FAQ protection des données

Une sélection de questions relatives à la protection des données pour les musées suisses.

A– Questions spécifiques

1) Publication de données personnelles :

- Dans quelle mesure les données personnelles collectées par un musée peuvent-elles être publiées ?
- Peut-on par exemple distribuer une liste de participant-e-s à des congrès ?
- Quelles informations peuvent être publiées sur le site web ou dans le rapport annuel ?

La publication de données personnelles constitue un traitement de données (→ voir à ce sujet sous B - Exigences générales en matière de protection des données, question 1). En tant que telle, elle doit être conforme aux principes de traitement des données (→ B - Exigences générales en matière de protection des données, question 7).

Pour les musées qui n'agissent pas en tant qu'organes publics (et qui sont donc soumis au droit de la protection des données pour les personnes privées de la LPD[1]), les règles suivantes s'appliquent :

- Ici, l'accent est mis sur les finalités pour lesquelles les données personnelles ont été collectées et sur le fait de savoir si les personnes concernées ont été informées que les données personnelles seraient publiées.
- Information:
    - Si l'on a informé les personnes concernées de la publication dès le début (c'est-à-dire lors de la collecte des données personnelles), celle-ci est en principe autorisée.
- Finalité:
    - Si la publication des données était reconnaissable dès le départ pour la personne concernée (par exemple en indiquant dans le formulaire d'inscription au congrès « Une liste des participant-e-s sera envoyée avant le début du congrès »), elle est en principe autorisée.
    - Mais si l'on veut extraire les données de leur contexte de traitement initial et les traiter dans un autre but, cela constitue une violation du principe de finalité.
    - Exemple : une photo d'une conservatrice indépendante, prise pour la réalisation d'un panneau d'information d'une exposition passée, doit maintenant figurer dans la newsletter du musée adressée à 2’000 personnes et faisant la promotion d'une autre exposition à venir.
    - Pour que ce changement de finalité soit autorisé, il doit être justifié. Cela peut se faire notamment en demandant l'accord de la conservatrice. Il n'est pas nécessaire de le faire explicitement et par écrit (on pourrait l'appeler et obtenir son accord par téléphone), mais il est recommandé de documenter l'accord, ce qui se fait le plus simplement par un document écrit et signé.

Conseils pratiques:

- Les coordonnées d'une personne assumant un rôle spécifique au sein du musée (par exemple, responsable d'un secteur d'activité ou d'une exposition) peuvent être publiées sur le site web du musée ou dans le rapport annuel, avec les informations nécessaires, dans la

[1] Loi fédérale sur la protection des données (Loi sur la protection des données, LPD) du 25 septembre 2020, RS 235.1. Lorsque la LPD est mentionnée dans la FAQ, elle fait référence à la version totalement révisée qui entrera en vigueur le 1er septembre 2023.

mesure où cela fait partie de l'accomplissement de la mission de la personne concernée (par exemple, parce qu'elle doit pouvoir être contactée dans le cadre de sa fonction).

- Les données relatives à des personnes connues du public (« personnes de la vie publique », ce qui devrait être régulièrement le cas pour les artistes ou les personnes ayant une importance historique) et qui font partie de leur activité publique peuvent être traitées et donc également publiées.
- S'il s'agit de prendre des photos de personnes participant à une conférence et de les publier, un véritable consentement n'est normalement pas nécessaire (au-delà de l'information → voir ci-dessus). Selon le contexte, il peut toutefois être recommandé, pour des raisons de preuve, de documenter un consentement vérifiable (signature, case à cocher, etc.).

Autre élément à prendre en compte :

- Sécurité : il convient d'examiner comment les données peuvent être sécurisées de manière adéquate. Par exemple, l'ensemble des photos des participant-e-s à un congrès ne peut être accessible que dans une zone du site web protégée par un mot de passe (au lieu d'être librement accessible), il en va de même pour une liste de participant-e-s.
- Proportionnalité : si l'on souhaite utiliser des photos d'un événement dans une publication ou une newsletter, il convient de choisir, dans la mesure du possible, celles qui ne montrent pas un nombre excessif de visages directement identifiables. Pour les listes de participant-e-s, il est plus justifié de publier le nom, le prénom et l'adresse e-mail que l'adresse et le numéro de téléphone.

