RGPD : ce qui change pour les organisateurs d'ACM

Depuis le 25 mai, date à laquelle le Règlement général sur la protection des données personnelles (RGPD) est entré en vigueur, en France, comme dans les autres pays de l'Union européenne, tous les particuliers se sont familiarisés avec l'acronyme RGPD. Quelles sont les nouveautés introduites par ce règlement ? Les organisateurs d'accueils collectifs de mineurs sont-ils concernés ? Qu'est-ce que cela change pour eux ?

© Estelle Perdu

Depuis le 6 janvier 1978, date de l'entrée en vigueur de la célèbre loi Informatique et Libertés, le numérique a transformé complètement les grands équilibres entre sphère privée et sphère publique, en investissant quasiment tous les champs de la vie sociale. Bien sûr, la loi de 1978 ne pouvait pas anticiper les nouveaux sens que la vie privée allait prendre. À l'heure du « *big data* », où il est devenu difficile de savoir entre les mains de qui peuvent tomber nos données personnelles, il a fallu poser de nouvelles règles juridiques et renforcer certains droits.

Quel est le risque ?

À l'âge de « *l'homo numericus* », toute donnée connectée peut servir de fondement à la reconstitution d'informations plus précises et attentatoires à l'intimité de la personne. Car, si le prélèvement d'une donnée prise individuellement ne paraît pas porter à conséquence, la somme des données que l'on renseigne en ligne peut produire des renseignements très détaillés sur les caractéristiques de la vie privée d'une personne, par le biais de processus d'agrégations et de recoupements automatisés.

On a pu, par exemple, reprocher aux politiques de ressources humaines fondées sur un traitement automatique de données personnelles de catégoriser de façon discriminante les profils de personnes. Par ailleurs, les failles de sécurité des systèmes de stockage des données personnelles menacent aussi la vie privée.

Les organisateurs d'ACM sont-ils concernés par le RGPD ?

Oui et non.
Le RGPD concerne toutes les structures qui rassemblent ce qu'on appelle des « *données personnelles* », c'est-à-dire « *toute information se rapportant à une personne physique identifiée ou identifiable [...] directement ou indirectement* ». Ce sont les grands groupes internationaux, comme les GAFAM (acronyme des géants du Web : Google, Apple, Facebook, Amazon et Microsoft), qui sont bien sûr visés en premier lieu. En ayant désormais une emprise considérable sur nos vies privées, ces entreprises peuvent y porter atteinte via une marchandisation généralisée des données personnelles et leur ciblage par des algorithmes pointus. La gratuité d'accès à de nombreux services du Web n'est bien sûr pas réelle, mais conditionnée par l'échange, souvent inconscient sur sa portée, des données personnelles des utilisateurs. Mais, si dans certaines circonstances, les individus exposent volontairement leurs données personnelles (par exemple sur les réseaux sociaux), ils peuvent aussi être amenés à les céder du fait d'exigences d'intérêt général : c'est le cas notamment du cadre scolaire et du cadre extrascolaire.
Dans cette dernière situation, la collecte d'informations touchant à la vie privée des personnes s'impose. Mais, pour autant, leur utilisation doit se faire de manière légitime, pertinente et proportionnée. Ces trois adjectifs sont importants.

Qu'est-ce qu'une donnée à caractère personnel ?

Le RGPD définit les données à caractère personnel comme « *des informations se rapportant à une personne physique identifiée ou identifiable* ». Par exemple, un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de Sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, etc.
Peu importe que ces informations soient confidentielles ou publiques. Les règles du RGPD s'appliquent lorsqu'elles sont utilisées, conservées ou collectées, que ce soit numériquement ou sur papier.
À noter : Pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc. Mais, attention ! S'il est possible, par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.

Quels sont les grands principes des règles de protection des données personnelles ?

- **Le principe de finalité : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime.**
- **Le principe de proportionnalité et de pertinence : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier.**
- **Le principe d'une durée de conservation limitée : il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier.**
- **Le principe de sécurité et de confidentialité : le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations.**
- **Les droits des personnes.**

Qu'est-ce qu'une donnée sensible ?

