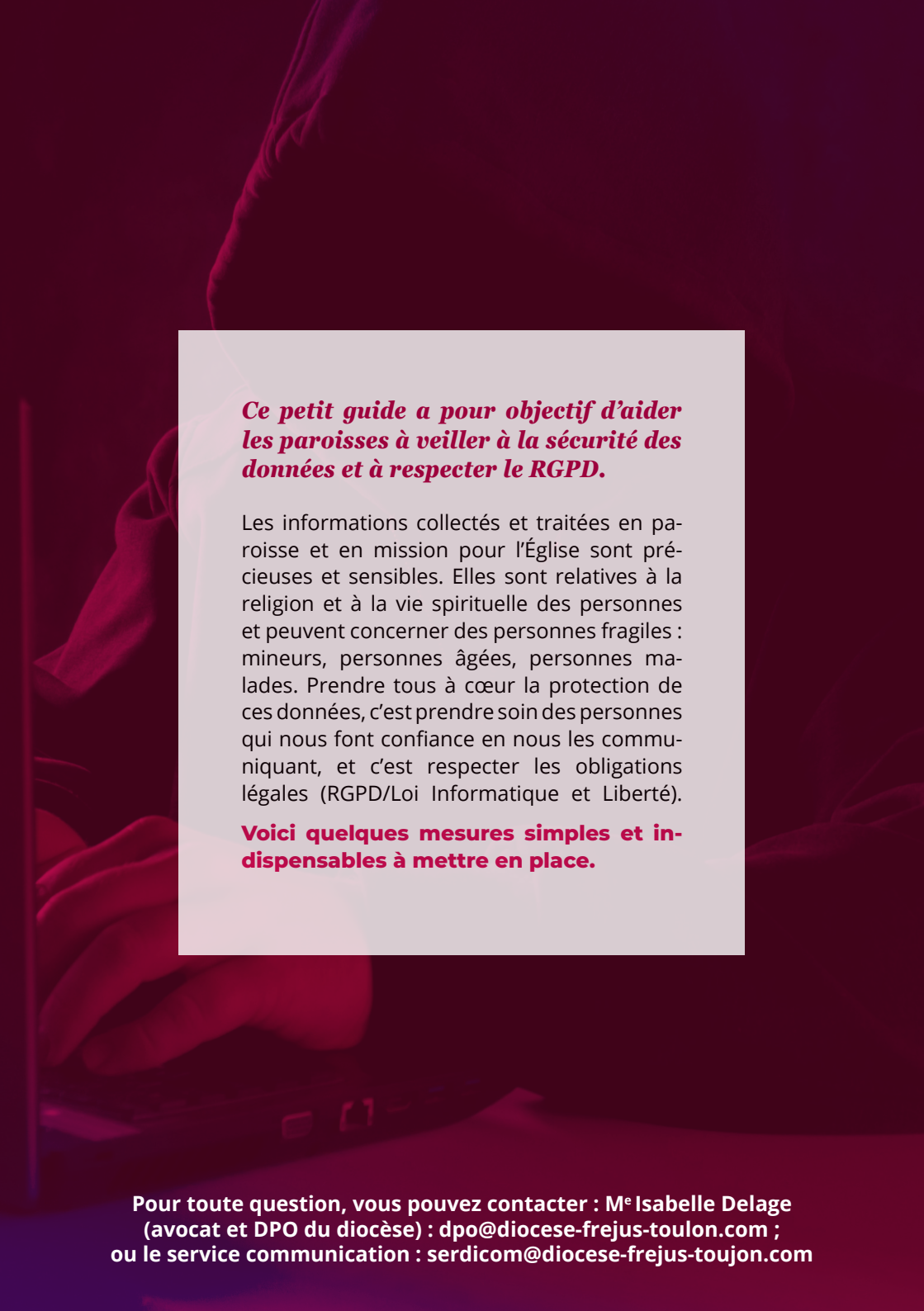
Le point Com'

SÉCURITÉ & RGPD

Piratage, cybercriminalité : que faire ?

diocèse de
FREJUS-TOULON



Ce petit guide a pour objectif d'aider les paroisses à veiller à la sécurité des données et à respecter le RGPD.

