Gouvernance des données personnelles du Groupe Arcade

Décembre 2018

Table des matières

1. Préambule

Les sociétés du Groupe Arcade inscrivent leur activité dans le respect des obligations relatives à la protection des données personnelles, et veillent à s'adapter en continu à leur évolution. Soucieuses de favoriser l'innovation tout en construisant une relation de confiance durable basée sur le partage de valeurs sociales responsables, les sociétés du Groupe Arcade ont mis en place depuis plusieurs années les moyens techniques et organisationnels nécessaires afin de protéger les données à caractère personnel qu'elles traitent.

Comme toute entreprise, mais plus encore dans le prolongement de notre mission de service d'intérêt général, et dans l'intérêt de chacune des entités constitutives du Groupe, chaque entité porte une attention particulière au respect des personnes, et à la protection de la vie privée et des informations individuelles ainsi qu'au respect de la confidentialité qui y est attachée.

La présente politique a pour objet de présenter les dispositions et les engagements pris par les sociétés du Groupe Arcade, en matière de protection des données personnelles. Elle s'applique à l'ensemble des traitements mis en œuvre par les sociétés du Groupe Arcade. Dans le texte ci-dessous le Groupe Arcade désigne toutes les sociétés qui le constituent et qui ont signé la Charte du Groupe Arcade - pôle HLM. Il est entendu que chaque société est responsable des traitements qu'elle met en œuvre.

2. Les délégués à la protection des données (DPO) au sein du Groupe

2.1 Le positionnement

Toute société qui rejoint le Groupe Arcade a la liberté de désigner le DPO mutualisé au niveau du Groupe ou de désigner son propre DPO. Le DPO mutualisé est relayé dans les sociétés qui l'ont désigné par un référent ou interlocuteur Informatique et libertés. DPO et interlocuteurs Informatique et libertés travaillent ensemble dans le cadre d'un réseau décrit ci-dessous. Ce travail en commun et la participation au réseau sont systématiques, quel que soit le choix fait par la société pour le DPO. En décembre 2018, en plus du DPO mutualisé, le Groupe compte deux autres DPO. Les trois DPO couvrent 2000 salariés et 300 000 personnes logées.

Les DPO ont reçu une lettre de mission de chacune des sociétés qui les ont nommés, et ont été désignés auprès de la CNIL par ces sociétés. Ils agissent dans le cadre de la charte du Groupe Arcade-pôle Hlm, paragraphe 5-3 Protection des données personnelles : « Respect des personnes, confidentialité, protection des données ».

Le Groupe permet aux délégués à la protection des données d'entretenir leurs connaissances spécialisées, par exemple par la participation à des formations, des conférences, tables-rondes ou par l'abonnement à des lettres d'information spécialisées. En outre, les sociétés mettent à la disposition de leur délégué à la protection des données les conditions de travail nécessaires à l'exercice de ses missions. Le Groupe bénéficie de l'appui d'un cabinet d'avocats spécialisé ; la relation et le budget sont gérés par le DPO mutualisé.

Le DPO mutualisé au niveau du Groupe est membre du collège des associés du GIE Arcade Services et rend compte directement au Président du Comité exécutif du Groupe.

2.2 La lettre de mission

Le délégué à la protection des données a les missions suivantes, conformément à sa lettre de mission :

- informer et conseiller le responsable de traitement sur les obligations en matière de protection des données à caractère personnel
- dispenser des conseils en ce qui concerne les études d'impact relatives à la protection des données et vérifier l'exécution de celles-ci en vertu du RGPD
- coopérer avec la CNIL et être son point de contact
- présenter un bilan annuel de ses activités
- analyser tout projet en relation avec un traitement de données à caractère personnel, qui est porté à sa connaissance
- tenir 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
- contrôler le respect des dispositions légales et règlementaires en matière de protection des données et des règles internes du responsable de traitement, notamment en ce qui concerne :
    - la répartition des responsabilités
    - la sensibilisation et la formation du personnel
- auditer les traitements et leurs conditions de mise en œuvre
- piloter la production et la mise en œuvre de la documentation nécessaire à la conformité (politiques, lignes directrices, procédures, règles de contrôle, …)
- piloter et contrôler la tenue du registre des traitements par l'interlocuteur désigné par le responsable de traitement
- si besoin, informer le responsable de traitement des manquements constatés, conseiller dans les mesures à prendre pour y remédier, soumettre les arbitrages nécessaires ;
- assister et conseiller le responsable de traitement lors
    - des demandes d'exercice de droits, de réclamations et de requêtes formulées par des personnes concernées
    - d'éventuelles violations de données.

