans l'utilisation des services numériques ;
- le renforcement de la sécurité des données à caractère personnel ;
- la transformation numérique des administrations l'État ;
- le renforcement de la sécurité des acteurs critiques pour l'État.

Ces réglementations s'architecturent autour de trois principes fondamentaux :

- la gouvernance qui vise à impliquer l'ensemble des acteurs (décideurs, agents, etc.) des collectivités territoriales dans la sécurité par la définition et le suivi d'une politique de sécurité des systèmes d'information (PSSI) ;
- la gestion des risques qui doit amener les collectivités territoriales à s'interroger sur les menaces auxquelles elles sont exposées et les mesures à mettre en œuvre pour s'en protéger tout en tenant compte d'un certain nombre de contraintes (financière, humaine, sociale, etc.) ;
- l'amélioration continue qui permet à la collectivité d'évaluer régulièrement son niveau de sécurité afin d'identifier les domaines dans lesquels elle doit progresser.

Pour les non-spécialistes et, singulièrement, pour les élus déjà en proie avec une multitude de règles et de textes à appliquer, le cadre règlementaire national participant à la protection des systèmes d'information des collectivités territoriales méritait un guide. Ce document se veut donc synthétique, pratique et abordable en particulier par les élus et les cadres territoriaux chargés d'en garantir l'application et la conformité.

**Document 9 – site de l'Agence nationale de sécurité des systèmes d'information – extrait du guide Anticiper et gérer sa communication de crise cyber (décembre 2021)**

Face à une attaque, la technicité d'une crise cyber peut déstabiliser les plus aguerris des communicants, confrontés à des codes, des enjeux et à un écosystème parfois très éloignés de leur cœur de métier.

Tout en s'attardant sur les spécificités liées au cyber, ce guide tend à démontrer qu'une bonne communication de crise cyber reprend avant tout les réflexes et les outils communs à toute stratégie de communication de crise.

« *Lorsqu'une crise cyber survient, l'action des communicants passe trop souvent au second plan. C'est une erreur. Pour une gestion globale de la crise, il est indispensable que la communication travaille main dans la main avec la réponse technique.* » Guillaume Poupard, directeur général de l'ANSSI

## À quoi sert ce guide ?

En se basant sur les situations rencontrées par l'ANSSI depuis sa création en 2009 dans son rôle d'assistance auprès de victimes, et en partenariat avec l'association Cap'Com, ce guide vise à apporter des conseils et des recommandations très opérationnels afin de construire puis de déclencher le volet communication de crise lors d'une attaque informatique.

Si aucune recette magique n'existe en gestion de crise, quelques réflexes et certaines notions essentielles peuvent être intégrés dès aujourd'hui par votre organisation, privée ou publique, afin d'être prêt à faire face à une crise cyber.

Les recommandations de ce guide sont ainsi également adaptées à la gestion de situations qualifiées de « sensibles », qui précèdent souvent une éventuelle crise médiatique.

## À qui s'adresse-t-il ?

Ce guide s'adresse à toutes les personnes occupant une fonction de communicant lors de la gestion d'une crise. En fonction de la taille et de l'organisation de l'entité, il peut s'agir d'un professionnel de la communication (DIRCOM, chargé de communication ou agence de communication), mais parfois aussi d'autres profils (cabinet, juriste, décideur), faute de communicants. Selon la situation, l'équipe opérationnelle peut même parfois jouer ce rôle de communicant.

Si ce guide s'adresse en premier lieu aux professionnels de la communication, qui ont un rôle clé à jouer en matière de gestion de crise, il a également pour objectif de donner des outils et des conseils à d'autres métiers, techniques et décisionnels, pouvant intervenir aux côtés des communicants.

## Quels sont les prérequis ?

Ce guide vise à apporter un éclairage sur les spécificités d'une communication de crise cyber, telles que perçues par l'ANSSI. Il n'a pas pour objectif de revenir en détails sur la construction d'une stratégie de communication de crise en général. Ce travail doit être idéalement réalisé et testé en amont afin de pouvoir adapter l'organisation et les outils à la singularité d'une crise cyber.

Ce guide propose cependant quelques rappels des fondamentaux de la communication de crise pour familiariser l'ensemble des lecteurs aux notions et aux enjeux clés poursuivis par la fonction communication.

## Et d'ailleurs, qu'est-ce qu'une crise cyber ?

Une crise « d'origine cyber » se définit par la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc.) en raison d'une ou de plusieurs actions malveillantes sur ses services et outils numériques (cyberattaques de type rançongiciel, déni de service – DoS, etc.). C'est donc un évènement à l'impact fort, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal de l'organisation. Par convention, on parlera par la suite de « crise cyber ».

**Document 10 – la Gazette des communes « cyberattaques : les collectivités de plus en plus transparentes » - 24 février 2021**

Publié le 24/02/2021 • Par Alexandre Léchenet • dans : Dossiers d'actualité, France

Alors que les cyberattaques se multiplient, élus et agents acceptent de plus en plus de communiquer à leur sujet. Outre les raisons juridiques, cela permet aussi une sensibilisation et une prévention face à un risque croissant.

Christophe Béchu, une semaine après l'attaque qui a touché la mairie et la communauté d'agglomération d'Angers qu'il dirige, a reçu les caméras du média en ligne Brut. On peut y voir les agents retrouver les annuaires en papier ou sortir un fax des réserves.

A la mi-janvier, Angers a connu une cyberattaque qui a paralysé ses systèmes informatiques. Le temps de tout remettre en ordre, il a fallu se tourner vers l'analogique, et l'expliquer aux Angevins.

L'attaque a été rapidement maîtrisée, si bien que le lundi suivant, une grande majorité des démarches étaient accessibles. Mais il n'en était pas de même pour les agents, avec l'ensemble de la collectivité qui fonctionnait en mode dégradé. « Il n'y avait aucune raison de ne pas communiquer », nous indique-t-on à la ville. Une transparence en pratique encore relativement rare, mais les comportements changent.

## Des dizaines de collectivités touchées

Dimanche 20 février, l'agglomération du Grand Chalon prévient sur Facebook que « les systèmes informatiques de la ville de Chalon-sur-Saône et du Grand Chalon ont été victimes d'une cyberattaque ».

Le 18 février, la ville de Villecresnes annonce sur son site qu'après deux attaques au début du mois, les services étaient encore perturbés.

Selon notre décompte, au moins huit collectivités ont communiqué sur des cyberattaques qu'elles ont subies depuis le début de l'année, principalement par des rançongiciels.

En 2020, au moins 67 collectivités ont été ciblées par des cyberattaques, qu'il s'agisse de défaçages, c'est-à-dire une intrusion sur le site web pour en modifier le contenu ; d'attaques par rançongiciels, aux conséquences potentiellement très importantes ; de minage, c'est-à-dire l'utilisation des ordinateurs de la collectivité pour fabriquer des crypto-monnaies ou d'autres encore, comme le cheval de Troie Emotet qui ouvre une porte dans l'infrastructure pour faciliter les utilisation frauduleuses. Parmi les victimes, on trouve des collectivités de toutes tailles, de la métropole d'Aix-Marseille-Provence à des petites villes de l'Oise.

## Pédagogie

A Houilles, dans les Yvelines, le maire a témoigné, dans une vidéo, de l'impact de l'attaque sur les services. « C'était important pour moi de dire à quel point l'attaque avait été extrêmement violente pour les agents et impactante pour nos services publics », raconte Julien Chambon, maire (LREM) de la ville.

« Il faut qu'on prenne nos responsabilités, qu'on sécurise absolument nos dispositifs de façon plus professionnelle, qu'on renouvelle le matériel et, surtout, qu'on se pose la question, à cette occasion-là, de comment on fabrique un service public moderne et une mairie 2.0 sécurisée et qui n'exclut personne. »

Christophe Béchu tient le même discours dans l'interview qu'il accorde à Brut : « On s'est beaucoup plus concentrés sur le fait d'augmenter les services qu'on offrait à la population grâce au numérique qu'au fait de protéger l'architecture de ces systèmes. Ça ne veut pas dire qu'on n'a rien fait, ça veut dire qu'on n'a pas mis assez d'efforts là-dessus. »

## Maturité

Le changement est notable ces derniers mois : les élus et agents acceptent plus facilement de raconter ces cyberattaques. « A l'heure actuelle, témoigner qu'on a été piraté, c'est faire preuve de maturité. Ne pas le dire, c'est être dans le déni », confirme Cyril Bras, RSSI de Grenoble-Alpes métropole, de la ville de Grenoble et du CCAS.