Les informations collectés et traitées en paroisse et en mission pour l'Église sont précieuses et sensibles. Elles sont relatives à la religion et à la vie spirituelle des personnes et peuvent concerner des personnes fragiles : mineurs, personnes âgées, personnes malades. Prendre tous à cœur la protection de ces données, c'est prendre soin des personnes qui nous font confiance en nous les communiquant, et c'est respecter les obligations légales (RGPD/Loi Informatique et Liberté).

Voici quelques mesures simples et indispensables à mettre en place.

Pour toute question, vous pouvez contacter : Me Isabelle Delage (avocat et DPO du diocèse) : dpo@diocese-frejus-toulon.com ; ou le service communication : serdicom@diocese-frejus-toujon.com

Les mots de passe

CHOISISSEZ UN MOT DE PASSE UNIQUE ET SOLIDE POUR CHAQUE UTILISATION

- Pour accéder à votre ordinateur
- Pour accéder à votre mobile
- Pour votre messagerie (mot de passe qu'il est essentiel de bien protéger)
- Pour chaque site web et application

Critères pour un mot de passe solide :

- Il contient au moins 12 caractères et 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux.
- Il ne dit rien sur vous.
- N'utilisez pas un mot de passe unique pour tous vos comptes, mais un mot de passe spécifique pour chacun.

NE COMMUNIQUEZ JAMAIS VOS MOTS DE PASSE

Votre mot de passe doit absolument rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « *maintenance* » ou un « *dépannage informatique* ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

NE STOCKEZ PAS VOS MOTS DE PASSE EN CLAIR

Astuce :
Il est humainement impossible de retenir des dizaines de mots de passe : ne les notez pas sur un papier, dans votre messagerie, dans votre téléphone, mais utilisez un gestionnaire de mot de passe. Comme cela, vous n'aurez qu'un seul mot de passe à retenir ,la technologie fera le reste. Exemple : www.keepass.info

CHANGEZ RÉGULIÈREMENT VOS MOTS DE PASSE ET IMMÉDIATEMENT EN CAS DE DOUTE.

Installez un anti-virus et un pare-feu

Utilisez une solution antivirus (payante) et tenez-la à jour. Configurez votre pare-feu. Même si aucune solution n'est totalement infaillible, de nombreux produits peuvent vous aider à vous protéger des différentes attaques.
Cette mesure est indispensable et élémentaire, que vous utilisiez un PC ou un Mac.

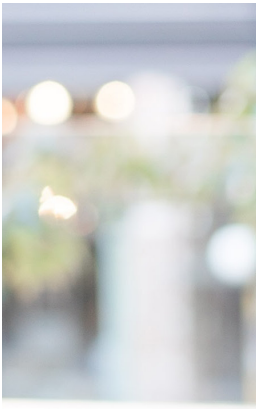
Les mises à jour

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'une montre connectée ou d'un équipement mobile. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour.
Mettez à jour sans tarder l'ensemble des applications et appareils et activez les mises à jour automatiques.

Distinguez les usages

Si vous en avez la possibilité, utilisez l'ordinateur mis à votre disposition par le diocèse ou la paroisse.

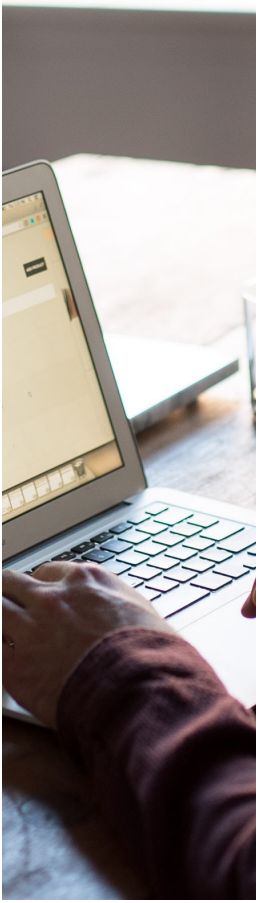
Si vous utilisez votre ordinateur personnel, alors vous utilisez sans doute les mêmes appareils pour vos missions paroissiales et / ou pastorales et votre usage personnel. Créez un compte utilisateur et un mot de passe différents pour vos activités personnelles et vos activités en paroisse ou en mission. Si vous ne le faîtes pas et qu'un des services auquel vous accédez se fait pirater, les données sensibles que vous traitez seront piratées également.



Protégez les données stockées

Les données stockées sur vos ordinateurs, téléphones portables, ordinateurs portables ; clés USB doivent être chiffrées. En cas de vol, seul le chiffrement des données contenues dans votre appareil empêchera une personne malintentionnée de contourner les codes d'accès et d'accéder quand même à vos informations.

Les données papier aussi doivent être protégées et doivent toujours être rangées sous clefs en lieux sûr.



Sauvegardez

En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques, vous perdrez les données enregistrées sur ces supports. Il peut s'agir de données sensibles traitées dans le cadre de votre mission pour l'Église, de données auxquelles vous accordez une importance particulière, ou que vous considérez comme essentielles. Ayez le réflexe de réaliser régulièrement une sauvegarde au moins partielle des données les plus essentielles et précieuses dont bien sûr celles de la paroisse ou de votre mission pastorale. N'oubliez pas de chiffrer les données sauvegardées.

Restituez ou détruisez

Ne conservez pas infiniment les informations que vous avez collectées ou traitées.

A la fin de la mission, ou lorsque les informations ne sont plus utiles, demandez des instructions au curé de la paroisse ou au responsable de la mission, afin de les restituer (sans conservation de copies) ou de les détruire (définitivement).

Utilisez des réseaux sécurisés

CHEZ VOUS OU À LA PAROISSE :

Assurez-vous du bon paramétrage de votre box Internet : vérifiez son mot de passe d'accès administrateur, changez-le s'il est faible et mettez à jour son logiciel interne. Le site web de votre opérateur (par exemple celui de Bouygues, SFR, Orange et Free), vous accompagnera dans la bonne mise en œuvre de ces étapes.

WIFI : activez l'option de chiffrement WPA2 ou WPA3, désactivez la fonction WPS et supprimez le Wi-Fi invité.

EN MODE NOMADE :

Les réseaux wifi publics dans les gares, restaurants, hôtels etc. ne sont pas sécurisés.

Tout ce que vous saisissez est donc visible pour une personne malveillante.

N'utilisez aucun mot de passe sur ces réseaux et ne les utilisez jamais quand vous traitez des informations de la paroisse ou de la mission pastorale.

COMMENT RECONNAITRE LES RÉSEAUX ?

Ne vous connectez qu'aux réseaux wifi avec un cadenas.

Vous pouvez aussi souscrire l'abonnement à un VPN (Virtual Private Network ou réseau privé virtuel) ce qui sécurise votre navigation et vos échanges.

Communiquez en toute sécurité

Ne transmettez pas de fichiers relatifs à vos missions et contenant des listes de personnes ou des informations confidentielles via des services grand public de stockage, de partage de fichiers en ligne, d'édition collaborative ou via des messageries. À défaut, chiffrez les données avant de les transmettre et transmettez les codes par un canal de communication distinct (par exemple par SMS). Des logiciels grand public comme 7-zip pour Windows et 7zX pour Mac OSX permettent de chiffrer les données avec des algorithmes réputés fiables.

Utilisez une adresse de messagerie dédiée pour votre mission pastorale (diocésaine ou paroissiale), distincte de votre messagerie personnelle. Si le diocèse ou la paroisse ne vous fournit pas une adresse de messagerie, créez un compte dédié à votre mission (avec un mot de passe sécurisé) non partagé avec les personnes de votre entourage.