Pour permettre au délégué à la protection des données de mener à bien ses missions, le responsable du traitement s'engage à :

- veiller à ce qu'il puisse exercer ses missions en toute indépendance, et à ce qu'il ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions de DPO/DPD.
- l'associer d'une manière appropriée et en temps utile
    - à toutes les questions relatives à la protection des données à caractère personnel (analyse d'impact, exercice des droits des personnes, notification des violations de données, …)
    - à tout projet de création ou de modification de tout traitement de données à caractère personnel
- fournir les ressources budgétaires, humaines et matérielles, nécessaires pour exercer ses missions. En particulier, le responsable de traitement désigne en interne un ou plusieurs interlocuteur(s) dédié(s) à la protection des données personnelles, disposant des compétences, des ressources et de l'autorité nécessaires. Ce(s) interlocuteur(s) participe(nt) activement à la conformité du responsable de traitement. Il(s) est (sont) notamment chargé(s) de mettre en œuvre les actions nécessaires à la création et au maintien des conditions de conformité du responsable de traitement, en collaboration étroite avec le DPO. Le DPO notifie au responsable de traitement toute insuffisance dans les moyens et ressources qui lui sont alloués pour réaliser ses missions.

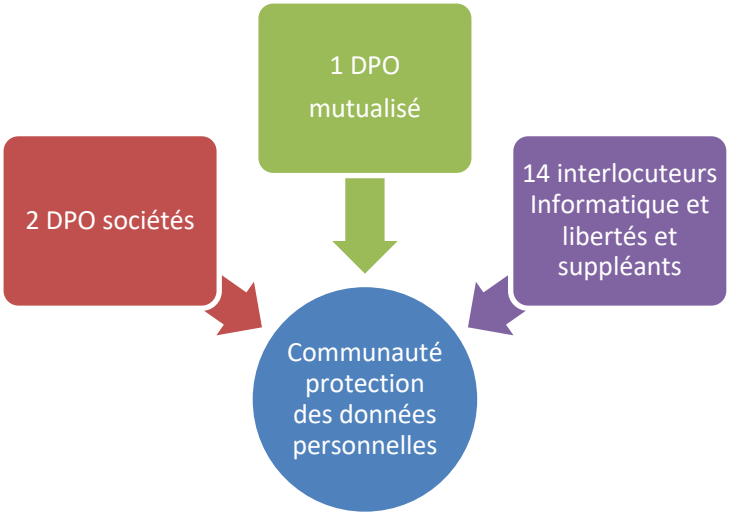
- communiquer et rendre accessibles les informations et la documentation nécessaires à l'exécution de ses missions,
- participer au maintien et à l'acquisition des connaissances et qualification du DPO
- veiller à ce que les missions qu'il pourrait lui confier n'entraînent pas de conflit d'intérêt avec ses missions de DPO.

3. La communauté « Protection des données personnelles »

Les sociétés qui ont désigné le DPO mutualisé Groupe, ont également nommé un Interlocuteur Informatique et libertés, directement rattaché au Directeur Général de la société. Les DPO, auxquels s'ajoutent les interlocuteurs Informatique et libertés, forment la communauté « Protection des données personnelles » du Groupe. Cette organisation s'inscrit dans une approche d'amélioration continue de l'application de la règlementation Informatique et Libertés. Elle permet de :

- diffuser une culture de protection des données personnelles au sein des sociétés du Groupe et au plus près du terrain;
- favoriser le respect de la législation par la mutualisation des compétences et le partage d'expérience Informatique et Libertés ;
- favoriser le maintien d'une adéquation permanente entre les recommandations de la CNIL et la règlementation pour la protection des données personnelles avec les réalités « métier » quotidiennes dans les sociétés.

