

FAQ PROTECTION DES DONNÉES

Remarques préliminaires à l'utilisation de ce document

La présente FAQ (Foire Aux Questions) est à disposition des paroisses du diocèse de Bâle dans le but de les aider dans leur travail au quotidien. Celui-ci doit toujours appliquer les sept principes du droit relatif à la protection des données. Ce document tente cependant d'appliquer au cas concret les principes les plus importants sur le sujet. Il peut cependant, selon le contexte, s'avérer nécessaire de respecter également d'autres obligations. La présente FAQ doit donc être lue en relation avec les autres documents mis à disposition – notamment les documents « Protection des données : les bases pour le travail dans les paroisses du diocèse de Bâle », « Tenue des registres paroissiaux – respecter la protection des données » ou les modèles préparés (Contrat de sous-traitance du traitement des données, déclarations de protection des données, registre de traitement des données).

N°	FAQ	Réponse
1	Programmes informatiques alternatifs : Existe-t-il des alternatives aux programmes les plus répandus ?	Une liste d'exemples de programmes alternatifs se trouve en annexe. Il faut vérifier la conformité de tous les programmes utilisés en matière de protection des données. Les fournisseurs mettent aujourd'hui à disposition des déclarations de protection des données ainsi que des documents contractuels.
2	Applis pour le travail sur le téléphone privé : Dans quelle mesure est-il opportun que les collaborateurs et collaboratrices installent et utilisent sur leurs portables privés des applis qu'ils/elles utilisent pour travailler ? Dans quels cas est-ce à déconseiller expressément ?	Du point de vue de la paroisse, il faut déconseiller expressément de traiter dans des applis des données (d'affaires ou personnelles) qui doivent rester sous le contrôle de la paroisse. Il faut déconseiller leur installation tant qu'aucune solution technique n'est implémentée pour gérer de tels appareils et effacer à distance les données de la paroisse, si nécessaire aussi sur des appareils privés, quand l'appareil est perdu ou que la personne concernée part (ce qu'on appelle Mobile Device Management MDM avec Remote-Wipe). S'il ne s'agit pas de traiter des données de contenu mais de clarifier des questions organisationnelles (calendrier, etc...), la paroisse peut recommander une solution sûre de messagerie et communiquer aux collaboratrices et collaborateurs par directive la manière de l'utiliser (limitation à l'organisation, pas de données de contenu, etc...).
3	Contrat de sous-traitance des données : À quoi dois-je faire attention si je mandate des tiers pour traiter des données ?	Le modèle « Protection des données : Modèle de contrat de sous-traitance du traitement des données, y.c. TOM » contient les points essentiels d'un tel contrat.
4	Droits des personnes concernées : (cf. Droits)	Le droit relatif à la protection des données prévoit différents droits qu'une personne concernée par un traitement des données peut faire valoir auprès des paroisses ou des communes ecclésiastiques en relation avec ses propres

N°	FAQ	Réponse
	Sur quoi portent les droits des personnes concernées ?	données. Elle a notamment le droit d'accéder à ses données et de les consulter, de corriger ou faire détruire des données inexactes, d'interdire ou de constater un traitement de données illégitime, de limiter ou de bloquer ses propres données.
5	Droits à l'image : À quoi dois-je faire attention pour des images ?	Le centre médiatique kath.ch a introduit une information sur les droits à l'image dans le blog suivant (dernier appel 15.02.2024) : https://www.blogs-kath.ch/bilder-rechtskonform-nutzen/
6	Cloud/Nuage : À quoi faut-il faire attention lorsque des fichiers/données sont stockés dans un nuage ?	Le stockage correct de données dans un nuage n'est pas toujours simple du point de vue de la protection des données. Si les données sont traitées en Suisse par un fournisseur du pays, il faut un document contractuel complet, comprenant, entre autres, un contrat de sous-traitance (cf. le modèle) et des mesures techniques et organisationnelles (TOM) appropriées. La solution en nuage souhaitée doit être analysée précisément sur ses aspects techniques et contractuels avant la conclusion du contrat. Si les données sont traitées à l'étranger par le fournisseur de services ou si celui-ci peut (p.ex., pour des raisons de support ou de service) y avoir accès depuis l'étranger, la situation est un peu plus complexe : en plus du contrat, il faut une analyse pour savoir si l'ordre juridique étranger garantit un niveau adéquat de protection des données. C'est le cas pour les pays-membres de l'UE ainsi que différents autres pays. Les USA ne sont pas considérés, au moment de l'établissement de cette FAQ (décembre 2023) comme un pays tiers sûr, le Conseil fédéral est cependant en train de conclure avec eux un cadre de protection appelé « Data Privaca Framework » qui devra garantir un niveau adéquat de protection pour le traitement des données dans/depuis les USA. Si le pays tiers n'est pas jugé adéquat, il faut prendre des mesures supplémentaires de sécurité afin que la transmission des données soit conforme à la législation. Cela passe notamment par certaines dispositions contractuelles supplémentaires ainsi que des mesures techniques comme, par exemple, la pseudonymisation des données stockées afin que ne puisse être établi aucun lien avec des personnes en dehors de l'organisation. C'est une mesure souvent techniquement très exigeante. Si les données relèvent du secret de fonction ou professionnel, il est recommandé de les garder en Suisse.
7	Traitement des données : À quoi faire attention si le traitement des données est confié à des tiers ?	Lorsque la paroisse fait appel à des tiers pour son activité (entreprises ou personnes individuelles) et que ceux-ci traitent des données personnelles dans le cadre de leur mandat, on parle alors de sous-traitance (p.ex., logiciel pour infolettre ou outil collaboratif d'entreprises tierces). Dans ce cas, la paroisse (appelée responsable) reste responsable du respect de la protection des données. Elle doit garantir que les tiers (appelés sous-traitants) ne traitent les données que selon ses instructions et selon les finalités indiquées. La paroisse doit, à cet effet, conclure un contrat écrit avec les sous-traitants (appelé contrat de sous-traitance du traitement des données), qui règle et transfère les obligations nécessaires en matière de protection des données. Le diocèse de Bâle met à disposition un modèle de contrat de sous-traitance que les paroisses peuvent utiliser.

