MODULE 18

Systèmes de classement et gestion des documents

Les avocats et les ONG qui travaillent sur des affaire de torture doivent avoir mis en place des systèmes efficaces de gestion des documents. Il est utile de disposer d'une structure de gestion des dossiers qui soit uniforme dans toute l'organisation et qui permette aux membres actuels et futurs du personnel de naviguer et de localiser facilement les dossiers. Certaines organisations peuvent utiliser des outils de gestion des dossiers en ligne ou de stockage dans le cloud pour faciliter la gestion et le stockage des documents.

1. Gestion des documents

Systèmes de classement : Si possible, il convient de conserver des copies électroniques de tous les documents afin de ne pas perdre les dossiers. Les fichiers électroniques sont souvent moins vulnérables aux saisies. Si vous utilisez des outils en ligne pour la gestion des documents, assurez-vous qu'ils répondent aux exigences de sécurité nécessaires.

Configuration des dossiers et sous-dossiers pour chaque affaire : Lorsque les dossiers sont stockés sous forme électronique, les dossiers peuvent être organisés comme suit, avec des sous-dossiers : (i) Administration ; (ii) Documents de référence ; (iii) Correspondance ; (iv) Soumissions ; (v) Décisions ; et (vi) Mise en œuvre.

Convenir d'une convention d'appellation pour les documents : Il est utile de convenir d'une convention d'appellation pour les documents, **par exemple**: Date (année/mois/jour) - Nom de l'affaire - Titre abrégé - Initiales de l'auteur.doc - Multiples brouillons.com.

Revue régulière des documents : Il est utile de revoir régulièrement les documents d'un dossier pour s'assurer qu'ils sont enregistrés correctement et qu'il ne manque rien dans le dossier.

2. Gestion de la correspondance

Toutes les communications doivent être effectuées de manière sûre et sécurisée. Le contact avec les survivants doit être maintenu tout au long d'une affaire, même pendant les périodes d'inactivité. Les organisations doivent conserver un registre de toutes les communications avec les survivants, en particulier lorsque des conseils ou des instructions sont donnés, ou que la stratégie est discutée avec des partenaires ou d'autres avocats.

Communication en personne ou par téléphone : Conservez un registre de toutes les communications - en personne ou par téléphone, des notes de réunion peuvent être prises pour résumer brièvement la communication et toute action convenue.

Correspondance par courrier électronique : Les systèmes basés sur le cloud qui permettent le classement automatique des dossiers sont utiles et, même lorsqu'il n'existe pas de systèmes automatisés, toutes les communications par courrier électronique doivent être copiées dans le dossier de l'affaire pour des registres précis.

Correspondance par voie postale : Toutes les lettres doivent être scannées et enregistrées dans le dossier électronique. Il suffit de conserver une copie scannée et de jeter la lettre originale, à moins que le document original ne soit pas remplaçable, **par exemple** un affidavit notarié ou un document judiciaire estampillé.

Correspondance avec les Cours et Tribunaux : La correspondance substantielle doit être envoyée dans une lettre formelle, qui peut être envoyée par courrier électronique et doit être envoyée conformément aux règles de procédure de la juridiction ou de l'organe concerné, **par exemple**, la CADHP accepte désormais les documents en version électronique uniquement (envoyés par courrier électronique). Les instructions pratiques de la juridiction doivent être examinées afin de déterminer s'il existe des exigences spécifiques en matière de format pour la correspondance et les plaidoiries écrites, **c'est-à-dire** que certaines exigent que les communications soient effectuées à l'aide de formulaires spécifiques.

3. Gestion et collecte des éléments de preuve

La collecte de preuves implique souvent plusieurs partenaires - en particulier lorsque l'affaire se situe en dehors de votre juridiction - et il est essentiel que les questions logistiques liées à la constitution d'une base de preuves soient prises en compte dès le début du processus.

Lors des entretiens, il convient de tenir compte des éléments suivants

- **Préparation :** quelles sont les informations que vous cherchez à obtenir ?
- **Logistique :** les personnes interrogées doivent se sentir à l'aise et en sécurité.
- **Langue :** vous aurez peut-être besoin d'un interprète, ce qui nécessitera une planification et un budget à l'avance.
- **Confidentialité :** vous devez expliquer comment leur déclaration sera utilisée et comment elle sera protégée.
- **Emplacement :** vérifiez si la personne interrogée se sent en sécurité et à l'aise.
- **Enregistrement et stockage :** demandez le consentement de la personne interrogée et assurez-vous que vous avez les moyens de stocker les données en toute sécurité.
- **Dispositions particulières :** les enquêteurs doivent avoir les connaissances et les compétences nécessaires pour mener les entretiens.
- **Autres considérations** : il peut s'agir notamment de l'impact du traumatisme sur la personne interrogée, de la présence d'un soutien médical ou psychologique, de la crainte de représailles, de la garantie de la sécurité de la personne.

De plus, toutes les preuves doivent être correctement nommées et classées dans le dossier de l'affaire et, si elles sont dans une langue autre que celle dans laquelle la soumission est rédigée, les fichiers doivent être traduits. La collecte ou le stockage des preuves peut

également présenter des risques de sécurité, tant pour le survivant que pour les organisations ; il convient donc d'évaluer ces risques, d'y faire face et d'adopter des mesures d'atténuation.