En décembre 2018, la communauté « Protection des données personnelles » du Groupe Arcade regroupe :



En plus des missions décrites plus haut, le DPO groupe anime la communauté. Par ailleurs, il se rend dans les sociétés, notamment pour rendre compte de l'exécution de ses missions, aussi souvent que ses missions l'exigent ou que le responsable de traitement le demande.

Les interlocuteurs Informatique et libertés, comme les DPO, participent activement à la conformité du responsable de traitement. Ils sont notamment chargés de :

- mettre en œuvre les actions nécessaires à la création et au maintien des conditions de conformité du responsable de traitement, en collaboration étroite avec le DPO
- tenir le registre des traitements de la société
- former les collaborateurs, avec l'appui du DPO Groupe si besoin

- faire respecter la règlementation liée à la protection des données personnelles dans leur société
- répondre aux questions des collaborateurs de la société, en s'appuyant si besoin sur le DPO Groupe
- répondre aux demandes d'exercice des droits dans leur société.

Le DPO Groupe est joignable à l'adresse dpo@groupe-arcade.com ou par courrier à l'adresse suivante : Groupe Arcade DPO, 59, rue de Provence 75009 Paris.

4. Les instances de la gouvernance

4.1 Comité technique Informatique et libertés

La communauté pour la protection des données personnelles groupe se réunit une fois par mois en télé-conférence (Skype) et deux à trois fois par an en présentiel. Le DPO Groupe anime ces réunions.

Les réunions mensuelles ont pour objet le traitement de sujets spécifiques, le point sur l'actualité dans les sociétés ou au niveau de notre environnement, ainsi qu'une veille règlementaire.

Les journées en présentiel ont pour objectif la montée en compétence du réseau, par un apport théorique sur des sujets précis, ainsi que la définition de la position Groupe et la production de livrables dans le cadre de la mise et du maintien des sociétés en conformité.

Le comité a notamment pour missions :

- de promouvoir la culture et la conformité informatique et libertés au sein du Groupe en s'assurant en particulier de la sensibilisation et de la formation de tous.
- de traduire la règlementation en dispositifs opérationnels pour les métiers
- d'évaluer les risques en matière de protection des données
- de proposer aux directions générales la mise en place ou l'évolution des mesures techniques, organisationnelles, de formation ou autres, nécessaires au maintien de la conformité.
- d'assurer l'évaluation du dispositif de conformité des sociétés

En 2018 et 2019, il est en outre chargé du pilotage de la mise en conformité des sociétés du Groupe avec le RGPD.

Le comité travaille en lien avec les communautés métiers ou thématiques qui fonctionnent au sein du Groupe. Le lien se fait via les membres de la communauté protection des données personnelles, qui relaient les travaux et réflexions auprès des autres communautés auxquelles ils peuvent participer du fait de leur métier, RH, gestion locative, informatique, maîtrise des risques par exemple. Il s'opère également par les contacts pris par le DPO Groupe avec les autres animateurs de communauté.

Le travail inter-communautés permet d'associer des acteurs différents et complémentaires à la définition et l'expérimentation des mesures à prendre. Il vise également à apporter des réponses réalistes et opérationnelles aux questions posées au quotidien, facilitant ainsi l'application de la règlementation. Il facilite enfin le retour d'expérience et sa prise en compte.

4.2 Le rôle du sponsor

Un sponsor, directeur général de l'une des sociétés du groupe, appuie le DPO groupe pour l'animation de la communauté. Il relaie les travaux du comité technique auprès des autres directeurs généraux à l'occasion des réunions de coordination des directeurs généraux. A son initiative ou à la demande du DPO groupe il peut alerter les directeurs généraux en cas de besoin.

