Charte d’assistance aux personnes concernées

Un grand pouvoir implique de grandes responsabilités

En tant que personne allant assister des personnes concernées dans leurs démarches administratives, vous allez avoir accès à des documents très personnels de tiers engagés dans des procédures suite à des violations de leurs droits.

Cette charte a pour objectif d’encadrer ce traitement de données à caractère personnel, certaines pouvant relever de l’article 9 du RGPD (données sensibles).

1. Les échanges avec la personne concernée doivent être dans la mesure du possible chiffrés avec GPG (si elle en a fait la demande ou possède une clef). Les communications internes par mail doivent être obligatoirement chiffrées avec GPG (Schleuder s’en occupe pour vous côté réception extérieure). Attention à votre fournisseur d’email : les emails personnels US/GAFAM & cie seront bien entendus non utilisables côté association pour ce type de communication. Faites éventuellement valider votre fournisseur par un administrateur en cas de doute.
   1. : Infomaniak, Scaleway, Hertzner, AlwaysData, Proton, RiseUp
   2. : Google, Apple, Microsoft
2. Les documents dont vous pourrez avoir connaissance ne doivent être communiqués à des tiers non habilités sous aucun prétexte. L’association a pour vocation à être transparente sur ses dossiers et à communiquer autant que possible sur ceux-ci, mais l’anonymat d’éventuelles communications publiques sur un dossier doit être garanti.
3. Lors des réponses à une personne concernée ou d’échange interne à l’association, assurez-vous avant envoi du destinataire afin d’éviter de communiquer des informations à la mauvaise personne
4. Les échanges de coordination/relecture ne doivent passer que par des canaux sécurisés approuvés par l’association
   1. liste de diffusion procedures@
   2. canal dédié Mattermost
   3. section dédiée restreinte du forum

   Sur des échanges personnels concernant un dossier, l’usage de canaux sécurisés est aussi obligatoire
   1. Signal, Matrix :
   2. Whatsapp, Telegram, SMS :

   Le chan IRC #purr-procedures n’est pas suffisamment fiable (contrôle par un tiers et communications non chiffrées) pour véhiculer des informations précises concernant un

dossier et doit servir uniquement pour la coordination générique et les échanges plus informels.
5. Les documents fournis par les personnes concernées ou produits par l'association doivent être stockés sur des machines sécurisées pour éviter toute communication à un tiers. L'association n'intervient pas dans un environnement aussi contrôlable qu'en entreprise, et il s'agit bien sûr de vos machines personnelles, mais les éléments suivants sont à vérifier :
    1. De préférence disque chiffré (FDE LUKS), sinon conteneur VeraCrypt chiffré
    2. Mot de passe de session conforme aux standards ANSSI
    3. Verrouillage du poste ou du conteneur chiffré hors utilisation
    4. Idéalement sur matériel non nomade et non partagé
    5. En cas de matériel nomade ou partagé, l'usage de conteneur Veracrypt ou équivalent est nécessaire pour éviter qu'une personne ayant aussi accès à votre machine puisse accéder aux données sensibles en votre possession.
6. La 2FA doit être activée dès que possible sur vos comptes liés aux outils de coordination (forum, IRC, etc)
7. Des précautions toute particulières doivent être prises dans le cas de contact avec des lanceurs d'alerte. Signalez par un canal sécurisé à un administrateur de l'association tout dossier ou personne dans ce cas, afin de prendre les mesures adéquates à chaque situation.
8. En cas de rupture de confidentialité, même mineure, vous devez en informer un administrateur de l'association dans les meilleurs délais, pour prendre les mesures correctrices adéquates et permettre les déclarations légales obligatoires le cas échéant. Commettre une erreur arrivera à tout le monde.
9. N'hésitez jamais à poser une question en cas de doute.

TODO possible à faire côté association :

- fournir des boîtes mails
- ~~Mattermost~~
- Instance Matrix

Pour signer la charte :

```
curl https://wiki.asso-purr.eu.org/books/conformite/page/charte-dassistance-aux-personnes-concernees/export/pdf -o charte.pdf
gpg --detach-sign --armor charte.pdf
```

et envoyer les 2 fichiers (`charte.pdf` et `charte.pdf.asc`) par mail à `bureau@`

Revision #13
Created 2024-09-05 21:22:27 UTC by aeris
Updated 2024-10-05 22:45:08 UTC by aeris