4. Registre des affaire et calendriers des litiges

En plus de sauvegarder les documents et d'enregistrer les communications, il est utile de suivre les mouvements significatifs d'une affaire en utilisant un registre d'affaires. Les registres doivent être régulièrement mis à jour et peuvent inclure des informations telles que : (i) le personnel affecté à l'affaire ; (ii) les coordonnées du survivant ; (iii) des informations sur le contexte de l'affaire ; (iv) les violations/crimes ; (v) les soumissions faites ; et (vi) et les prochaines étapes. L'enregistrement et le respect des délais sont cruciaux ; un délai non respecté peut priver un survivant de sa seule chance d'obtenir justice, vérité et réparations. Il est utile d'enregistrer les échéances de toutes les affaires dans un calendrier commun afin que les organisations aient une vue d'ensemble claire de la charge de travail et puissent planifier en conséquence.

5. Clôture d'un dossier de litige

Un dossier doit être clôturé de manière à ce que toutes les données liées à l'affaire soient traitées conformément aux obligations légales et éthiques, et en conformité avec les règles de réglementation des données applicables dans la juridiction concernée.

Quand clore une affaire : Les critères à prendre en compte lors de la clôture de l' affaire reflètent ceux utilisés au début d'un affaire, **c'est-à-dire le mandat et l'expertise, les considérations relatives aux survivants, les considérations relatives au affaire, la stratégie d' affaire, l'impact** et **les considérations relatives à l'organisation/aux ressources.**

Clôture d'un dossier : Une lettre peut être envoyée au survivant pour lui expliquer les modalités de stockage et/ou de destruction de son dossier. Les dossiers électroniques ne doivent pas être immédiatement détruits afin de se protéger contre tout risque d'action en justice qui pourrait être engagée concernant les conseils donnés.

Consentement : Les dossiers ne doivent pas être détruits sans le consentement du client. Si vous n'avez pas le consentement pour détruire le dossier, il faudra trouver un équilibre entre le coût permanent du stockage des dossiers et les risques liés à leur destruction (**par exemple**, que le client veuille récupérer le dossier ou qu'il dépose une plainte).

La sécurité numérique pour une gestion efficace des dossiers

1. Principes généraux de sécurité numérique

- **Prévenir :** Concevoir et mettre en œuvre un **plan de prévention des violations de données**. Ce processus doit inclure une formation sur les étapes et les procédures à suivre pour gérer une éventuelle violation et atténuer l'impact sur la vie privée et la sécurité des survivants.
- **Protéger :** Les outils de gestion d'affaire en ligne ou de stockage dans le cloud doivent répondre aux critères de sécurité nécessaires pour le travail qu'ils effectuent. Ils doivent être soutenus par des fournisseurs fiables, configurés pour réduire les failles de sécurité, administrés de manière sûre et responsable, et les failles de sécurité doivent pouvoir être identifiées en temps utile.

- **Réagir :** Dès que vous avez connaissance d'une violation de données, vous devez évaluer le type de données compromises par la violation, les groupes touchés, le préjudice potentiel qu'ils subissent du fait de la violation et mettre en œuvre un plan de récupération pour réparer les dommages subis.

2. Définir et comprendre les risuqes

Lors de l'évaluation des risques de sécurité, les avocats et les ONG doivent tenir compte des points suivants :

- Quelles sont les ressources informatiques les plus cruciales ?
- Quel type de violation de données aurait un impact significatif sur notre travail ?
- Quelles sont les sources des menaces et l'impact potentiel de chaque menace identifiée ?
- Quel niveau de risque sommes-nous prêts à prendre lorsque nous traitons des informations sensibles et confidentielles fournies par des survivants ?

3. Communication et partage d'informations en toute sécurité

Pratique générale : Lors du partage d'informations sensibles, les actions suivantes peuvent être envisagées :

- Utilisez des avis de confidentialité ou des clauses de non-responsabilité lorsque vous partagez des informations confidentielles par courrier électronique.
- Faire preuve de prudence lors de l'accès à des courriels, des liens ou des pièces jointes provenant de sources non familières.
- Utiliser des plateformes cryptées, telles que Tresorit, Protonmail, ou des systèmes de partage numérique, tels que le partage Office 365 ou Dropbox, pour partager des documents.

Mesures de sécurité renforcées : Pour renforcer la protection des communications et des informations, les avocats et les eTravailleurs peuvent :

- utiliser les noms de code du projet lorsqu'ils discutent des informations du projet avec des parties externes
- utiliser le courrier électronique de bout-en-bout, le partage de fichiers cryptés et les applications de messagerie et de voix cryptées
- utiliser des mots de passe pour les réunions sensibles sur Zoom
- utiliser des systèmes de messagerie privés et sécurisés tels que Signal, et envisager d'activer la disparition des messages
- Organisez des réunions en face à face et éteignez vos téléphones ou laissez-les en dehors de la salle de réunion.
- Nettoyez le bureau et la corbeille de recyclage de votre téléphone et de votre ordinateur portable lors de vos déplacements
- Protégez les documents sensibles en ajoutant des mots de passe
- Fournissez des impressions de documents lorsque la situation de sécurité l'exige.
- Utilisez un inspecteur de documents Microsoft pour supprimer les métadonnées lorsque la sécurité est en jeu.
- Utilisez des comptes de médias sociaux anonymes pour rechercher des personnes d'intérêt.
- Utilisez la fonction "incognito"/"navigation privée" pour protéger votre historique et vos cookies lorsque vous effectuez des recherches.

Préparation et gestion des violations : Il faut mettre en place une stratégie pour atténuer les dommages causés, signaler les obligations, attribuer les responsabilités et permettre l'accès à des recours et à des compensations si nécessaire.

Compliance : Le personnel doit être conscient des obligations de protection des données lorsqu'il collecte ou traite des données soumises à des normes régionales/domestiques dans leur juridiction, **par exemple**, les organisations de l'UE sont tenues de collecter et de traiter les données personnelles conformément à leurs responsabilités en vertu du RGPD.