A l'initiative conjointe du sponsor et du DPO groupe, un comité de gouvernance pourra être réuni, par exemple pour intégrer une évolution significative liée à l'utilisation des données personnelles. Ce comité pourra établir des limites et définir ce qui n'est pas compatible avec les valeurs du groupe. Les compétences à mobiliser seront déterminées en fonction du sujet à traiter.

4.3 Le rapport annuel

Le DPO groupe et la communauté pour la protection des données personnelles rendent compte de leur activité dans un bilan annuel, destiné aux responsables de traitement.

Ce bilan est élaboré au cours du premier trimestre de chaque année. Il est composé d'un tronc commun groupe qui décrit les actions mutualisées, rédigé par le DPO groupe, et d'une partie spécifique aux actions menées dans les sociétés, rédigées par chaque interlocuteur Informatique et libertés. Le comité technique valide le tronc commun.

Les DPO sociétés rédigent leurs propres bilans, en incorporant le tronc commun groupe.

5. Effectivité des droits des personnes

Une procédure spécifique permet de gérer les réclamations et les demandes relatives à l'exercice des droits des personnes.

La procédure est destinée à faciliter l'exercice des droits des personnes (droit d'accès, de rectification, d'effacement, de limitation du traitement, à la portabilité, d'opposition, de définir le sort de ses données après son décès), en comprenant les modalités d'identification/authentification de la personne concernée exerçant ses droits et permettant de respecter les délais de réponse.

Le DPO ou l'interlocuteur Informatique et libertés selon le cas, fait office de point de contact des personnes concernées et s'assure du traitement des réclamations adressées au responsable de traitement. L'interlocuteur informatique et libertés de l'entité concernée traite lui-même la demande.

6. Politiques interne et externe de protection des données

Le groupe Arcade a établi ses politiques de protection des données, une politique interne concernant la protection des données des salariés, stagiaires, candidats à un emploi et intérimaires, et deux politiques externes, concernant la protection des données des locataires et des demandeurs de logement d'une part, des clients et des prospects d'autre part.

Ces politiques de protection des données incluent l'ensemble des principes nécessaires pour garantir la mise en œuvre de traitements équitables et transparents. Elles comprennent notamment les

coordonnées du responsable de traitement, celles du délégué à la protection des données, ainsi que les principes énoncés par le règlement européen général sur la protection des données, au regard notamment de la mise en œuvre de traitements licites, du respect des droits des personnes, des éventuels transferts vers un pays tiers, des destinataires des données collectées, de la sécurité et de la durée de conservation des données collectées.

Le délégué à la protection des données contrôle le respect des politiques mises en place en matière de protection des données.

Ces politiques seront réexaminées et actualisées si nécessaire, a minima tous les trois ans.

7. Des salariés informés

Les données personnelles sont des données confidentielles. Les salariés des sociétés du Groupe sont sensibilisés, informés et formés sur l'importance d'assurer la sécurité et la confidentialité des données qu'ils traitent.

Des actions de sensibilisation sont réalisées par le délégué à la protection des données et par les interlocuteurs informatique et libertés ; elles sont adaptées au public visé. Ces actions peuvent prendre la forme de :

- formation ;
- diffusion de bonnes pratiques ;
- réalisation de supports de communication ;
- rappel de consignes ;
- création d'outils pédagogiques et méthodologiques.

En outre, afin de permettre la diffusion des bonnes pratiques que chacun au sein de l'entreprise doit respecter en matière de protection des données, il sera établi une charte de protection des données à l'intention des collaborateurs. Ce document, en cours de rédaction, sera publié au premier semestre 2019.