N°	FAQ	Réponse
8	Registre de traitement des données : Que faut-il indiquer dans un registre de traitement des données ?	Un registre de traitement des données contient une brève description de tous les processus de traitement des données (soit de tous les processus durant lesquels des données personnelles sont traitées), qui sont entrepris au sein d'une organisation. Le site internet du diocèse de Bâle contient un modèle de registre (remarques préliminaires comprises).
9	Communication de données : Que faire lorsque quelqu'un veut obtenir ses données ?	En premier lieu, il faut informer la personne responsable des questions de protection des données dans la paroisse ou la commune ecclésiastique (pour autant qu'elle existe). Il faut identifier correctement la personne requérante afin que les données ne soient pas transmises à la fausse personne. Cela peut se faire par contact personnel (en cas de demandes orales), par la demande d'informations complémentaires (en cas de demandes par téléphone) ou par l'obtention d'une copie (éventuellement partiellement caviardée) de la carte d'identité. Il faut chercher les données de la personne sur tous les supports de données internes. Suivant l'étendue de la demande, cela peut concerner aussi des données de login. Cela permet d'établir ensuite la liste des données et de la mettre (évt. d'entente avec la personne responsable à l'interne) à disposition de la personne requérante (droit d'accès, droit de la personne concernée). Attention : il n'est pas nécessaire de fournir des documents entiers mais seulement la liste des données personnelles dont dispose la paroisse. Les renseignements doivent être fournis dans les 30 jours. S'il existe des intérêts prépondérants de la paroisse ou de tiers ou si la demande de renseignement est posée pour des motifs clairement abusifs (c-à-d. non pas pour obtenir des renseignements effectifs sur ses propres données mais, p.ex., pour clarifier ses chances de procès en cas de plainte contre la paroisse), il est possible de limiter ou de refuser le droit d'accès. En vertu de la loi, la personne concernée peut exiger des renseignements sur les données suivantes : - L'identité et les coordonnées du responsable (c-à-d. de l'organisation qui traite les données ainsi que, le cas échéant, d'une personne de contact pour la protection des données) ; - Les données personnelles traitées en tant que telles ; - La finalité du traitement ; - La durée de conservation des données personnelles ou, si cela n'est pas possible, les critères de fixation de cette durée ; - Les indications disponibles sur l'origine des données si celles-ci n'ont pas été fournies par la personne elle-même ; - Le cas échéant, l'existence d'une décision individuelle automatisée ainsi que la logique sur laquelle repose cette décision ; - Le cas échéant, les destinataires ou catégories de destinataires à qui sont communiquées les données personnelles ainsi que d'autres informations (État et mesures de protection) si les données personnelles sont communiquées à l'étranger.

N°	FAQ	Réponse
10	Droit de la protection des données : obligation de l'appliquer Quand faut-il respecter le droit relatif à la protection des données ?	Le droit relatif à la protection des données s'applique chaque fois que des <i>données à caractère personnel sont traitées</i>. Les données à caractère personnel sont les informations qui se rapportent à une personne physique identifiée ou identifiable. Une personne est identifiée lorsque les données l'identifient directement (p.ex., nom et prénom). Une personne est identifiable lorsque les données peuvent permettre son identification par les personnes qui les traitent ou en combinaison avec d'autres informations disponibles (p.ex., numéro d'identification dans la banque de données en relation avec une banque de données ou numéros de téléphone avec accès direct à tel.search.ch). Le traitement des données concerne toutes les actions en relation avec les données personnelles, p.ex. leur collecte, leur enregistrement, leur modification, leur envoi, leur suppression ou leur anonymisation. Donc : même des données qui « dorment » inutilisées sur un serveur sont traitées ! De manière générale, les notions de « données à caractère personnel » et de « traitement » ont une acception très large. <i>Cela signifie que le droit relatif à la protection des données s'appliquera dans la plupart des cas dans le travail quotidien de la paroisse.</i>
11	Droit relatif à la protection des données : finalité Quelle est la finalité du droit relatif à la protection des données ?	Toute personne a droit à ce que les données relatives à sa personne soient protégées. La protection des données garantit la protection de la sphère privée dans la gestion des données à caractère personnel comme un droit fondamental de chacun. Le droit relatif à la protection des données prévoit à cet effet diverses règles dans le traitement des données personnelles (par des entreprises, des organes publics ou des personnes privées). Il donne aussi aux personnes concernées par des traitements de données une série d'outils pour garder la haute main sur leurs données.
12	Protection des données : principes de base Quels principes faut-il toujours respecter ?	Le droit relatif à la protection des données énonce une série de principes de base qui doivent être respectés lors de chaque traitement de données. On peut se les représenter comme une sorte de « chapeau » pour tous les traitements de données. Ces principes sont concrétisés plus en détail dans diverses dispositions d'exécution dans la loi sur la protection des données. Les sept principes de base sont les suivants : - Licéité : les traitements des données doivent être licites et ne doivent pas enfreindre le droit en vigueur. Cela implique aussi pour les organes publics que le traitement de données personnelles usuelles n'est autorisé que sur une base légale (ou dans certains cantons : le traitement des données doit être nécessaire à l'exécution d'une tâche légale). - Minimisation : il est possible de collecter et d'enregistrer seulement autant de données à caractère personnel que nécessaires ! Lorsque des données ne sont plus utilisées, elles doivent être anonymisées ou effacées. - Finalité : les données à caractère personnel ne peuvent être traitées que pour des buts qui ont été communiqués à la personne concernée ou que celle-ci peut identifier ou qui sont compatibles avec le but initial (interdiction de changer la finalité). Par exemple, les données personnelles reçues lors de postulations (p.ex., coordonnées, références, CV) ne peuvent être utilisées qu'à des fins de recrutement et non, par exemple, pour l'envoi d'une infolettre ou autre. - Transparence : les personnes concernées sont informées du traitement de leurs données.

N°	FAQ	Réponse
		- Exactitude des données : des données incorrectes doivent être corrigées et supprimées. - Sécurité : les données personnelles doivent être protégées de la perte, de la falsification ou de l'accès indu. Il est possible d'y parvenir en général par des mesures de protection techniques et organisationnelles (lesdites TOM). - Responsabilité : les organisations sont tenues d'appliquer en interne les processus nécessaires pour garantir la sécurité des données et pour prouver la conformité à la protection des données.
13	Protection des données : analyse d'impact Qu'est-ce qu'une analyse d'impact de la protection des données et comment la faire ?	Comme son nom l'indique, l'analyse d'impact de la protection des données (AIPD) est une réflexion sur les risques d'un traitement de données que l'on documente et essaye de réduire. La loi relative à la protection des données prévoit que les conséquences d'un traitement de données pour les personnes concernées soient toujours mesurées en amont, et ceci pour tout nouveau projet impliquant un traitement de données à caractère personnel ainsi que pour toute modification d'un traitement existant de données. L'introduction d'un nouveau logiciel pour gérer d'importants volumes de données (CRM, registre de membres) ou l'installation d'une caméra de surveillance sur le territoire de la paroisse sont des exemples de faits qui exigent de procéder à une AIPD. Le préposé fédéral à la protection des données et à la transparence (PFPDT) met à disposition une notice d'aide : Analyse d'impact relative à la protection des données personnelles (admin.ch) .
14	Dispositions de protection des données : Que se passe-t-il si des dispositions de protection des données ne sont pas respectées ?	La protection des données à caractère personnel n'est pas facultative, elle est prescrite par la loi. L'autorité compétente en matière de protection des données pour les paroisses est le Préposé fédéral à la protection des données et à la transparence (PFPDT) et celle pour les communes ecclésiastiques sont les autorités cantonales de protection des données. Ces autorités surveillent la mise en œuvre des prescriptions en matière de protection des données et ont un droit de contrôle (droit d'accès ou de consultation), elles peuvent faire des recommandations ou statuer sur l'adaptation ou l'arrêt du traitement de données. À côté des mesures de surveillance, les personnes concernées peuvent faire valoir des violations de la protection des données par voie de droit civil ou administratif directement auprès de la paroisse et exiger, par exemple, la cessation ou la suppression de traitements illicites de données. En cas de dommages financiers ou de violation grave de la personnalité, la personne concernée a le droit de réclamer des dommages et intérêts ou réparation. La LPD prévoit des sanctions pénales pour les personnes privées et des amendes pouvant se monter jusqu'à 250'000.-. Celles-ci pourraient concerner au premier chef la direction des paroisses qui est, en tant qu'organe exécutif de la paroisse, responsable de l'introduction et de l'application des procédures et obligations nécessaires. La punissabilité n'est cependant 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'a pas été voulue mais que son risque était accepté. À côté de ces sanctions juridiques, le non-respect du droit relatif à la protection des données peut causer un grave dégât d'image.
15	Sécurité des données : Qu'entend-on par sécurité des données. Que sont les TOM ?	La sécurité des données est un élément de la protection des données. Elle règle la disponibilité, la confidentialité, l'intégrité des données à caractère personnel traitées, ainsi que la traçabilité des processus de traitement des données.

N°	FAQ	Réponse
		nées. Les organisations doivent, pour cela, prendre des mesures techniques et organisationnelles adaptées (appelées TOM). Des exemples de telles mesures sont les concepts d'accès, l'anonymisation, la protection par mot de passe, l'authentification double, les formations, les directives, etc... Plus les données à caractère personnel sont sensibles, plus les exigences en matière de mesures de sécurité sont élevées (« adéquation »). Il existe cependant aussi un domaine de la « sécurité de l'information » dont le cadre dépasse celui de l'exigence de sécurité demandée par la protection des données. Le but de celle-ci est également de garantir disponibilité, confidentialité et intégrité ; mais, contrairement à la protection des données, son champ d'application est plus étendu. Il porte en effet sur toutes les informations importantes pour l'entreprise et pas seulement sur les données à caractère personnel. Conseil pratique : il est recommandé lier sécurité de l'information et protection des données, de manière à exploiter des synergies et à éviter des doublons.
16	Sécurité des données : Que faut-il faire en cas de violation de la sécurité des données ?	Il y a violation de la sécurité quand l'intégrité, la confidentialité, la disponibilité ou la traçabilité des données ne sont plus garanties et que des données à caractère personnel sont perdues, effacées, détruites ou modifiées de manière involontaire ou illicite ou qu'elles sont montrées ou rendues accessibles à des personnes non autorisées. C'est, par exemple, le cas lorsqu'une clef USB ou un ordinateur professionnel est perdu ou oublié, lors de cyberattaques (attaques par déni de service distribué DDoS ou phishing) ou lorsque des personnes non autorisées accèdent à des données. Les paroisses doivent analyser en interne les violations de la sécurité des données et elles doivent les signaler au Préposé fédéral à la protection des données (ou à l'autorité cantonale de surveillance en matière de protection des données pour les activités dont la responsabilité est partagée avec la commune ecclésiastique) lorsqu'il en résulte un risque élevé pour les droits fondamentaux des personnes concernées (notification de violation de la protection des données). Nota bene : certaines lois cantonales mettent la barre un peu plus bas et toute violation de la protection des données doit être signalée. Toute personne travaillant dans la paroisse doit annoncer immédiatement (!) tout soupçon de violation de la protection des données au service interne désigné pour cela – dans l'idéal, le délégué à la sécurité ou le conseiller à la protection des données – ainsi qu'à la direction de la paroisse et à la direction de la commune ecclésiastique. Le vicaire général du diocèse peut également être contacté pour un conseil. Il s'agit aussi d'analyser et de documenter en interne s'il y a une violation de la protection des données au sens de la loi. Si c'est le cas, les démarches suivantes s'imposent : • Prise de mesures pour réduire le risque • Annonce immédiate auprès de l'autorité de surveillance de la protection des données (dans le délai de 72 heures selon la pratique ou selon les dispositions cantonales en matière de protection des données), pour le PFPDT, le formulaire suivant peut être utilisé : https://databreach.edoeb.admin.ch/report • Information à la personne concernée si la violation comporte un grand risque pour elle et qu'elle doit prendre elle-même des mesures de protection (p.ex., changement du mot de passe).

N°	FAQ	Réponse
17	Groupelements : À quoi faut-il faire attention pour des listes de groupements ?	Les listes des membres de groupements doivent être protégées par des mesures adéquates contre la perte ou la consultation non autorisée. Par principe, elles ne peuvent être établies que pour permettre à la paroisse ou à la commune ecclésiastique de remplir sa mission légale (principe de licéité) et les principes de protection des données sont applicables (notamment la proportionnalité : droits d'accès restrictifs, saisie des seules données indispensables ; et la sécurité : archivage dans un environnement sûr, evt. mot de passe pour les envois, etc...). Les membres doivent être informés du traitement qui sera fait de leurs données lors de leur collecte (principe de transparence, accord des personnes concernées). Si elles sont transmises, les listes de membres doivent être sécurisées, par exemple par mot de passe, surtout lorsqu'elles contiennent de nombreuses données personnelles. Il faut vérifier, avant l'envoi, si le destinataire (personne ou organisation) est autorisé à recevoir les données. Si ce n'est pas le cas (p.ex., parce qu'aucune tâche ecclésiale n'a été confiée à cette personne/organisation), il faut demander l'accord des personnes concernées. Pour les envois internes à la paroisse, il faut utiliser un lien vers un dossier partagé et ne pas annexer les listes dans un courriel. La direction de la paroisse est la première responsable de la protection des données.
18	Site internet : Qu'est-ce qui doit absolument figurer dans les mentions légales d'un site internet de paroisse ?	Les mentions légales devraient indiquer les coordonnées de l'organisation responsable du site : nom complet de l'organisation avec, le cas échéant, une personne ou un service de contact dans la paroisse, adresse postale et courriel, dans l'idéal aussi un numéro de téléphone.
19	Catéchèse/Enseignement religieux : Est-il possible d'établir des listes d'élèves (avec indications telles que domicile, numéros de téléphone, courriel des parents, adresses d'envoi supplémentaire) ? Les parents doivent-ils donner leur accord pour le stockage de ces données ?	Il est permis d'établir des listes pour autant que celles-ci soient indispensables à l'enseignement religieux et à la catéchèse. Il faut veiller à ne collecter que des données uniquement nécessaires et à prendre des mesures pour garantir la sécurité (archivage dans un milieu sûr, pas de copies, sécurité par mot de passe en cas d'envoi, etc...) et la proportionnalité (droits d'accès limités au strict nécessaire à l'intérieur de la paroisse). Lorsque la collecte des données est autorisée pour l'enseignement religieux/la catéchèse (parce que les parents ont accepté de les donner à cette fin ou que le droit cantonal prévoit la transmission des données personnelles des fidèles de la confession dans ce but à la paroisse), la paroisse a le droit de les enregistrer pour la même finalité. Si la paroisse souhaite plus tard étendre cette finalité et exploiter les données pour inviter les élèves ou leurs parents à d'autres manifestations ou leur envoyer des infolettres, il est recommandé de demander leur autorisation.
20	Catéchèse/Enseignement religieux : Les listes des élèves peuvent-elles être remises aux parents d'une classe ?	C'est une zone grise dans laquelle donner des listes d'élèves peut s'avérer sensé (et souvent utile) (p.ex., pour que les parents puissent s'organiser), sans que ce soit forcément <i>indispensable</i> à l'enseignement religieux/la catéchèse au sens de la loi sur la protection des données. C'est pourquoi les personnes concernées font parfois preuve de peu de compréhension. En cas de doute, il est recommandé de signaler aux parents, lors de l'inscription (p.ex., à l'aide d'un formulaire), que des listes d'élèves seront remises et de leur donner la possibilité, soit de donner leur accord

N°	FAQ	Réponse
	Dans ce cas, quelles sont les informations qui peuvent y figurer et lesquelles sont interdites ?	(p.ex., par une coche sur le formulaire), soit de s'annoncer auprès de la paroisse s'ils ne veulent pas que leur enfant paraisse sur une telle liste. En cas de protestation, l'enfant en question - ou certaines de ses données comme le numéro de téléphone - peut être enlevé de la liste. Quoiqu'il en soit, les indications doivent se réduire au minimum permettant d'atteindre l'objectif souhaité (p.ex., numéro de téléphone des parents, pas de dates de naissances ou autres indications non indispensables).
21	Listes (cf. aussi Groupements, Associations) Comment faire avec des listes de clients au sens large du terme (p.ex., communion régulière aux malades, services sociaux) ?	Il faut respecter le principe de minimisation. Toutes les personnes ayant accès aux listes sont responsables qu'elles soient utilisées de manière conforme à la protection des données et qu'elles ne soient pas transmises à des tiers (principe de licéité).
22	Listes : A-t-on le droit de consigner qui est soutenu par le service social, quand et sous quelle forme ?	Il est en principe possible de consigner ceci pour des raisons de traçabilité. Les informations sur une personne à l'aide sociale font partie des données sensibles et doivent être protégées en conséquence.
23	Listes avec coordonnées : Comment régler l'accès à ces données ?	Les droits d'accès à ces listes doivent être limités au strict minimum. Elles doivent être enregistrées dans un environnement sûr (dans le dossier partage de la paroisse, pas sur dropbox ou un appareil privé, etc..) et détruites dès qu'elles ne sont plus utilisées. Si elles doivent être envoyées, le fichier correspondant devrait être sécurisé par mot de passe. Il faut définir qui doit avoir accès à ces informations dans la paroisse (ou la commune ecclésiastique) pour pouvoir remplir sa tâche (principe du besoin d'en connaître). Les principales lois sur la protection des données considèrent les données relatives à l'aide sociale comme des données sensibles qui méritent une protection particulière. Il est donc recommandé de les ranger dans un dossier accessible à peu de personnes avec, éventuellement, une protection par mot de passe.
24	Listes des manifestations périodiques : Ai-je le droit de tenir des listes sur des années (p.ex., liste d'un congrès annuel) ?	Il est permis de tenir de telles listes. Proposition pour la déclaration correspondante de protection des données : <i>Les données personnelles que vous nous communiquez par votre inscription à [manifestation] sont tenues dans une liste par [organisation] et actualisées en permanence, dans le but de pouvoir vous inviter à de futures manifestations du même type [et de pouvoir vous demander éventuellement votre aide]. Cette liste n'est accessible qu'aux [organismes] ainsi qu'aux tiers impliqués dans l'organisation], elle est protégée par des mesures adéquates et enregistrée par nos soins avec éventuellement l'aide de tiers dans un environnement sécurisé en Suisse ou dans l'UE. Vous pouvez faire effacer vos données en tout temps de cette liste. Pour toute question ou demande, vous pouvez vous adresser à XY@xyz.ch.</i> Ces données peuvent être utilisées pour établir une liste de participant·es à la manifestation avec nom, prénom et lieu.

N°	FAQ	Réponse
25	Trafic e-mail : Dans quels cas la protection des données interdit-elle un échange d'e-mails non crypté ?	Des échanges courriel non cryptés à des destinataires externes à son organisation sont inappropriés pour des données personnelles sensibles ou des données qui doivent être traitées confidentiellement pour d'autres raisons (p.ex., données relevant du secret professionnel ou de fonction).
26	Messageries : Quels services de messagerie est-il possible d'utiliser sans souci dans le contexte paroissial ? Lesquels devrait-on laisser de côté ?	En principe, du point de vue de la protection des données, il est préférable d'utiliser Threema ou Signal plutôt que d'autres services de messagerie comme WhatsApp ou Telegram. La paroisse peut édicter une directive pour que l'utilisation de, par exemple, WhatsApp par les collaboratrices et collaborateurs se limite à des questions organisationnelles (p.ex., pour trouver une date, etc.) sans livrer aucune donnée sur la teneur des activités de la paroisse.
27	Programmes Office : La loi fédérale sur la protection des données permet-elle de continuer aujourd'hui à utiliser les produits Microsoft sans problème dans le cadre de la paroisse ? Où y-a-t-il des réserves ? Quelles seraient les alternatives ?	Au moment de la rédaction de cette FAQ (décembre 2023), une utilisation conforme au droit des services en nuage de Microsoft requiert a) des garanties contractuelles dont certaines doivent être conclues en plus avec Microsoft, b) des mesures de sécurité contractuelles et techniques supplémentaires pour limiter le risque inhérent aux traitements de données par Microsoft aux USA et c) une classification interne des données qui les répartit dans différents niveaux de sécurité et qui fait des prescriptions différentes pour leur traitement (p.ex., aucune donnée relevant du secret professionnel n'est enregistrée dans le nuage de Microsoft). Le prochain accord sur le cadre de protection des données « Data Privacy Framework » entre le Conseil fédéral et le gouvernement américain devrait résoudre certains de ces problèmes, mais les données relevant du secret professionnel ou de fonction nécessiteront toujours un soin particulier. En cas d'utilisation des services en nuage de Microsoft, il est recommandé de s'adjoindre une aide spécialisée pour procéder aux démarches ci-dessus et de garantir par des directives internes que les données relevant du secret professionnel ou de fonction sont stockées séparément (p.ex., avec CMI Axioma pour documents officiels).
28	Données du personnel (employés) : Quelles sont les prescriptions ?	Il s'agit ici de : certificats de travail, certificats intermédiaires, contrat de travail, description de poste, entretien avec les collaborateurs. Ces documents sont déposés, conservés auprès de l'autorité d'engagement, (partiellement aussi) auprès du supérieur ecclésial (paroisse). Il faut définir qui a le droit d'avoir ces documents et qui a le droit de les consulter, en appliquant pour cela le principe du besoin d'en connaître. Il faut éviter de les stocker inutilement à double. Les dispositions générales s'appliquent avec une attention particulière sur la proportionnalité (droits d'accès restrictifs) et la sécurité (stockage dans un environnement adapté, droits d'accès restrictifs). La paroisse a l'obligation de respecter, elle aussi, le droit étatique qui s'applique à la commune ecclésiastique (droit du personnel de l'Eglise cantonale ou du canton ainsi que droit des obligations).
29	Données du personnel (employés) : Combien de temps peut-on les garder ?	L'ordre juridique prévoit des délais de conservation et de péremption très variés qui peuvent entrer en ligne de compte pour la conservation de documents relatifs au personnel. Pour les rapports de travail, il y a prioritairement deux sortes de délais légaux de conservation :

N°	FAQ	Réponse
		a. Les délais de conservation pour des livres de comptabilité qui doivent garantir la traçabilité de versements de salaires pendant 10 ans (raison pour laquelle certaines données des rapports de travail, p.ex. le contrat, devraient être conservées durant cette même durée) ; b. Les délais de prescription pour les revendications de salaire (p.ex., cinq ans pour des revendications issues des rapports de travail, lorsque le droit des obligations s'applique directement ou comme droit cantonal subsidiaire). Il est recommandé de procéder par étapes et de détruire, 5-6 ans après le départ ce qui n'est pas nécessaire à la traçabilité des livres comptables (les évaluations suite aux entretiens de collaborateurs, les quittances de salaire pour autant qu'elles ne soient pas importantes pour les livres comptables, les documents relatifs à des prestations et des contributions des assurances sociales ainsi que de la prévoyance professionnelle). Les données restantes sont effacées après 10-11 ans.
30	Données du personnel (employés) : Procédure en cas de changement de poste	Si le changement de poste se fait au sein de l'organisation, les documents relatifs au poste précédent peuvent être conservés si c'est nécessaire. Si la personne quitte l'organisation, les indications au point précédent s'appliquent.
31	Données personnelles : Que sont des données sensibles ?	Les données à caractère personnel sensibles doivent être mieux protégées à cause de leur sensibilité pour la personne concernée. C'est le cas lorsque des données permettent de percer particulièrement bien la personnalité et la vie d'une personne (p.ex., des informations personnelles tirées d'entretiens pastoraux ou avec des travailleurs sociaux ainsi que des informations sur des employés), lorsqu'elles sont traitées d'une manière risquée ou lorsque de nombreuses données sont combinées ensemble. La LPD cite les exemples suivants : • les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, • les données sur la santé, la sphère intime ou l'origine raciale ou ethnique, • les données génétiques, • les données biométriques identifiant une personne physique de manière univoque, • les données sur des poursuites ou sanctions pénales et administratives, • les données sur des mesures d'aide sociale.
32	Données personnelles : À quoi faut-il veiller tout spécialement dans le traitement des données personnelles sensibles ?	Ces données, de par leur nature sensible, doivent être <i>particulièrement bien protégées</i> – en d'autres termes, il faut porter une attention toute particulière aux mesures techniques et organisationnelles de protection (TOM) de la <i>sécurité des données</i> . De plus, il n'est autorisé de communiquer des données personnelles sensibles à des tiers (c-à-d. de les transmettre ou de les rendre accessibles à une autre organisation ou personne qui les utilisera pour ses propres buts) que pour un motif justifié ; cela signifie qu'il faut pour cela une <i>base légale</i> , un <i>intérêt prépondérant</i> de la paroisse ou d'un tiers ou <i>l'accord exprès</i> des personnes concernées. L'accord exprès est un accord pour lequel la personne concernée est active, par exemple en cochant une case ou en signant. Important : les communes ecclésiastiques, en tant que corporations de droit cantonal, ont généralement besoin d'une base légale explicite pour traiter des données sensibles.

N°	FAQ	Réponse
33	Données personnelles : Comment faut-il envoyer des listes contenant des données personnelles (p.ex. par courriel) ?	Lorsque c'est possible, il faut privilégier un lien sur un dossier commun interne au lieu de faire un envoi par courriel. Cela permet d'éviter une multiplication de cette même liste, ce qui n'est pas recommandé du point de vue de la protection des données. S'il n'est pas possible de faire un lien sur un dossier interne commun, il est recommandé de protéger le document par mot de passe et de transmettre ce mot de passe au ou à la destinataire par un courriel séparé ou par un autre canal (téléphone, SMS). Un cryptage e-mail général est recommandé.
34	Données personnelles : À quoi faut-il veiller lors de la transmission de données personnelles à l'étranger ?	Il y a transmission de données à caractère personnel lorsque celles-ci sont enregistrées physiquement à l'étranger (p.ex., hébergeur étranger) ou que des personnes ont un accès (<i>Remote Access</i>) depuis l'étranger à des données enregistrées localement (p.ex., support de logiciel par un fournisseur étranger). Lorsque des données à caractère personnel sont transmises à l'étranger, c'est la législation de cet état en matière de traitement des données qui s'applique. Si celle-ci n'est pas équivalente au droit local relatif à la protection des données, il faut prendre des mesures supplémentaires de sécurité et procéder à une analyse de risques. En résumé, il en va ainsi : 1. État tiers sûr : tous les États de l'EEE sont considérés comme des pays ayant un niveau suffisant de protection des données (États tiers sûrs), mais pas les USA (au moment de la rédaction de cette FAQ en décembre 2023), la Chine ou la Russie (États tiers non sûrs). Aucune mesure supplémentaire n'est nécessaire pour transmettre des données dans des États tiers sûrs. 2. Mesures adéquates de protection : transmettre des données dans des États tiers non sûrs implique de prendre des mesures supplémentaires ; il faut, par exemple, conclure des clauses de protection des données approuvées par l'autorité de surveillance ou conclure les clauses contractuelles types de la commission européenne. 3. Motif d'exception : des données ne peuvent être transférées à l'étranger sans mesures adéquates de protection que dans des cas exceptionnels. C'est le cas notamment lorsqu'il y a un accord formel ou que cette transmission est nécessaire pour préserver des intérêts prépondérants.
35	Banque de données personnelles : Quelles données ai-je le droit de stocker ?	Seules peuvent être enregistrées les données à caractère personnel qui sont indispensables à l'exécution des tâches de la paroisse ou de la commune ecclésiastique (principes de licéité, de proportionnalité, de finalité). Il n'est pas permis de saisir des informations supplémentaires en réserve sans but défini. En ce qui concerne les données personnelles effectivement autorisées pour la gestion des membres (en général avec le programme « KiKartei »), le droit cantonal prescrit les données (attributs) que la paroisse peut tirer du registre cantonal des habitants (principe de licéité).
36	Banque de données personnelles : Combien de temps puis-je garder ces données ?	Les données à caractère personnel peuvent être conservées seulement tant qu'elles sont nécessaires à leur finalité (principe de finalité). Elles devraient être effacées ensuite. Ce n'est pas toujours très facile à déterminer, car il se peut que la paroisse ou la commune ecclésiastique soit tenue de conserver certaines données pendant longtemps pour des raisons de traçabilité d'actions ecclésiales (registre des baptêmes, perception de l'impôt ecclésial). Si l'on constate cependant que certaines données ne sont plus nécessaires (p.ex., une ancienne adresse), il faut les détruire.

N°	FAQ	Réponse
		Pour ne pas oublier ces obligations, il faut procéder, une fois par année, à une journée de nettoyage des données avec tous les employés. Certains programmes informatiques ont des programmations automatiques de suppression de données.
37	Banque de données personnelles : Dans quels événements dois-je supprimer ces données ?	Il y a en principe deux situations dans lesquelles les données doivent être supprimées : 1. Lorsqu'elles ne sont plus utiles pour la finalité originelle de traitement. 2. Lorsque la personne concernée exige qu'elles soient effacées et que la paroisse ne puisse opposer aucune raison prépondérante à leur conservation. Une raison prépondérante de conservation peut être la tenue des registres ecclésiaux, si la traçabilité de certaines actions (p.ex., la date du baptême) n'est plus garantie autrement.
38	Feuille paroissiale : Puis-je publier les baptêmes, mariages, décès dans la feuille paroissiale ? Ai-je besoin d'une autorisation ?	Il en va de l'intérêt des membres de toute la paroisse de savoir qui y est nouvellement admis, qui s'y marie ou meurt parce que cela les concerne en tant que communauté. La publication des bans constitue une exception. Il est possible d'y renoncer avec une dispense. La dispense est donnée dans le cadre de l'entretien de préparation au mariage. Les personnes qui ne sont pas membres de la paroisse n'ont pas droit à l'information. Les personnes concernées sont informées de la publication lors des entretiens de préparation. Si quelqu'un ne veut pas de publication, sa volonté est respectée. CIC/1983 : c. 747 droit d'annonce, c. 220 Protection de la personnalité, c. 1067 Dispense de publication.
39	Droits (cf droits des personnes concernées) : Quels droits ont les personnes concernées ?	La LPD accorde certains droits aux personnes dont les données à caractère personnel sont traitées (appelées personnes concernées). Elles ont en premier lieu un droit de consultation, c-à-d. d'accès à leurs données, elles ont ensuite aussi le droit de faire corriger des données erronées et, éventuellement, de les faire effacer. Il existe un droit à remettre des données personnelles dans un format électronique usuel lorsque leur traitement est automatisé et que la personne concernée est d'accord ou pour remplir un contrat.
40	Vitrine : Ai-je le droit de publier des baptêmes, mariages, décès (dates des cérémonies d'ensevelissement) par un affichage public ? Ai-je besoin d'une autorisation ?	Il en va de l'intérêt de membres de toute la paroisse de savoir qui y est nouvellement admis, qui s'y marie ou meurt parce que cela les concerne en tant que communauté. La publication des informations à l'adresse des membres de la paroisse dans le cadre des messes est autorisée (cf. aussi Annonces). Les personnes concernées en sont informées dans les entretiens préparatoires. Si quelqu'un ne veut pas de publication (dans la vitrine, la feuille paroissiale), cette volonté est respectée. La publication des bans constitue une exception. Il est possible d'y renoncer avec une dispense. La dispense est donnée dans le cadre de l'entretien de préparation au mariage.
41	Médias sociaux : À quoi faut-il faire attention dans l'utilisation des médias sociaux (p.ex., Instagram, Facebook, TikTok, SnapChat, etc.) ? Peut-on les utiliser sans autre ? Sur quels points la prudence s'impose-t-elle ?	Il est recommandé de connaître le niveau de protection des données et les conditions d'utilisation des canaux de médias sociaux et de décider en conséquence si on veut ou non en utiliser un (qui en est l'exploitant, quelles sont les données collectées et où sont-elles stockées ?). Connaître et installer des paramètres de protection des données par défaut. Il est recommandé d'établir une directive interne sur l'utilisation que la paroisse veut faire d'un canal et sur la manière dont les collaboratrices et collaborateurs ont le droit de l'utiliser. Sans l'accord des personnes concernées, il