Pour les musées qui agissent en tant qu'organes publics (et qui sont donc soumis au droit de la protection des données pour les organes fédéraux de la LPD ou au droit cantonal de la protection des données), il convient en outre de vérifier si les bases légales existantes sont suffisantes pour la communication des données personnelles.

2) Comment traiter les données personnelles dans le cadre de la recherche de provenance ? Ou comment garantir un traitement des données conforme à la protection des données, compte tenu du fait que les personnes décédées ne peuvent plus donner leur consentement ?

En simplifiant à l'extrême, on peut dire ce qui suit :

En principe autorisé	A vérifier au cas par cas et à résoudre avec une pesée des intérêts ou un consentement.
Recherche de provenance par le musée	Communication à des tiers de données concernant des personnes encore vivantes
Communication de données personnelles concernant des personnes décédées depuis très longtemps	Communication à des tiers de données concernant des personnes décédées lorsque les proches pourraient éventuellement faire valoir un droit à la protection de leur réputation.

Dans le cadre de la recherche de provenance, le droit de la protection des données n'est applicable que tant que le musée traite des données personnelles de personnes encore vivantes.

Le décès met fin à la personnalité et donc à l'application du droit de la protection des données (voir ci-dessous). La recherche de provenance portant sur des données personnelles de personnes décédées ne pose donc a priori aucun problème du point de vue du droit de la protection des données (voir toutefois ci-dessous pour la protection de la mémoire).

Remarque : pour le traitement de données par des organes publics, il convient de vérifier au cas par cas quelle est la situation légale et s'il existe des restrictions qui s'opposent aux explications suivantes.

Personnes vivantes :

- Recherches du musée en tant que traitement de données : la recherche de provenance par le musée lui-même sera justifiée par un intérêt public ou privé prépondérant (cf. art. 31 al. 1 LPD). En d'autres termes, il existe un intérêt à connaître les propriétaires légitimes, ce qui pèsera plus lourd dans la balance que le droit des personnes concernées à ne pas subir de traitement de données dans la grande majorité des cas. La recherche de provenance est donc en principe autorisée.
- Communication d'informations à des tiers : Si des tiers demandent l'origine d'œuvres ou d'objets, le traitement juridique exact de la question devra être examiné au cas par cas, en fonction de la constellation et de la loi. Mais en règle générale, il s'agit à nouveau de mettre en balance les intérêts du tiers demandeur (son intérêt à connaître les données personnelles paraît-il légitime et compréhensible ?) et les intérêts de la personne qui veut empêcher que ses données personnelles soient communiquées (ici aussi : son intérêt paraît-il digne de protection ?)
    - Un musée privé sans mandat public devra vérifier s'il existe un intérêt prépondérant à la communication des données demandées dans un cas particulier (par exemple l'intérêt du public à connaître l'identité d'une personne). Si ce n'est pas le cas, les données ne devraient être communiquées qu'avec le consentement de la personne concernée, par mesure de précaution.
    - Un musée public sera déjà tenu de procéder à la mise en balance dans le cadre des lois sur la transparence en vigueur (voir, pour les organes fédéraux, l'article 36, paragraphe 3, de la LPD). S'il existe un intérêt public prépondérant à ce que les données personnelles puissent être communiquées (p. ex. parce que le public doit savoir qu'une personne est ou a été propriétaire d'une œuvre), il est alors permis de communiquer également les données personnelles correspondantes.

Personnes décédées:

- Comme mentionné ci-dessus, les données de personnes décédées ne sont pas protégées par la législation sur la protection des données. Le traitement des données par le musée dans le cadre de ses recherches ne pose donc pas de problème.
- S'il s'agit de la communication à des tiers, les proches encore en vie peuvent, dans certains cas, faire valoir un droit à la protection de la réputation de la personne décédée ; ce droit diminuera toutefois avec le temps. Dans ce cas, on procède à nouveau à une pesée des intérêts.
- En règle générale, plus la période concernée (ou le décès de la personne concernée) est éloignée dans le temps, plus les données personnelles peuvent être communiquées.

B – Exigences générales en matière de protection des données

1) Quand le droit de la protection des données doit-il être respecté ?

Le droit de la protection des données s'applique à chaque fois que des données personnelles sont traitées.

Les données personnelles sont des informations qui se rapportent à une personne physique identifiée ou identifiable. Une personne est déterminée lorsque les données l'identifient directement (par ex.

nom et prénom). Une personne est identifiable lorsque les données permettent, du point de vue de la personne qui traite les données ou en combinaison avec d'autres informations disponibles, d'identifier cette personne (p. ex. numéros de clients en relation avec une liste de clients ou numéros de téléphone avec accès à tel.search.ch).

Le traitement comprend toutes les actions en rapport avec les données personnelles, par exemple la collecte, l'enregistrement, la modification, l'envoi, la suppression ou l'anonymisation. Donc : même les données qui « dorment » sur un serveur sans être utilisées sont traitées !

De manière générale, les notions de données personnelles et de traitement sont très larges. Cela signifie que le droit de la protection des données s'appliquera dans la plupart des cas.

2) Quel est le sens et le but de la protection des données ?

Toute personne a le droit de voir ses données personnelles protégées. La protection des données garantit la protection de la vie privée lors de l'utilisation de données personnelles en tant que droit fondamental de tous les êtres humains.

A cet effet, le droit de la protection des données prévoit diverses règles pour les personnes traitant des données (entreprises, organes publics ou personnes privées) en ce qui concerne le traitement des données personnelles. En outre, il offre aux personnes concernées par le traitement des données une série d'instruments leur permettant de conserver la maîtrise de leurs données.

3) Qui doit respecter la législation sur la protection des données au sein d'un musée ?

Tout le monde ! L'action de tous les collaborateurs et toutes les collaboratrices, des organes et de leurs membres au quotidien est essentielle pour la protection des données. Chaque loi, chaque directive, chaque instruction est inutile si elle n'est pas appliquée dans le travail quotidien.

C'est pourquoi toutes les personnes mentionnées doivent veiller à ce que les principes de la protection des données et de la sécurité de l'information soient appliqués dans leur domaine d'activité et dans leur travail quotidien.

Les obligations à respecter découlent du droit applicable en matière de protection des données ainsi que des instructions et directives en vigueur au sein d'une organisation.

Il est toutefois important de noter que la responsabilité suprême de la mise en œuvre de la protection des données incombe à la direction : C'est à elle de prendre les mesures nécessaires et d'équiper les collaborateurs/trices afin qu'ils puissent mettre en œuvre la protection des données au quotidien.

4) Quelle loi sur la protection des données s'applique à un musée ?

Cette question doit être clarifiée séparément pour chaque musée et il convient de distinguer les constellations suivantes :

- Musées organisés selon le droit privé sans mandat de prestations public ;
- Musées organisés selon le droit privé avec un mandat de prestations public de la Confédération ou d'un canton ;
- Musées organisés selon le droit public (organes publics de la Confédération ou d'un canton). Pour les organes publics de droit cantonal, c'est le droit (de l'information et de la protection des données) du canton concerné qui s'applique (par exemple la loi sur l'information et la protection des données (IDG) du canton de Zurich, LS 170.4).

La loi fédérale sur la protection des données (LPD) s'applique aux particuliers et aux organes fédéraux. Les particuliers sont des personnes physiques ou morales. La notion d'organe fédéral englobe les autorités fédérales ainsi que les particuliers chargés de tâches publiques de la Confédération.

5) Le droit européen de la protection des données est-il également applicable ?

Pour certains traitements de données, le règlement général sur la protection des données de l'UE (RGPD ou GDPR [en anglais]) peut également jouer un rôle.

Le RGPD de l'UE peut également s'appliquer aux entreprises ou organisations en Suisse si a) ces personnes physiques proposent des biens ou des services dans l'UE ou b) si elles suivent le comportement de personnes physiques dans l'UE, par exemple en suivant dans une large mesure le parcours de navigation de ces personnes sur Internet.

Pour les musées suisses, cela peut être le cas si, par exemple, un suivi web élaboré est utilisé sur le site web (par exemple Google Analytics et mise en relation avec d'autres bases de données) ou si des offres sont explicitement adressées à des personnes dans l'espace de l'UE (par exemple, une formation continue promue en Allemagne ou en France dont le prix est fixé en euros).

6) Que sont les données personnelles sensibles et à quoi faut-il faire attention lors de leur traitement?

Les données personnelles sensibles nécessitent une protection accrue en raison de leur caractère sensible pour la personne concernée. C'est le cas lorsque les données permettent de se faire une idée particulièrement précise de la personnalité et de la vie d'une personne (sphère intime, santé), lorsqu'elles sont traitées de manière risquée ou lorsque de nombreuses données sont combinées entre elles.

La loi sur la protection des données contient des exigences plus strictes pour le traitement de données personnelles sensibles et cite les exemples suivants (ici à l'exemple de la LPD suisse) :

- Données relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales,
- données relatives à la santé, à la sphère intime ou à l'appartenance à une race ou à une ethnie,
- données génétiques,
- données biométriques permettant d'identifier une personne physique de manière unique,
- données relatives aux poursuites ou sanctions administratives et pénales,
- données relatives aux mesures d'aide sociale.

Un exemple de données personnelles sensibles dans le contexte des musées suisses peut être les données relatives à la santé des collaborateurs/trices - par exemple des informations concernant une opération ou une gestion d’un cas de l'AI.

S'il s'agit de données personnelles sensibles, il faut notamment respecter les exigences supplémentaires suivantes :

- Pour les musées publics, les exigences relatives au principe de légalité sont plus élevées et une base légale formelle est normalement nécessaire pour le traitement et la communication des données.
- Pour les musées privés, il convient de noter que la communication de données personnelles sensibles requiert un motif justificatif et - dans la mesure où un consentement est nécessaire

- que celui-ci doit être explicite (p. ex. cocher activement une case au lieu de cocher des cases déjà cochées).
- Les données sensibles exigent, en raison de leur sensibilité accrue, des mesures techniques et organisationnelles supplémentaires afin de garantir leur sécurité.

Si les lois cantonales sur la protection des données sont applicables, il faut en outre vérifier au cas par cas quelles exigences supplémentaires elles prévoient pour les données sensibles (ou souvent appelées « données personnelles spéciales »).

7) Quels principes doivent toujours être respectés lors du traitement des données ?

Le droit de la protection des données prévoit une série de principes de base qui doivent être respectés lors de tout traitement de données. On peut se les représenter comme une sorte de « toit » au-dessus de tous les traitements de données. Ces principes sont encore concrétisés dans diverses dispositions d'exécution de la loi sur la protection des données.

Les 7 principes de base sont les suivants :

- Légalité : les traitements de données doivent être effectués de manière légale et ne doivent pas enfreindre le droit en vigueur. Pour les organes publics, cela signifie en outre que le traitement de données personnelles ordinaires n'est autorisé que dans le cadre d'une base légale (ou dans certains cantons : le traitement des données doit être nécessaire à l'accomplissement d'une tâche légale). Des données personnelles spéciales ne peuvent être traitées par des organes publics qu'en présence d'une base légale formelle.
- Économie de données : seulement autant de données personnelles que nécessaire ! Lorsque les données ne sont plus nécessaires, elles doivent être anonymisées ou effacées.
- Affectation à un but précis : Les données personnelles ne peuvent être traitées qu'à des fins indiquées à la personne concernée ou reconnaissables pour elle, ou qui sont compatibles avec la finalité initiale (interdiction de modifier la finalité). Par exemple, les données personnelles collectées auprès des candidat-e-s (p. ex. coordonnées, références, CV) ne peuvent être utilisées que dans le but du recrutement et non pour l'envoi d'une newsletter, etc.
- Transparence : les personnes concernées sont informées des traitements de données.
- Exactitude des données : les données inexactes doivent être corrigées ou supprimées.
- Sécurité : les données personnelles doivent être protégées contre la perte, la falsification ou l'accès non autorisé.
- Responsabilité : les processus et procédures nécessaires pour garantir et prouver la conformité avec la protection des données doivent être mis en œuvre au sein de l'organisation.