8. Validation des activités touchant à la protection des données personnelles

8.1 Consultation préalable du DPO

Le délégué à la protection des données ou l'interlocuteur informatique et libertés est consulté préalablement à tout déploiement de projet ayant une incidence sur la protection des données par le chef de projet et par tout opérationnel souhaitant mettre en œuvre un traitement de données personnelles ou en modifier un. Il est associé systématiquement en amont des réflexions sur toutes les questions relatives à la protection des données. Il procédera à une analyse à chaque fois qu'il le jugera utile, dans le but d'introduire le respect de la protection des données par défaut et dès la conception du projet. Les modalités de gestion de projet en vigueur dans les sociétés du Groupe ont été modifiées à cet effet. Une grille d'analyse d'un traitement a été mise au point.

8.2 Etudes d'impact

Lorsqu'il est consulté, le délégué à la protection des données s'assure que les traitements soumis à l'analyse d'impact font bien l'objet d'une analyse. Dans ce cas, le délégué à la protection des données informe l'opérationnel en charge du projet de la nécessité de procéder à une analyse de risque pour le traitement concerné, et l'assiste pour la réalisation. A cet égard, le délégué à la protection des données peut également demander à un tiers d'intervenir.

Le délégué à la protection des données est consulté pour toute analyse d'impact et vérifie son exécution. En tout état de cause, les résultats de l'analyse d'impact sont remis au délégué à la protection des données qui formulera ses recommandations avant la mise en œuvre du traitement. Si le responsable de traitement ne suit pas les recommandations du délégué à la protection des données, la documentation de l'analyse d'impact doit en mentionner la raison.

8.3 Validation des documents

Les documents sortants qui comportent des données personnelles, contrats ou formulaires de collecte de données font, dans la mesure du possible, l'objet d'un visa de l'interlocuteur Informatique et libertés de la société, qui sollicite le délégué à la protection des données s'il le juge utile, afin qu'il s'assure que les documents répondent aux contraintes légales. La même démarche de validation s'applique pour les productions web.

9. Registre des traitements

Chaque entité du Groupe Arcade tient un registre des traitements mis en œuvre, pour répondre aux exigences du règlement européen sur la protection des données.

Les interlocuteurs informatique et libertés désignés tiennent à jour le registre. En cas de changement dans les modalités de mise en œuvre d'un traitement, ils apportent au registre les modifications nécessaires.

10. Sécurité

Compte tenu des nouvelles obligations en matière de notification des failles de sécurité à la Commission Nationale de l'Informatique et des Libertés (CNIL), une procédure en matière de réponse à apporter lors d'une faille ou incident de sécurité a été établie.

La procédure comprend notamment une obligation de notification à la CNIL, si possible dans les 72 heures après avoir pris connaissance de la faille, ainsi que les actions à mettre en œuvre selon les cas, en particulier, l'information des personnes, le dépôt de plainte...

11. Evaluation du dispositif de conformité en matière de protection des données

Le délégué à la protection des données contrôle le respect de la réglementation informatique et libertés. Il s'assure que les politiques et procédures définies en ce domaine sont respectées et peut

diligenter, ou faire diligenter, des audits pour un examen de conformité périodique permettant de s'assurer que les traitements considérés comme les plus sensibles au regard des risques sont mis en œuvre dans le respect des contraintes légales.

En cas d'écarts constatés, le délégué à la protection des données fera part à la direction générale d'un plan d'actions de remédiation.
Le risque de non-conformité à la règlementation européenne et nationale en matière de protection des données personnelles, à travers ses différentes composantes, est intégré dans le dispositif de maîtrise des risque mis en œuvre dans les sociétés. Une fiche risque type a été établie à cet égard.

12. Glossaire

Commission Nationale Informatique et Libertés (CNIL) : la CNIL est le régulateur français des données personnelles.

Données à caractère personnel : il s'agit de toutes informations relatives à une personne physique pouvant être identifiée directement ou indirectement.

Traitement : toute opération ou tout ensemble d'opérations automatisés ou non, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Personne concernée : la personne concernée désigne les personnes dont les données font l'objet d'un traitement.

Responsable du traitement de données à caractère personnel : il s'agit de l'entité ou du service qui détermine les finalités et les moyens d'un traitement.

RGPD : Règlement Général pour la Protection des Données

Sous-traitant : de façon générale, toute société traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant