

PROTECTION DES DONNÉES PERSONNELLES



Crédit photo :

POLITIQUE INTERNE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL AU MUSÉE DU LOUVRE

(présentée au Comité hygiène, sécurité et conditions de travail du 13 février 2020 et au Comité technique du 21 février 2020)

TABLE DES MATIÈRES

- ◆ 1. Introduction
- ◆ 2. Délégué à la protection des données
- ◆ 3. Définitions
- ◆ 4. Principes
 - 4.1 Licéité
 - 4.2 Loyauté et transparence
 - 4.3 Limitation des finalités
 - 4.4 Minimisation des données et durées de conservation
 - 4.5 Exactitude des données
 - 4.6 Respect des droits des personnes
 - 4.7 Sécurité, confidentialité et protection des données
 - 4.8 Responsabilité
 - 4.9 Encadrement des transferts hors Union européenne
- ◆ 5. En pratique
- ◆ 6. Pour aller plus loin

1. INTRODUCTION - CADRE GÉNÉRAL

- ◆ Textes de référence :

[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 dit « RGPD », entré en vigueur le 25 mai 2018](#)

[Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles](#)

Ces textes ont vocation à renforcer les droits des personnes concernant leurs données personnelles et à responsabiliser les acteurs traitant ces données.

Les obligations découlant de ces objectifs se matérialisent pour l'EPML notamment par :

- ◆ la désignation en 2019 du cabinet Alain Bensoussan en tant que Délégué à la protection des données (DPD) qui a vocation à accompagner les établissements dans leur mise en conformité RGPD et à en assurer le suivi et le contrôle;
- ◆ la mise en place d'une organisation propre : des instances de gouvernance - comité de suivi et équipe projet - chargées de piloter, déterminer et assurer le suivi des actions de mise en conformité ; et des « référents informatique et libertés » dans chaque département et direction ;
- ◆ la tenue d'un registre des activités de traitement. Dans le cadre du principe de responsabilisation des acteurs, le dispositif qui consistait à procéder à des déclarations de traitement auprès de la CNIL a été supprimé au profit de la tenue en interne d'un registre des traitements de données à caractère personnel ;
- ◆ la mise en conformité des traitements existants au moyen de plan d'actions spécifiques à chaque département et direction.
- ◆ la conduite, pour tous les traitements à risque, d'une étude d'impact faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées.
Cela concerne le système de billetterie, le système de vidéo protection et le système de gestion de la relation visiteur ;
- ◆ l'application du concept de protection des données dès la conception et par défaut (prise en compte des données personnelles dès la création d'une application ou d'un outils susceptible de traiter des données personnelles) notamment par l'adoption d'une procédure relative à la création et l'analyse des nouveaux traitements de l'établissement;
- ◆ l'adoption d'une procédure de notification des violations de données personnelles à la CNIL et, en cas de risque élevé pour les droits et les libertés fondamentales des personnes physiques, la communication aux personnes concernées par ladite violation ;
- ◆ la garantie d'une information des personnes susceptibles d'être concernées par les traitements (mentions légales des sites ; dispositions contractuelles) ;
- ◆ la mise en place de procédures qui permettent aux personnes d'exercer leurs droits tels que accès, suppression, modification des données personnelles ;
- ◆ l'établissement de politique(s) de protection des données : une politique externe, et une politique interne quant à elle destinée aux agents du musée, présentée ci-dessous.
En effet, chaque agent peut être amené dans l'exercice de ses fonctions à collecter, conserver ou traiter des données personnelles.

La politique interne a donc vocation d'une part à préciser l'ensemble des définitions utiles et nécessaires à la compréhension de la réglementation et d'autre part à décrire les règles de bonne conduite pour assurer la protection des données à caractère personnel des personnes concernées par les traitements de l'établissement;

Cette politique pourra être amenée à évoluer en fonction du contexte légal et réglementaire applicable.

2. DÉLÉGUÉ À LA PROTECTION DES DONNÉES

L'Etablissement Public du Musée du Louvre a désigné le 13 mars 2019, auprès de la Commission nationale de l'informatique et des libertés (CNIL), le cabinet d'avocats

Alain Bensoussan Selas en qualité de délégué à la protection des données (DPO) de l'Etablissement Public du Musée du Louvre.