C'est une information qui révèle les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle d'une personne physique. **>>>**

>>> Elles font donc l'objet de protections particulières. Il est interdit de recueillir et d'utiliser ces données. Sauf dans certains cas précis et notamment :

- si la personne concernée a donné son consentement exprès (écrit, clair et explicite) ;
- si ces données sont nécessaires dans un but médical ou pour la recherche dans le domaine de la santé ;
- si leur utilisation est justifiée par l'intérêt public et autorisée par la Commission nationale de l'informatique et des libertés (CNIL) ;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

À noter : Les informations relatives aux infractions ou condamnations ne sont pas considérées comme des données sensibles, mais elles font l'objet de la même protection. Seules certaines autorités publiques – comme les Directions départementales de la cohésion sociale (DDCS) – peuvent les utiliser, ainsi que la personne morale victime dans le cadre de la défense de ses intérêts.

Les données personnelles et sensibles en ACM

Tout organisateur d'accueil collectif de mineurs collecte et utilise des données personnelles, dont certaines sont sensibles. Parmi les données personnelles non sensibles, notons celles relatives :

- aux représentants légaux de l'enfant concerné (identité et coordonnées, leurs droits sur le mineur, l'administration des services visés par la présente norme simplifiée, les autorisations aux interventions chirurgicales d'urgence, à la prise et/ou la diffusion de photographies, et aux sorties ou activités spécifiques) ;
- à l'enfant (identité, coordonnées, photo, services fréquentés, état et besoins) ;
- aux personnes autorisées à venir chercher le mineur ou à prévenir en cas d'urgence.

Parmi les données sensibles

Régime alimentaire

Des renseignements relatifs au régime alimentaire du mineur peuvent être collectés au sein des traitements de données à caractère personnel effectués. Selon la Commission nationale consultative des droits de l'homme (CNCDH), certaines « *données scolaires* » sont susceptibles de révéler de vastes pans de la vie privée des élèves, en particulier à la suite d'opération de recoupement : en agrégeant les données relatives aux absences et celle relatives à la fréquentation de la cantine, on peut, par exemple, déduire la confession d'un élève.

La CNIL recommande que ces données soient le plus neutres possible. De ce fait, ces renseignements ne peuvent contenir de données faisant apparaître les origines raciales, ethniques ou religieuses du mineur concerné ni aucune donnée de santé.

À titre d'exemple, ne peuvent pas apparaître les mentions « *halal* » ou « *casher* ». Les mentions suivantes peuvent en revanche être enregistrées dans les traitements concernés : « *sans porc* », « *sans gluten* », « *sans viande* », etc.

Santé

Selon la CNCDH, certains traitements de données de santé peuvent relever d'une « *finalité d'intérêt public* ». Cette formule renvoie directement à la « *mission d'intérêt public* » contenue dans le RGPD, selon laquelle les données traitées dans ce cadre, y compris sensibles, peuvent bénéficier de certaines exceptions. Compte tenu de l'extrême confidentialité des données de santé, la CNCDH incite fortement à ce que le partage de ces données se fasse à travers un cryptage de qualité et des mesures drastiques de conservation.

En matière de santé, seules les données suivantes (exigées par la réglementation) peuvent être enregistrées :

- les données relatives à l'état vaccinal obligatoire, à jour, de l'enfant ;
- la fiche sanitaire ;

© Laurence Fragnol

Le RGPD prévoit plusieurs droits pour les particuliers

- **Le droit de savoir ce que l'entreprise fait avec les données, le droit à l'information.**
- **Le droit d'accès aux données.**
- **Le droit de s'opposer à la récolte des données.**
- **Le droit de corriger des données.**
- **Le droit à l'oubli et de faire supprimer ses données.**
- **Le droit de regard en cas de décisions automatisées.**
- **Le droit à la portabilité des données.**
- **Le droit d'information en cas de mise en péril ou d'atteinte aux données.**

• les dispositions légales concernant le suivi sanitaire des mineurs interdisent la conservation de cette fiche sous un format informatisé. Ces informations doivent donc être fournies au directeur de centre :
– sous enveloppe cachetée comprenant le nom du mineur concerné ;
– après avoir recueilli le consentement des représentants légaux du mineur concerné ;
• les données nécessaires à une prise en charge spécifique.