Téléphones mobiles

Parce qu'ils vous accompagnent partout et contiennent un nombre impressionnant de données les téléphones portables qui sont particulièrement exposées à la perte et aux vols doivent être sécurisés :

- **Activez le code PIN :** Pour protéger votre téléphone ne désactivez pas le code PIN et changez celui proposé par défaut.
- **Activez le code de verrouillage** et mettez en place un délai de verrouillage automatique du téléphone.
- **Utiliser un code complexe** et évitez les codes trop faciles (date de naissance, 0123, etc.).
- **Activez le chiffrement** des informations sur votre téléphone lorsque c'est possible.

TUTO - COMMENT CHIFFRER LES DONNÉES DE SON SMARTPHONE

Attention le chiffrement est irréversible : pour le désactiver, un paramétrage de données d'usine et donc la suppression totale de vos données est nécessaire !

- Rendez-vous dans les paramètres « sécurité » de votre téléphone (Android ou iOS).
- Assurez-vous que la batterie de votre téléphone atteint une capacité supérieure à 80%.
- Appuyez sur la fonction « chiffrer ».
- Votre smartphone vous demandera un mot de passe à chaque déverrouillage.

- **Notez le numéro « IMEI » du téléphone** pour le bloquer en cas de perte ou de vol.
- **N'installez des logiciels que depuis les plateformes officielles et évitez à tout prix les applications de sources inconnues :** lorsque vous installez de nouvelles applications sur votre appareil, lisez les conditions d'utilisation et la politique de confidentialité et limitez les données auxquelles elles peuvent avoir accès au strict nécessaire.
- **Réglez les paramètres de géolocalisation** afin de toujours contrôler quand et par qui être géolocalisé.

Soyez vigilants quant aux tentatives de piratage par e-mail

N'ouvrez les pièce jointes et ne cliquez sur les liens que si vous êtes certain qu'ils proviennent d'une source sûre et d'un destinataire connu.

- Attention aux emails de destinataires inconnus ou provenant faussement d'organismes tels que banques, impôts, police (le texte fait souvent référence à une situation d'urgence, de danger ou de secret ou peut créer un sentiment de crainte ou d'inquiétude).
- Attention aux e-mails prévenants de destinataires connus mais au texte surprenant et inhabituel, il est probable que le compte a été piraté et qu'une tentative d'escroquerie est en cours.

En cas de doute vérifiez la source en téléphonant par exemple à l'expéditeur.

Alertez immédiatement en cas d'incident

Un incident peut être :

- Un acte de malveillance (phishing, vol de matériel, frande externe ou interne, accès frauduleux, manipulation de données, bombre logique, logiciels malveillants, défiguration de sites, etc.)
- Un accident (incendie, panne matérielle,e tc.) entrainant une indisponibilité des données
- Une personne malveillante ou qui enverrait un fichier avec des données personnelles pour un usage détourné par courrier électronique,
- Un cryptolocker qui rend indisponibles les données

Dans un de ces cas, ***alertez immédiatement*** le responsable (curé de la paroisse, responsable de groupe) qui devra à son tour transmettre à l'Évêché, aux adresses suivantes : informatique@diocese-frejus-toulon.com et econome@diocese-frejus-toulon.com.

Nous avons 72h pour faire remonter la violation à l'État ; cela engage la responsabilité partagée de l'ADFT et du curé.

Des mesures appropriées devront être prises sans délai afin de respecter la législation en vigueur et de protéger les personnes dont les données auront été compromises.

Pour toute question,
vous pouvez contacter :

Me Isabelle Delage
(avocat et DPO du diocèse)
dpo@diocese-frejus-toulon.com

ou le service communication
serdicom@diocese-frejus-toujon.com

Alerte incident :
informatique@diocese-frejus-toulon.com
econome@diocese-frejus-toulon.com