En cette qualité de DPO, le cabinet Alain Bensoussan Selas a notamment pour mission d'informer et de conseiller l'Etablissement public du Musée du Louvre sur les obligations

qui lui incombent en vertu de la réglementation sur la protection des données personnelles mais aussi de contrôler, d'une manière indépendante, le respect de ces obligations par l'Etablissement Public du Musée du Louvre.

En cas de questions relatives à la protection des données à caractère personnel, votre interlocuteur demeure la direction financière juridique et des moyens (DFJM) et plus particulièrement la sous-direction juridique et de l'achat public et la sous-direction des systèmes d'information (cellule RGPD) qui peuvent être contactées à l'adresse suivante : rgpd@louvre.fr.

En tant que de besoin, votre demande pourra être traitée avec l'assistance du DPO.

3. DÉFINITIONS

Pour bien comprendre la réglementation sur la protection des données à caractère personnel, il est important d'en maîtriser les concepts principaux, dont vous trouverez une définition ci-dessous :

- ◆ Données à caractère personnel :

Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne physique peut être identifiée notamment par référence à élément tel qu'un nom, des données de localisation (adresse), une photographie, un n° de téléphone, une adresse mail, ou un ou plusieurs éléments spécifiques propres à son identité physique, génétique, économique, culturel, social... ces données sont des données à caractère personnel.

◆ Données à caractère personnel particulières :

Il s'agit de données sensibles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale,

ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le traitement de ces données est par principe interdit. Si de telles données devaient être recueillies (ex donnée de santé pour la médecine de prévention) il convient de se rapprocher de la cellule RGD.

◆ Traitement de données à caractère personnel :

Constitue un traitement de données à caractère personnel toute opération effectuée ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de 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.

◆ Responsable d'un traitement de données à caractère personnel :

Au sens général, le responsable de traitement est celui qui détermine à la fois les finalités et les moyens d'un traitement. C'est sur lui que pèse la majorité des obligations de protection des données, dont il est le garant.

Ainsi, le responsable d'un traitement peut être toute personne physique ou morale, autorité publique, service ou tout autre organisme qui détermine, seul ou conjointement avec d'autres, les finalités et les moyens du traitement (Alain Bensoussan, Règlement européen sur la protection des données, textes, commentaires et orientations pratiques, Larcier 2016 p.66.)

L'EPML est responsable de traitement.

◆ Sous-traitant :

Il s'agit de la personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable du traitement.

Le sous-traitant ne peut procéder à des opérations de traitement de données à caractère personnel que sur instructions du responsable du traitement.

En d'autres termes, il s'agit d'une entité juridique distincte du responsable du traitement qui traite des données à caractère personnel pour le compte de ce dernier et sur ses instructions.

4. PRINCIPES

La réglementation relative à la protection des données à caractère personnel se décline en plusieurs grands principes qu'il vous est demandé d'observer scrupuleusement.

(Article 5 du RGPD)

◆ 4.1 Licéité

Pour mettre en œuvre un traitement de données à caractère personnel, les données doivent avoir été collectées de manière licite (caractère de ce qui est autorisé par la loi.)

Cela signifie que la personne a dû donner son consentement quant au traitement de ses données.

D'autres modalités sont envisagées par les textes : la collecte des données peut être nécessaire à l'exécution d'un contrat, une mission d'intérêt public, ou nécessaire aux intérêts légitimes de l'EPML.

Dans tous les cas, ce fondement doit être identifié et il convient de s'en assurer.

◆ 4.2 Loyauté et transparence

Les données à caractère personnel doivent être traitées de manière transparente.

Cela signifie que les données ne doivent pas être collectées et traitées à l'insu des personnes concernées.

Aussi, avant de mettre en œuvre un traitement, il est nécessaire de vérifier que les personnes concernées ont été informées :

◆ des traitements portant sur les données à caractère personnel les concernant ;

- ◆ de leurs droits.

Des mentions permettant de diffuser clairement cette information (sur un site internet, par affichage d'un panneau, dans un contrat...) doivent être mises en œuvre.

De même, il convient d'être en mesure de répondre aux questions des personnes concernées de la manière la plus complète possible.

Si vous vous procurez des données à caractère personnel auprès de tiers, il faut vous assurer au préalable que ces tiers ont les droits nécessaires pour collecter et céder de telles données.

◆ 4.3 Limitation des finalités

Il convient de déterminer clairement les finalités de votre traitement. Les données doivent uniquement être collectées pour des finalités spécifiques, explicites et légitimes.

Toute réutilisation des données pour des finalités incompatibles avec les finalités initiales est prohibée.

◆ 4.4 Minimisation des données et durées de conservation

Seules peuvent être collectées des données à caractère personnel adéquates, pertinentes et limitées à ce qui est nécessaire à la réalisation des finalités du traitement.

Il convient donc de s'interroger sur la pertinence des données collectées au regard des finalités du traitement à mettre en œuvre, il ne faut pas être excessif dans la collecte des données.

En particulier, il est interdit de collecter et de traiter des données sensibles en dehors des cas particuliers spécifiquement prévus par la réglementation applicable.

Dès la création de votre traitement, il est nécessaire de déterminer la durée pendant laquelle vous aurez besoin de conserver les données pour pouvoir atteindre l'objectif du traitement.

◆ 4.5 Exactitude des données

Il est indispensable de s'assurer régulièrement que les données à caractère personnel que vous traitez sont exactes et si besoin, il faut procéder à la mise à jour des données et plus largement des bases de données.

Toutes les mesures raisonnables doivent être prises pour que les données inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

Les zones de commentaires libres sont par principe prohibées.

Si elles sont absolument nécessaires au traitement, une vigilance particulière est attendue : aucune information excessive ne doit figurer dans lesdites zones.

◆ 4.6 Respect des droits des personnes

Les personnes dont les données font l'objet d'un traitement bénéficient des droits suivants :

- ◆ le droit à l'information ;
- ◆ le droit d'accès ;
- ◆ le droit de rectification ;
- ◆ le droit à l'effacement (« droit à l'oubli ») ;
- ◆ le droit à la limitation du traitement ;
- ◆ le droit à la portabilité ;
- ◆ le droit d'opposition ;
- ◆ le droit de définir des directives relatives à la conservation, à l'effacement et à la communication des données personnelles après la mort.

Les personnes concernées doivent être en capacité d'exercer leurs droits, il faut pour cela leur donner les moyens de le faire.

Les adresses mails donneespersonnelles@louvre.fr pour les personnes extérieures au Musée et l'adresse rgpd@louvre.fr pour les agents ont été créées spécifiquement à cet effet.

Toute demande d'une personne concernée en lien avec l'exercice de ses droits doit être traitée de manière efficace.

Une procédure spécifique est mise en œuvre au sein de l'établissement pour y parvenir.

Vous pouvez consulter la cellule RGPD pour vous accompagner dans ces démarches.

4.7 Sécurité, confidentialité et protection des données

Les fichiers doivent être protégés et les données sécurisées. A cet égard, il faut respecter les mesures de sécurité définies notamment dans les documents diffusés en interne.

Les données à caractère personnel que vous traitez doivent rester confidentielles : cela suppose de ne pas divulguer ces informations auprès d'autres services ou auprès de tiers qui ne seraient pas habilités à en prendre connaissance.

Un niveau de protection adéquat sur vos traitements de données doit être maintenu, et ce dès les premières étapes de leur conception. De même, toutes les mesures techniques et organisationnelles appropriées doivent être mises en place pour garantir que seules les données nécessaires au regard de chaque finalité seront traitées. Ces mesures doivent garantir que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

Si vous avez recours à un sous-traitant pour mettre en œuvre un traitement de données, vous devez lui imposer contractuellement des obligations fortes de sécurité, de confidentialité et de coopération.

Un document spécifique concernant les obligations des sous-traitants a été élaboré, il peut être annexé au marché public ou au contrat à conclure avec le sous-traitant.

La cellule RGPD est à votre disposition pour vous accompagner dans la préparation de cette annexe.

4.8 Responsabilité

D'une manière générale, il convient d'être en mesure de démontrer votre respect des points détaillés susmentionnés.

Pour cela, il est nécessaire d'établir et tenir à jour toute la documentation requise, afin de permettre au Musée du Louvre de prouver son respect de la réglementation relative à la protection des données personnelles.

4.9 Encadrement des transferts hors Union européenne

Les flux de données à caractère personnel doivent être maîtrisés.

Le transfert de données à caractère personnel vers un autre pays ne peut être envisagé qu'après avoir vérifié auprès de la cellule RGPD et du Délégué à la protection des données que vous êtes autorisé à le faire.

5. EN PRATIQUE

THEME	A FAIRE	A NE PAS FAIRE
Lors de la collecte et du traitement des données	Identifier précisément les finalités initiales de la collecte des données pour les rendre spécifiques, déterminées et explicites.	Collecter des données dont le responsable du traitement ne connaît pas l'origine.
	Examiner les mentions d'information pour déterminer si les finalités de la collecte et du traitement des données sont spécifiques, déterminées et explicites.	Traiter des données interdites (santé, religion, opinions politiques, notamment) au regard des conditions dans lesquelles le traitement est mis en œuvre.
	Analyser la licéité des finalités de la collecte et du traitement des données	Collecter des données sans informer les personnes sur les finalités de la collecte et du traitement des données.
		Utiliser un traitement pour d'autres finalités sans se poser la question de la compatibilité de ces nouvelles finalités avec les finalités initiales.
Qualité des données	Mettre à jour périodiquement les traitements et fichiers de données à caractère personnel.	Conserver et traiter des données inexactes, sans procéder à leur effacement ou à leur rectification
		Dans les zones de commentaires libres, sont interdites :

Pour les zones de commentaires libres, s'assurer que seules des données nécessaires au traitement sont collectées et que les informations renseignées dans ces zones ne revêtent aucun caractère disproportionné

- les appréciations d'ordre personnel, jugements de valeur : expressions injurieuses, désobligeantes, blessantes ;

- les appréciations sur le comportement de la personne (exemples : « personne timide », « mauvais caractère », etc.) ;

- ,la présence de données relatives à l'origine raciale, ethnique, aux opinions politiques, religieuses, philosophiques, à l'appartenance syndicale, à la santé, à la vie sexuelle des personnes concernées.

Durée de conservation des données

Vérifier qu'il existe des durées de conservation pour chaque catégorie de données traitées au sein du traitement.

Procéder à des extractions Excel des données d'une application et conserver ce fichier sans s'assurer de respecter la durée de conservation initiale.

Apprécier la durée de conservation par rapport à la finalité poursuivie.

Encourager ou faciliter les extractions Excel.

Ne pas définir de durée de conservation dans les applications lors de la phase de développement.

Destinataires des traitements

Identifier les destinataires de chaque traitement et les indiquer dans le champ correspondant du registre des activités de traitement.

Communiquer les données à des tiers sans vérifier leur habilitation.

Transferts de données

Identifier les transferts réalisés hors de l'Union européenne.

Mettre en œuvre des transferts de données vers des pays hors Union européenne n'ayant pas de protection adéquate sans encadrement juridique.

Vérifier à quel cadre juridique est soumis le transfert vers les pays identifiés.

Information des personnes concernées

S'assurer que les personnes concernées ont bien été informées du traitement qui va être mis en œuvre. Le cas échéant, informer les personnes concernées.

Ne pas apposer de mention ou la faire figurer de telle manière qu'elle soit peu visible et peu compréhensible.

Respect du droit des personnes

En cas de réception d'une demande d'exercice d'un droit, se référer à la procédure de gestion des droits.

Ne pas respecter le délai pour envoyer une réponse.

S'abstenir de répondre ou de traiter les demandes légitimes.

Imputer des frais à la personne exerçant son droit d'opposition ou des frais supérieurs au coût de la copie en cas de demande de copie.

Considérer comme abusive toute demande d'accès d'une personne sur les informations la concernant.

6. POUR ALLER PLUS LOIN

En cas de difficulté dans la compréhension ou l'application des règles définies dans la présente politique, vous pouvez contacter la direction Financière, Juridique et des Moyens (DFJM) et plus particulièrement la sous-direction juridique et de l'achat public et la sous-direction des systèmes d'information, qui peuvent être contactées à l'adresse suivante : rgpd@louvre.fr

Dernière mise à jour le 26.08.2021

Pour toutes questions ou suggestions sur le contenu cette page merci de contacter : rgpd@louvre.fr

Dernière mise à jour effectuée le 01/09/2021.

Pour toutes questions ou suggestions sur le contenu de cette page, merci de contacter :