Est-il toujours possible de demander des pièces justificatives ?

Oui. Les pièces justificatives strictement nécessaires à la réalisation des finalités poursuivies par le responsable de traitement peuvent être demandées aux usagers.
Par exemple, les avis d'imposition ou de non-imposition, ainsi que les attestations d'assurance scolaire, peuvent être exigés pour l'inscription à des activités périscolaires. De la même manière, une copie du livret de famille peut être demandée aux représentants légaux du mineur afin de prouver l'exercice de leurs droits sur celui-ci.

Quelle est la durée de conservation des données et des pièces justificatives ?

Les données à caractère personnel collectées ainsi que les pièces justificatives et afférentes ne doivent être conservées que le temps nécessaire à la réalisation des finalités ayant présidé à leur collecte. Par exemple, la durée de conservation des données ne peut excéder la durée pendant laquelle l'enfant est inscrit à la colo ou à l'accueil de loisirs.
De plus, la numérisation ou la conservation d'une photocopie des pièces apparaissent selon la CNIL disproportionnées lorsqu'il est envisageable, au regard de la finalité, de ne procéder qu'à la retranscription dans un fichier des données pertinentes y figurant (ex. : adresse issue du justificatif de domicile).

Qui sont les destinataires des informations recueillies ?

Les destinataires varient en fonction des finalités des données collectées.
Si les données ou pièces ont vocation à être utilisées par différents destinataires, il convient de prévoir une gestion rigoureuse des droits d'accès et habilitations afin que ceux-ci n'aient accès qu'aux seules données nécessaires.
Par exemple, en ce qui concerne l'inscription des enfants aux accueils de loisirs et accueils de jeunes municipaux peuvent seuls, dans la limite de leurs attributions respectives, être destinataires des données :
• le maire, les élus ayant reçu une délégation en ce sens et les agents municipaux en charge de l'enfance et de la jeunesse ;
• les directeurs d'accueils de loisirs ou d'accueils de jeunes pour ce qui concerne les enfants inscrits dans leur structure ;
• le responsable de traitement des données, à charge pour lui de s'assurer que les informations collectées ne sont pas traitées ultérieurement de manière incompatible avec les finalités de son traitement.

Une école peut-elle partager son fichier des enfants inscrits avec le périscolaire afin d'éviter aux parents la double inscription et fourniture des justificatifs ?

Oui, mais seulement si les parents ont coché une case à cet effet lors de l'inscription de leur enfant à l'école. Par exemple, le directeur de l'accueil de loisirs périscolaire peut avoir accès aux données relatives à l'état vaccinal ou de santé concernant l'enfant. >>>

La mutualisation des fichiers d'inscription entre différentes prestations est-elle possible ?

Oui. Le recueil des données à caractère personnel par un autre responsable de traitement est possible. Mais l'application informatique utilisée doit disposer de séparations logiques sur les accès aux données. Par exemple, les jours de présence ou des données relatives à un défaut de paiement apparaissant sur le traitement de la cantine ne doivent pas être accessibles au traitement concernant les activités périscolaires.

Vis-à-vis de la CNIL : ce que change le RGPD

Fin des déclarations auprès de la CNIL

Le RGPD supprime les déclarations de fichiers à effectuer auprès de la CNIL. Seules certaines formalités préalables vont subsister (demande d'autorisation pour certains traitements de données de santé notamment).

La responsabilisation des acteurs

En contrepartie de la disparition de l'accomplissement de démarches administratives auprès de la CNIL, les administrations, sociétés et associations traitant des données à caractère personnel, mais aussi leurs prestataires et sous-traitants, sont désormais pleinement responsables de la protection des données qu'ils traitent.

Il leur appartient d'assurer la conformité au RGPD de leurs traitements de données personnelles tout au long de leur cycle de vie et d'être en mesure de démontrer cette conformité. Elles doivent donc se concentrer sur le respect de leurs obligations de fond (finalité, pertinence, durée de conservation, droits des personnes, sécurité, documentation).

Toute structure traitant des données personnelles est pleinement responsable de leur protection.

© LF

Quels sont les risques en cas de non-respect de cette réglementation ?

Avant tout, le RGPD a été mis en place pour les grandes entreprises du Web ainsi que toutes les startups, les applications mobiles ou sites Internet qui stockent de nombreuses informations personnelles. Les associations et ACM ne sont pas les premiers concernés par cette réglementation. Mais, en cas de contrôle, il est important de montrer sa bonne foi et d'être en mesure de présenter ce qui a été mis en place pour cartographier les données personnelles recueillies et démontrer qu'elles ne sont pas utilisées sans autorisation ou sans contrôle. La sanction en cas de non-conformité est de 4 % du chiffre d'affaires, ou 20 millions d'euros.

En pratique, en France

Le RGPD consacre et renforce les grands principes de la bien connue loi Informatique et Libertés, en vigueur depuis 1978, et accroît sensiblement les droits des citoyens en leur donnant plus de maîtrise sur leurs données.

Le RGPD marque le passage d'un mécanisme de formalités préalables (auprès d'une autorité de contrôle – en France, la CNIL) à un mécanisme d'autocontrôle : les gestionnaires des données sont érigés en « *responsables de traitement* ». La plupart des formalités préalables actuelles auprès de la CNIL (déclarations, autorisations) disparaissent donc, au profit d'une logique de conformité continue gérée par les organisateurs eux-mêmes. Ceux-ci devront veiller au respect des textes tout au long du cycle de vie de la donnée. En contrepartie de cette réduction du contrôle en amont, le RGPD renforce les pouvoirs de sanction des CNIL nationales.

La méthode en 6 étapes de la CNIL

Étape 1 : Désigner un pilote

Seuls les organismes publics et les entreprises dont l'activité de base amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « *sensibles* » doivent nommer un délégué à la protection des données.

Son rôle consistera notamment à :

- s'informer sur le contenu des nouvelles obligations ;
- sensibiliser les décideurs sur l'impact de ces nouvelles règles ;
- réaliser l'inventaire des traitements de données de votre organisme ;
- piloter la mise en conformité en continu.

Pour les autres, il faudrait au minimum désigner au sein de votre structure un « *référent RGPD* » qui se préoccupera de ces questions et en assurera le suivi.

Étape 2 : Cartographier vos traitements de données personnelles

Il s'agit de recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

Étape 3 : Fixer des priorités aux actions à mener

Identifiez les actions à mener pour vous conformer aux obligations actuelles. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées. Assurez-vous ainsi que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées.

Étape 4 : Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mettre en place des mesures permettant de répondre aux principaux risques et menaces qui pèsent sur la vie privée des personnes concernées par vos traitements. L'objectif est de construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD.

Étape 5 : Organiser les processus internes

Pour assurer un haut niveau de protection des données personnelles en permanence, vous devez mettre en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire). Il s'agit aussi de former les personnes chargées de gérer les données personnelles et de savoir quoi faire en cas d'incident.

Étape 6 : Documenter la conformité

Pour prouver votre conformité au RGPD, vous devez constituer et regrouper la documentation nécessaire : registres, modèles de demandes de consentement, etc. Les actions et documents réalisés à chaque étape précédente doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu. ◗

Roselyne Van Eecke

Être en conformité avec le RGPD pour une association, qu'est-ce que cela veut dire ?


© LF

Pour une association, cela signifie qu'il faut désormais pour toutes les informations déjà stockées sur ses adhérents, bénévoles :

- **Demander et sauvegarder le consentement des personnes pour le traitement des données les concernant.**
- **Informer la CNIL et les personnes concernées, dans les 72 heures, si leurs données personnelles ont été piratées dans votre base.**
- **Collecter uniquement les renseignements dont vous avez besoin, leur utilisation devant se faire de manière légitime, pertinente et proportionnée.**
- **Laisser la possibilité aux personnes, dont les données sont collectées, de connaître les éléments que vous conservez sur elles.**
- **Tracer l'ensemble des documents mis en place servant au traitement des données personnelles.**