Cette communication « ne peut être que bénéfique », poursuit-il. Aussi bien pour faire prendre conscience aux élus et dirigeants de la nécessité d'embaucher des RSSI, mais aussi pour la prévention.

Il a d'ailleurs initié, en lien avec l'Anssi, un réseau de dialogue entre RSSI de régions, départements, métropoles et communes pour partager des expériences ou des informations sur les attaques subies. Informations utiles pour se préparer et anticiper.

## Protection juridique

La communication peut-être à double tranchant, selon Emmanuel Vivé, directeur de Déclic, réseau d'échange et de mutualisation informatique. Si elle est utile, notamment au regard du RGPD, elle pourrait aussi diriger les pirates vers une cible ou une autre, dans l'espoir d'une reprise médiatique. Il ne faut cependant pas garder tout ça pour soi. Notifications à la Cnil et plaintes permettent de se protéger juridiquement, mais permettent également aux autorités de prendre la mesure du phénomène.

Le nombre de notifications à la Cnil, à la suite d'activité malveillante, n'a fait que progresser depuis 2018 : on en comptait 13 au premier semestre 2018, contre 67 à la même période en 2020, pour les administrations publiques. Et sur les 158 notifications, seules 10 administrations déclaraient ne pas prévoir de prévenir les personnes touchées du problème.

Tous les acteurs interrogés s'accordent sur une chose : la sécurisation des systèmes d'informations, l'embauche d'un RSSI ou la prévention ne sauraient pâtir de réductions budgétaires. « L'erreur à ne pas faire, en ce moment, serait de baisser les budgets cybersécurité », alerte Emmanuel Vivé.

## « Si l'on ne communique pas sur une attaque, c'est terrible en termes d'image »

Anne Le Hénanff, première adjointe au maire de Vannes et vice-présidente de l'association Villes Internet, a participé à la rédaction du guide de l'Anssi et de l'AMF sur la cybersécurité. Elle témoigne de son travail de prévention : « Après l'attaque qu'on a subi à Vannes en 2016, nous avons décidé d'être transparents. Depuis l'attaque, dès que j'étais sollicitée et en accord

avec le maire, je suis allée témoigner. C'est un engagement de fond, et au fil des années, l'équipe s'est étoffée de profils différents, grâce à l'Anssi, à cybermalveillance.gouv.fr ou au pôle d'excellence « cyber ».

Les cyberattaques contre les collectivités n'étaient pas jugées comme une priorité par les acteurs il y a quatre ou cinq ans. On a réussi à en faire parler plus, mais ça ne suffit pas encore. Encore aujourd'hui, une cyberattaque subie reste la principale raison de la mise en œuvre de mesures de protection des systèmes d'information. Il y a encore beaucoup de prévention à faire. Il existe une différence notable, cependant, par rapport à 2016 : les collectivités commencent à libérer la parole autour de ces sujets et c'est fondamental. Grâce au RGPD, les élus commencent à prendre conscience qu'il est de leur responsabilité de protéger les données produites et hébergées par les collectivités. Et ils se rendent compte également que les données sont une richesse future, qu'il faut donc protéger.

Ce qui est terrible, si l'on ne communique pas sur une attaque, c'est en termes d'image : on pourra non seulement nous reprocher de ne pas avoir mis en place les outils nécessaires, mais aussi de ne pas avoir été transparents. Le RGPD impose qu'une structure cyberattaquée et qui a eu des failles dans son système le déclare assez rapidement à la Cnil, et informe les personnes touchées en cas de risque sérieux. Certes, il peut y avoir de la gêne à se présenter comme victime, mais c'est quelque chose qu'il faut dépasser et aller en parler, déposer plainte, communiquer. Ça aide notamment les services de sécurité à faire leur travail et à repérer les filières et les origines des attaquants. »

Document 11 : Charte de la donnée de Nantes métropole

Ville de Nantes | Nantes Métropole

# Charte métropolitaine de la donnée

## Un cadre éthique pour protéger les citoyens et réguler l'utilisation des données sur le territoire


metropole.nantes.fr

Johanna ROLLAND
Maire de Nantes
Présidente de Nantes Métropole

# PRÉAMBULE

**Les données sont de plus en plus présentes dans nos vies quotidiennes.** Elles sont produites et collectées en masse dans toutes nos activités. Chacun est concerné comme **citoyen, salarié, usager de services publics ou privés. La gestion des villes n'échappe pas à cette évolution.**

Des données sont aujourd'hui produites en grand volume par la gestion des services publics, par des opérateurs de mobilité, des distributeurs d'énergie, des gestionnaires de déchets et bien d'autres. En 2020, le volume des données produites en une seule journée pour la gestion des villes européennes, sera 4 fois supérieur à celui des données produites pour toute l'année 2015.

**Maîtriser et contrôler la gestion qui est faite de ces données est indispensable** car cette nouvelle étape de la transition numérique des territoires pose des enjeux juridiques, économiques et éthiques.

Plusieurs grandes collectivités dans le monde comme Boston, Montréal, Amsterdam, Barcelone s'en sont saisies. Chacune imagine **des dispositifs pour que la puissance publique encadre la façon dont les données de leurs habitants sont utilisées.**

**Nantes Métropole a fait le choix d'élaborer une charte métropolitaine de la donnée** qui pose des principes rigoureux et éthiques pour **protéger les citoyens et encadrer les usages de la donnée sur le territoire.**

Ce choix est le **fruit d'une histoire et d'une méthode.** Le dialogue entre la société civile et la collectivité s'est développé depuis plusieurs années autour du numérique et des enjeux relatifs à la donnée. Il s'est notamment traduit par une participation active d'habitants, de collectifs, de partenaires à des démarches de dialogue citoyen comme par exemple *« WiFi public : quel internet pour tous sur l'espace public ? », « Construisons ensemble les règles du jeu des rues connectées de l'île de Nantes ».*

Lors de ces démarches, une diversité de points de vue a été exprimée sur les usages de la donnée comme levier de la participation, l'accès à une information claire et instantanée, un besoin de pédagogie et de transparence concernant la sécurité et la protection des données personnelles.

Ces engagements, la collectivité les prend d'abord pour elle-même. Ils s'appliquent aussi aux acteurs publics et privés qui œuvrent dans le cadre de ses activités de service public.

La collectivité s'engage également à **mettre en place un cadre de dialogue avec les acteurs qui interviennent sur l'espace public afin de créer les conditions d'un accès à ces données au service de l'intérêt général.**

# Protection
# Confiance
# **Sobriété**

## Les valeurs de la charte métropolitaine de la donnée

> **CONFIANCE et ÉTHIQUE** pour la protection des données des citoyens et les usages de la donnée au service de l'intérêt général ;

> **TRANSPARENCE** des politiques publiques, pour rendre compte, au service de la vie démocratique ;

> **SOBRIÉTÉ et TRANSITION ENERGETIQUE** dans la collecte et la conservation des données pour contrôler et limiter les effets liés à la consommation énergétique des données massives ;

> **INNOVATION** pour susciter et animer l'expérimentation de nouveaux usages au service des citoyens ;

> **COLLABORATION** pour créer des espaces de dialogue sur le territoire et avancer collectivement sur ces enjeux complexes.

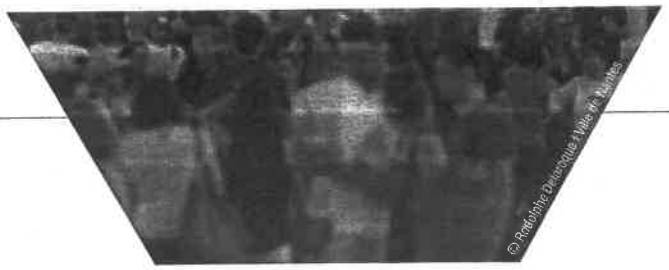
## Les 4 engagements de la collectivité

> Engagement 1 : **Garantir la souveraineté de la collectivité sur ses données**

> Engagement 2 : **Protéger les données**

> Engagement 3 : **Garantir la transparence**

> Engagement 4 : **Favoriser de nouveaux usages**




# ENGAGEMENT 1

## Garantir la souveraineté sur les données du service public

### Principe 1 | **Données publiques**

La mise en œuvre des missions de service public nécessite l'utilisation de données nombreuses.

Les données produites, collectées, traitées ou gérées par la collectivité ou par un tiers intervenant pour son compte dans le cadre de ses activités de service public et en lien avec ses compétences, ont le statut de « données publiques ». **Elles constituent un patrimoine qui est un bien public.**

### Principe 2 | **Propriété des données publiques**


Les données publiques sont propriété de la collectivité. **La collectivité est garante de leur utilisation et à ce titre elle se doit de définir les droits d'usage qui peuvent être accordés à des tiers.**

Ce principe ne s'applique pas aux **données personnelles dont la propriété est inaliénable** et reste celle des citoyens.

### Principe 3 | **L'hébergement des données publiques**


Face aux enjeux de sécurité et de souveraineté des données liées à la gestion des services publics, la collectivité fixe les règles d'hébergement de ses données.

**Afin de garantir la sécurité de ses données les plus sensibles, la collectivité impose leur hébergement en France.** Les autres données publiques sont hébergées en France ou dans l'Union Européenne.

La collectivité s'inscrit dans la démarche engagée par l'État pour définir une doctrine pour un hébergement souverain.

### Principe 4 | **Données d'intérêt métropolitain**

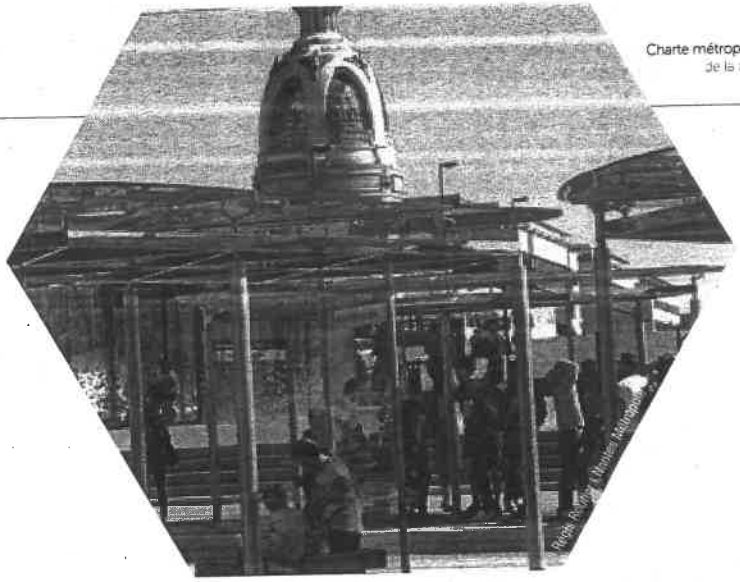

Des acteurs divers interviennent dans la vie du territoire métropolitain et sont susceptibles de produire **des données qui revêtent un caractère d'intérêt général.**

Certaines sont produites par des acteurs publics (services de l'Etat, collectivités territoriales, entreprises publiques ou délégataires de l'Etat...), d'autres sont produites par des acteurs privés.

Lorsqu'il est de l'intérêt de tous qu'elles soient partagées avec la puissance publique parce qu'elles peuvent contribuer utilement à la connaissance des dynamiques du territoire et à la mise en œuvre des politiques publiques, **la collectivité propose un cadre de dialogue avec les acteurs concernés pour créer les conditions d'un accès à ces données respectueux des droits de tous. Ces données sont dites d'intérêt métropolitain.**




31



# ENGAGEMENT 2

## Protéger les données

### Principe 5 | **La protection des données personnelles**

La législation européenne (Règlement Général de Protection des Données Personnelles - RGPD) et la loi française (loi Informatique et Libertés de 1978 modifiée par le RGPD) **imposent aux entreprises comme aux acteurs publics un cadre qui protège de manière renforcée les données personnelles des Européens.** Ce cadre est entré en application le 25 mai 2018.

**La collectivité applique ces règles pour ses propres services et veille également à leur respect par les entreprises qui travaillent pour son compte.** Afin de garantir le niveau le plus élevé de protection des données des citoyens, la collectivité intègre des **clauses de protection des données personnelles dans ses marchés publics comme dans ses contrats** dès lors que les projets soutenus impliquent la collecte et le traitement de données personnelles.

La collectivité s'engage à **favoriser les initiatives visant à renforcer la compréhension et la connaissance par les citoyens de leurs nouveaux droits créés par la législation sur la protection des données** (modalités de recueil du consentement, droit à l'oubli et effacement des données, portabilité des données...).

### Principe 6 | **La sécurité des systèmes d'information**

La protection des systèmes d'information de la collectivité permet de **garantir la sécurité des données des citoyens, de se prémunir des attaques extérieures, d'éviter les risques de perte ou de divulgation des données et de garantir la continuité du service public.**

**La collectivité met en place des mesures certifiées pour assurer la résistance de ses systèmes d'information** et maintenir la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées et collectées par elle.

### Principe 7 | **La sobriété dans la collecte et la conservation des données**


Les nouveaux outils de collecte et de traitement multiplient les possibilités d'exploiter des données de plus en plus massives. La collectivité adopte un principe de sobriété. **Elle collecte les données uniquement nécessaires à l'accomplissement de ses missions de service public et en limite le stockage.**

La durée de conservation de toutes les données, personnelles ou non, est déterminée en fonction de leur nature et de l'objectif poursuivi (à l'exception des données conservées et archivées à des fins de recherche scientifique ou historique).

# ENGAGEMENT 3

## Garantir la transparence

### Principe 8 | **Ouverture des données publiques**

L'ouverture des données publiques par la collectivité répond à trois objectifs prioritaires : **contribuer à la transparence de la vie publique, alimenter le dialogue citoyen et créer les conditions du développement de nouveaux services.**

La collectivité s'engage à ce que les **données publiques de la collectivité soient accessibles gratuitement sur le portail https://data.nantesmetropole.fr** en consultation et en téléchargement.

**Les données mises à la disposition du public excluent les données protégées par la loi** (données personnelles, données d'entreprises relevant du secret industriel ou commercial, données couvertes par des droits d'auteur).

La collectivité privilégie l'utilisation d'une licence d'utilisation des données qui permet l'usage le plus large des données ouvertes. Elle se réserve le droit d'appliquer des restrictions pour protéger l'intérêt général et limiter des utilisations de données qui iraient à l'encontre des politiques publiques du territoire.

### Principe 9 | **Publication et transparence des algorithmes**

Pour mettre en œuvre ses missions de service public, **la collectivité utilise des outils de calculs automatisés, par exemple pour définir des droits, calculer une aide ou établir une facture.**

La collectivité garantit la protection des droits des citoyens et s'engage pour une **transparence de l'utilisation des algorithmes.** Dans le respect des droits des éditeurs, elle publie le code informatique des algorithmes entraînant une prise de décision individuelle automatisée.

# ENGAGEMENT 4

## Favoriser de nouveaux usages

### Principe 10 | **Expérimentations**

La collectivité soutient et favorise les innovations et les expérimentations dans différents domaines (transports, énergie, éclairage public, habitat...).

**La collectivité et les acteurs du projet s'engagent par un protocole à définir ensemble les conditions de la mise en œuvre des expérimentations, de leur évaluation et de leur déploiement.** Ce protocole s'inscrit dans les principes de la charte.

Dans l'hypothèse où une expérimentation nécessiterait de déroger à l'un ou l'autre de ces principes, le protocole encadrera la dérogation. Il limitera notamment la durée de conservation des données.

Ces principes sont applicables à toute expérimentation conduite par des acteurs, publics ou privés, intervenant sur l'espace public métropolitain.

### Principe 11 | **Intelligence artificielle**


Dans l'avenir, il est possible que des outils d'intelligence artificielle accompagnent les acteurs publics dans leurs missions. Dans ce cadre, **la collectivité anticipe et fixe des principes éthiques et protecteurs.** Elle régule les expérimentations en imposant le respect de règles rigoureuses et responsables partagées avec les acteurs nantais du collectif NaonedIA en faveur d'une intelligence artificielle responsable.

**La collectivité s'interdit et interdit aux acteurs publics et privés agissant pour son compte, toute utilisation de l'intelligence artificielle pour des décisions individuelles concernant les usagers des services publics.**

# MODALITÉS DE MISE EN ŒUVRE

## Principes d'action

### Principe 12 | **Mise en œuvre et évaluation de la charte**

Il appartiendra aux parties prenantes (la collectivité, les acteurs publics et privés engagés dans la mise en œuvre des politiques publiques et les autres partenaires qui souhaitent s'engager) d'organiser les conditions d'application des principes et d'en garantir un suivi transparent et public.

### Principe 13 | **Présentation d'un rapport annuel**

Un rapport public est présenté chaque année pour dresser un état des lieux et assurer le suivi de la mise en œuvre de la charte.