N°	FAQ	Réponse
		n'est permis de publier aucun post de vidéos, photos ou autres données relatives à des personnes. Instagram, Facebook, TikTok et SnapChat ne peuvent être utilisés sans autre. Ces canaux diffusent des discours de haine, collectent énormément de données pour en tirer des profils et revendent des données à des courtiers en données pour envoyer de la publicité personnalisée, etc... Il n'est pas exclu que les exploitants de ces canaux coopèrent avec les autorités dans des buts de surveillance.
42	Registre des baptêmes : A-t-on le droit de continuer à tenir des registres des baptêmes ?	Les registres des baptêmes sont toujours autorisés, car leurs informations sont indispensables comme preuves de la réception du baptême ainsi que d'autres sacrements (mariage, ordination, etc...). cf. cc. 535 ; 849 ; 473 § 1 CIC/1983
43	Registre des baptêmes : À qui ai-je le droit de communiquer des données du registre des baptêmes et lesquelles ?	Les données peuvent être communiquées au/à la fidèle, à ses parents ou éducateurs, à ses représentants légaux ainsi que, dans des cas motivés, à d'autres instances ecclésiales. Le renseignement doit être donné gratuitement et par écrit sous forme de photocopie, de document numérique ou d'une impression. Il n'est pas prévu de pouvoir consulter le document original, afin d'éviter la violation de la protection des données d'autres personnes. Ce droit porte sur les inscriptions de baptême, de confirmation, de mariage, d'ordination et d'entrée dans les ordres (c. 220 CIC/1983).
44	Registre des baptêmes : Faut-il mettre sur le formulaire d'annonce au baptême que ces données sont enregistrées ? Et à quelle fin ?	Le CIC/1983 part automatiquement de l'idée que les données sont inscrites dans le registre des baptêmes. Les personnes concernées (la personne qui va recevoir le baptême, les parents ou éducateurs) sont informées de cette procédure. Les formulaires officiels signalent le fait.
45	Registre des baptêmes : Les parents doivent-ils donner leur accord à l'enregistrement de ces données ?	Le CIC/1983 part automatiquement de l'idée que les données sont inscrites dans le registre des baptêmes. Le CIC/1983 part implicitement de l'idée que, en s'annonçant pour le baptême, les parents ou la personne qui va recevoir le baptême sont d'accord avec l'enregistrement des données.
46	Associations : Comment procéder avec des listes de membres ?	Les listes des membres d'associations doivent être protégées contre la perte ou une consultation non autorisée par des mesures adéquates. Par principe, elles ne doivent être tenues que pour permettre à la paroisse ou à la commune ecclésiastique d'exécuter sa tâche de manière licite (principe de licéité) et les principes de la protection des données doivent être respectés (notamment la minimisation : droit d'accès restrictifs, saisie des seules données indispensables, et la sécurité : stockage dans un environnement protégé, evt. protection par mot de passe lors de l'envoi, etc...). Les membres doivent être informés de l'utilisation qui sera faite des listes lors de la collecte de leurs données (principe de transparence, accord des personnes concernées). Des listes de membres qui sont transmises doivent être protégées par mot de passe, surtout si elles comportent un grand nombre de données à caractère personnel. Avant de les transmettre, il faut vérifier si la personne ou l'organisation de destination est autorisée à recevoir ces données – si ce n'est pas le cas (p.ex., parce que ladite personne/organisation ne remplit plus de tâches ecclésiales), il faut demander l'autorisation des personnes concernées. Dans les envois internes à la paroisse, il ne faut pas

N°	FAQ	Réponse
		attacher les listes à un courriel, mais donner un lien sur un dossier commun. L'association est la première responsable de la protection des données.
47	Annonces : Peut-on annoncer à la messe par oral que NN est mort et sera enterré tel jour à telle heure au cimetière ?	Il en va de l'intérêt des membres de toute la paroisse de savoir qui y est nouvellement admis, qui s'y marie ou meurt parce que cela les concerne en tant que communauté. Les célébrations des messes sont en principe publiques. Y faire une annonce par oral est autorisé. Les personnes concernées en sont informées dans les entretiens préparatoires. Si quelqu'un ne veut pas d'annonce, cette volonté est respectée.
48	Visioconférence : Y a-t-il des dispositions relatives à l'utilisation des services de visioconférences (p.ex., Zoom, Teams, etc..) ?	Les paramètres de protection des données varient considérablement d'une offre à l'autre. Il en va de même pour leur mode d'utilisation, lequel peut être considérablement amélioré par un paramétrage du compte administrateur et par la conclusion d'un contrat de sous-traitance. Cela requiert en général pas mal d'efforts et exige d'étudier soigneusement le mode de fonctionnement technique du service ainsi que les dispositions contractuelles correspondantes. Parmi les principaux services de visioconférences, Webex (de Cisco) passe pour particulièrement sûr. Il faut en tout cas installer des paramètres de protection des données par défaut. Et il est recommandé de définir des règles de comportement, comme ne pas discuter de données personnelles particulières, ne pas enregistrer les entretiens.

Responsable : Vicariat général
Première publication : 01.03.2024
Dernière mise à jour :