8) Qu'entend-on par sécurité des données ?

La sécurité des données est un domaine partiel de la protection des données. Elle régit la disponibilité, la confidentialité, l'intégrité des données personnelles traitées ainsi que la traçabilité des processus de traitement des données. Pour ce faire, les organisations doivent prendre des mesures techniques et organisationnelles appropriées. Des exemples de telles mesures sont les concepts d'accès, l'anonymisation, la protection par mot de passe, l'authentification à deux facteurs, les formations, etc.

Plus les données personnelles sont sensibles, plus les exigences en matière de mesures de sécurité sont élevées (« adéquation »).

Outre l'exigence de sécurité des données dans la protection des données, il existe également un champ d'action plus large de la « sécurité de l'information ». Ici aussi, l'objectif est de garantir la disponibilité, la confidentialité et l'intégrité ; mais contrairement à la protection des données, le champ d'application est plus large. Il ne s'agit pas seulement de données personnelles, mais de toutes les informations pertinentes pour les opérations.

Conseil pratique : il est recommandé de relier la sécurité de l'information et la protection des données de manière à exploiter les synergies et à éviter les doublons.

9) A quoi faut-il faire attention lorsque des traitements de données sont confiés à des tiers ?

Lorsqu'un musée fait appel à des tiers (entreprises ou personnes physiques) dans le cadre de ses activités et que ceux-ci traitent des données personnelles dans le cadre du mandat, il s'agit d'un traitement de données sur mandat (par ex. logiciel de newsletter ou outil de collaboration d'entreprises tierces).

Le musée reste toujours responsable du respect de la protection des données. Le musée doit s'assurer que les tiers (appelés sous-traitants) traitent les données uniquement selon ses instructions et aux fins qu'il a définies.

Pour ce faire, le musée doit conclure un contrat écrit avec les sous-traitants, dans lequel il règle et impose les obligations nécessaires en matière de protection des données.

10) A quoi faut-il faire attention lorsque des données personnelles sont transmises à l'étranger ?

Il y a transmission de données personnelles lorsque celles-ci sont stockées physiquement à l'étranger (p. ex. fournisseur d'hébergement étranger) ou que des personnes de l'étranger ont accès (remote access) à des données stockées localement (p. ex. fournisseur de logiciels étranger dans des cas de support).

Si des données personnelles sont transmises à l'étranger, la législation étrangère s'applique au traitement des données. Si cette législation n'est pas équivalente à la législation locale en matière de protection des données, des mesures de protection doivent être prises. Pour ce faire, on procède selon la cascade suivante :

1. État tiers sûr : sont considérés comme des pays offrant un niveau de protection des données suffisant, par exemple, tous les États de l'espace EEE (États tiers sûrs), mais pas les États-Unis, la Chine ou la Russie (États tiers non sûrs). En cas de transfert vers des pays tiers sûrs, aucune mesure supplémentaire n'est nécessaire.

2. Mesures de protection appropriées : En cas de transfert vers des pays tiers non sûrs, des mesures supplémentaires doivent être prises, par exemple des clauses de protection des données approuvées par l'autorité de surveillance de la protection des données ou les clauses standard de données de la Commission européenne doivent être conclues.

3. Motif d'exception : sans mesures de protection appropriées, les données ne peuvent être transmises à l'étranger que dans des cas exceptionnels. Ceci, par exemple, lorsqu'il existe un consentement explicite ou que la communication est nécessaire à la sauvegarde d'intérêts prépondérants.

11) Qu'est-ce qu'une analyse d'impact relative à la protection des données et comment la réaliser ?

Comme son nom l'indique, l'analyse d'impact sur la protection des données est une réflexion sur les risques d'un traitement de données que l'on documente. La loi sur la protection des données prévoit que les conséquences d'un traitement de données sur les personnes concernées doivent toujours

être examinées au préalable, et ce pour tout nouveau projet impliquant le traitement de données personnelles ainsi que lorsqu'un traitement de données existant est adapté.

Le traitement de données envisagé, les finalités du traitement, les catégories de données et de personnes concernées, les risques éventuels et les mesures d'atténuation des risques ainsi qu'une série d'autres informations sont documentés.

Si, malgré la mise en œuvre de mesures de protection, des risques élevés subsistent pour les droits fondamentaux des personnes concernées (par exemple en cas de traitement de données à grande échelle ou d'utilisation de logiciels de vidéosurveillance avec des fonctions d'analyse), l'analyse d'impact sur la protection des données doit être soumise à l'appréciation de l'autorité fédérale ou cantonale de surveillance de la protection des données concernée.

12) Que faire en cas de violation de la sécurité des données ?

Les musées doivent analyser en interne les violations de la sécurité des données et les signaler à l'autorité fédérale ou cantonale de surveillance de la protection des données lorsqu'il en résulte un risque élevé pour les droits fondamentaux des personnes concernées (data breach notification). Nota bene : dans certaines lois cantonales, le seuil est fixé un peu plus bas et les incidents de protection des données doivent toujours être déclarés.

Il y a violation de la sécurité lorsque l'intégrité, la confidentialité, la disponibilité ou la traçabilité des données ne sont plus garanties et que des données personnelles sont perdues, effacées, détruites ou modifiées de manière involontaire ou illicite ou qu'elles sont divulguées ou rendues accessibles à des personnes non autorisées. C'est par exemple le cas lorsqu'une clé USB ou un ordinateur professionnel est perdu ou abandonné, en cas de cyberattaque (attaque DDoS, phishing) ou d'accès aux données par des personnes non autorisées.

- Tous les collaborateurs/trices des musées doivent signaler immédiatement (!) en interne tout soupçon d'incident de protection des données auprès d'un service désigné à cet effet - idéalement le/la responsable de la sécurité ou le/la conseiller/ère à la protection des données. En interne, il convient alors d'analyser et de documenter s'il y a eu un incident de protection des données au sens de la loi. Si c'est le cas, les étapes suivantes sont nécessaires : Prendre des mesures pour limiter les risques
- Annonce immédiate à l'autorité de surveillance de la protection des données (dans les 72 heures selon la pratique ou selon les dispositions cantonales en matière de protection des données).
- Information à la personne concernée si l'incident de protection des données représente un risque important pour elle ou si elle doit prendre elle-même des mesures de protection (p. ex. changement de mot de passe).

13) Que se passe-t-il si les dispositions relatives à la protection des données ne sont pas respectées ?

La protection des données personnelles n'est pas facultative, mais prescrite par la loi.

Les autorités de surveillance compétentes en matière de protection des données pour les musées suisses sont soit le Préposé fédéral à la protection des données et à la transparence (PFPDT), soit les autorités cantonales de protection des données (voir un aperçu sur https://www.privatim.ch/de/privatim/). Elles surveillent l'application des dispositions relatives à la protection des données et sont dotées de pouvoirs de contrôle (p. ex. droit d'accès ou de consultation), peuvent émettre des recommandations ou ordonner l'adaptation ou la cessation de traitements de données.

Outre les mesures de surveillance, les personnes concernées peuvent faire valoir les violations de la protection des données par voie civile ou administrative directement auprès du musée et exiger par exemple la cessation ou la suppression des traitements de données illégaux. En cas de dommage financier ou d'atteinte grave à la personnalité, la personne concernée a droit à des dommages et intérêts ou à une réparation morale.

La loi suisse sur la protection des données prévoit des sanctions pénales pour les personnes privées (concrètement les collaborateurs/trices) et des amendes pouvant aller jusqu'à 250 000 CHF. La punissabilité n'est toutefois prévue que pour certaines obligations de protection des données et exige au moins un dol éventuel. Le dol éventuel signifie que la violation de la protection des données n'est certes pas recherchée consciemment, mais qu'elle est acceptée.

Outre ces sanctions juridiques, le non-respect du droit de la protection des données peut entraîner de graves risques de réputation.