Ce rapport détaille les modalités d'application des obligations légales ayant trait à la protection des données personnelles des citoyens.


# GLOSSAIRE

**ALGORITHME**
Désigne une suite de calculs nécessaires pour effectuer une opération complexe.
Un algorithme informatique est la description dans un langage formel (un langage de programmation) d'une suite finie et ordonnée de processus qui, à partir de données en entrée, livre des données en sortie en un temps fini, en vue d'un objectif prédéterminé.

**CITOYEN**
Désigne chaque personne concernée par la gestion de ses données personnelles par la collectivité ou ses opérateurs sur le territoire métropolitain. Le terme citoyen rassemble les multiples dimensions que peut revêtir la relation personnelle de chacune et chacun au territoire et à l'action publique : habitant, usager, bénéficiaire, client, électeur...

**CYBERSÉCURITÉ**
Désigne l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

**DONNÉE**
Une donnée est une information stockée dans un format qui permet son utilisation par un programme. Par exemple, si l'on souhaite des informations sur l'âge des habitants d'un quartier, les données seront les âges disponibles (ou les dates de naissance) des habitants du quartier. Les données peuvent prendre de nombreuses formes : des chiffres, du texte (par exemple des couleurs), des coordonnées géographiques...

**DONNÉES À CARACTÈRE PERSONNEL**
Désigne aux termes de l'article 2 de la Loi Informatique et Libertés : *« toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».*

**DONNÉES D'INTÉRÊT MÉTROPOLITAIN**
Désigne toutes les données publiques ou privées dont l'intérêt général sur le territoire de la métropole justifie que la collectivité puisse y avoir accès.

**DONNÉES PUBLIQUES**
Désigne l'ensemble des données produites ou collectées par la collectivité ou les opérateurs intervenant pour son compte, dans le cadre de ses activités de service public.

**DONNÉES OUVERTES (OU OPEN DATA)**
Désigne les données qu'un organisme met à la disposition de tous sous forme de fichiers numériques afin de permettre leur réutilisation. La loi pour une République Numérique votée en 2016 a notamment pour objectif de favoriser une politique d'ouverture des données et des connaissances, dans un objectif de transparence ou afin de permettre leur réutilisation, notamment à des fins économiques.

**EXPÉRIMENTATION**
Désigne tout dispositif ayant pour objet de tester des produits, des usages ou des services innovants qui pourraient correspondre aux besoins du territoire métropolitain ou des Nantais.

**INTELLIGENCE ARTIFICIELLE**
Désigne l'ensemble des théories et des techniques développant des programmes informatiques complexes capables de simuler certains traits de l'intelligence humaine (raisonnement, apprentissage...) et notamment des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent pour améliorer leur performance.

**LOI INFORMATIQUE ET LIBERTÉS**
Désigne la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, aujourd'hui complétée par le Règlement Général sur la Protection des Données Personnelles.

**LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE**
Désigne la loi n°2016-1321 du 7 octobre 2016 pour une République numérique également appelée « Loi Lemaire ».

**PARTENAIRES**
La présente charte entend comme partenaires de la collectivité les différents acteurs qui agissent sur le territoire quel que soit leur statut. Certains partenaires ont un statut public, d'autres un statut privé. Certains agissent dans le cadre d'une délégation de service public ou d'une concession, d'autres interviennent au titre d'un partenariat privé.

**RESPONSABLE DE TRAITEMENT**
Désigne aux termes de l'article 3 de la Loi Informatique et Libertés : « sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ».

**RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES PERSONNELLES (RGPD)**
Désigne 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, abrogeant la directive 95/46/CE. Il est entré en vigueur le 25 mai 2018.

**SERVICES PUBLICS**
Désigne les activités exercées directement par la collectivité ou sous son contrôle, dans le but de satisfaire un besoin d'intérêt général.

En savoir plus sur la Charte métropolitaine de la donnée :
**metropole.nantes.fr/charte-donnee**

DG à l'information et à la relation au Citoyen Nantes Métropole - 2019-06-661 - © Tous droits réservés - Dupliqué - Imprimé sur papier PEFC

Ville de Nantes | Nantes Métropole
2 cours du Champ-de-Mars
Nantes 44 923 CEDEX 09
Tél. : 02 40 99 48 48
metropole.nantes.fr