Recommandation pour l'utilisation de la messagerie électronique et de Microsoft Teams dans le public cloud

1. But

   La présente note est une recommandation quant à l'utilisation de la messagerie électronique et la tenue de conférences en ligne et d'appels vidéo destinée à assurer la sécurité et le respect de la confidentialité des données à caractère personnel dans la communication entre les institutions, avec des entreprises, des citoyens et des tiers.

2. Champ d'application

   La recommandation concerne les services Microsoft 0365 "Exchange online" et "Teams" proposés dans le public cloud.

   La recommandation s'applique à l'ensemble des collaborateurs à la fois internes, externes (consultants) et temporaires.

   Il est souhaitable de prévoir une extension ou un ajout qui couvre les applications de messagerie électronique et les outils collaboratifs de différents fournisseurs dans une version ultérieure de cette recommandation.

3. Classification des données

   Les titulaires de processus doivent systématiquement classifier les données conformément à la Politique fédérale sur la sécurité de l'information (FISP). Les titulaires de processus doivent informer les utilisateurs de manière suffisante à ce sujet.

4. Détermination du risque

   Le risque que des données sensibles, telles que des données à caractère personnel, soient insuffisamment protégées lors de l'utilisation des services Microsoft 0365 est élevé.

   Microsoft prend diverses mesures de sécurité pour protéger ses environnements. Néanmoins, il subsiste un risque de traitement illicite et d'exportation illicite de données.

5. Recommandation générale

   La recommandation générale est que les collaborateurs ne partagent pas de données à caractère personnel en provenance d'e-mails, de dossiers ou d'autres sources par le biais de la messagerie électronique ou de Teams.

Ce type de traitement numérique doit passer par des canaux sécurisés tels que les plateformes d'échange ou les applications des institutions.

Cette recommandation s'applique à toutes les communications entre les institutions, avec des entreprises ou avec des citoyens.

Pour les e-mails entrants contenant des données à caractère personnel, il est également recommandé de ne pas envoyer de réponses contenant des données à caractère personnel, et nous proposons de recourir aux canaux sécurisés.

Exemple : une institution souhaite transmettre à une autre institution un ou plusieurs documents contenant des données à caractère personnel. Pour ce faire, l'institution peut en premier lieu utiliser les possibilités d'échange applicatif (exemple : API). Si cela n'est pas possible, il est possible d'utiliser Fedsender (Belnet) qui permet d'échanger ces documents sous forme chiffrée.

Exemple : un citoyen demande un état de son dossier par e-mail. L'institution envoie une réponse via l'eBox. L'institution renvoie à un portail où le citoyen peut consulter l'état et les détails de son dossier. Dans cette communication, aucune donnée à caractère personnel n'est transmise par l'institution.

Exemple : une institution met des informations actualisées concernant des dossiers à disposition sur l'un des portails gouvernementaux (MyPension, MyminFin...). Les citoyens et les entreprises qui souhaitent consulter ces informations et/ou fournir des données complémentaires le font en se connectant à ces canaux sécurisés.

6. <u>Exception à la recommandation</u>

   Dans la mesure où l'utilisation est limitée aux informations sur les personnes participant à l'échange d'informations ou sur les personnes dont un dossiers est traité et où l'échange ne divulgue aucune autre information sur ces personnes, dans les cas suivants, le risque lié à l'utilisation de Teams et de la messagerie électronique est acceptable :

   - Pour l'échange de données relevant du niveau de classification 0 de la FISP.
   - Pour l'échange de données d'identification et de contact simples telles que :
     - Nom et prénom
     - Adresse professionnelle (bâtiment, rue, numéro, boîte, code postal et commune)
     - L'organisation pour laquelle l'individu exécute sa mission professionnelle et la fonction au sein de cette organisation
     - Numéro de téléphone pour une prise de contact professionnelle
     - Adresse e-mail pour une prise de contact professionnelle
     - Références à des informations accessibles au public, telles que des références de contact professionnelles sur les médias sociaux (Facebook, Google+, LinkedIn)

- Métadonnées
    - contenant des données de production (exemple : titre d'un e-mail) : celles-ci doivent être traitées de la même manière que les données générales (voir ci-dessus) ;
    - nécessaires pour faciliter la réalisation technique de l'échange. Cela est comparable aux cookies, dont nous supposons que seules les données nécessaires sont traitées (par exemple, les participants à une conférence téléphonique, les adresses IP, la durée d'une conversation, les destinataires d'un e-mail, la qualité technique de la connexion de l'appel...).

7. Utilisation de canaux sécurisés

   Le collaborateur et l'institution disposent d'une série de canaux sécurisés pour traiter les cas où il n'est possible d'utiliser la messagerie électronique ou Teams.

   Vous trouverez ci-joint un arbre/tableau de décision qui recommande les différents moyens en fonction du destinataire, de la sensibilité de l'information et du type de communication.
   Cet arbre/tableau sera mis à jour si la situation l'exige.

   Les exemples de canaux sécurisés sont les suivants : messagerie électronique sécurisée, portail/site web, eBox Citoyen /Entreprise, applications sécurisées (Govapp, Wallet) ou éventuellement courrier postal.

8. Reporting des incidents

   Tout incident de sécurité suspecté lié à la messagerie électronique doit immédiatement être signalé au département IT et au DPO.

9. Évaluation et révision

   La présente recommandation sera périodiquement évaluée et révisée si nécessaire afin de s'assurer qu'elle est toujours efficace pour protéger les données. Les modifications feront l'objet d'un suivi par une gestion des versions.

10. Recommandations supplémentaires

    Il est recommandé de former les collaborateurs à l'identification des cyberattaques et de leur demander de signaler immédiatement les e-mails suspects.

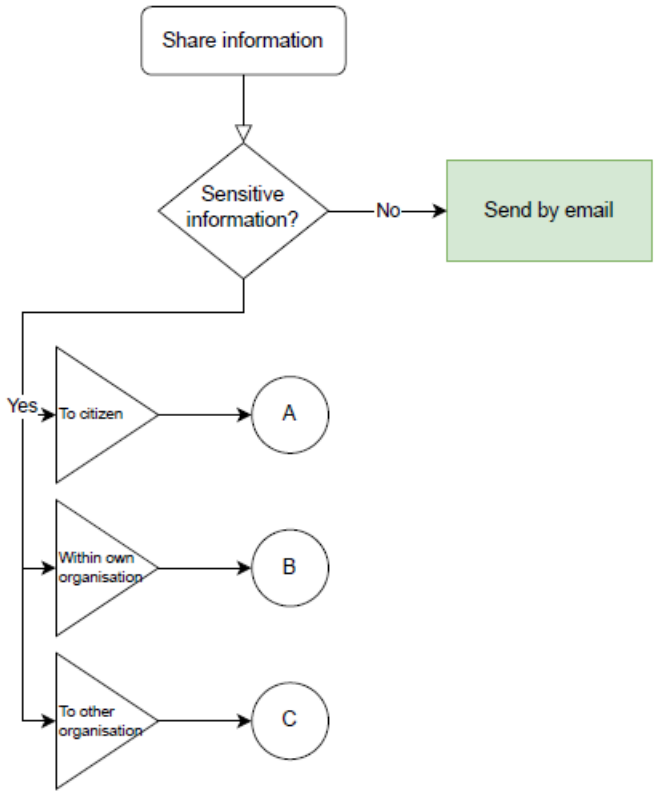
    Les appareils des utilisateurs et l'infrastructure seront configurés de manière à ne partager qu'un ensemble minimal de données des utilisateurs. Les directeurs IT disposent de bonnes pratiques pour mettre en œuvre cette recommandation.

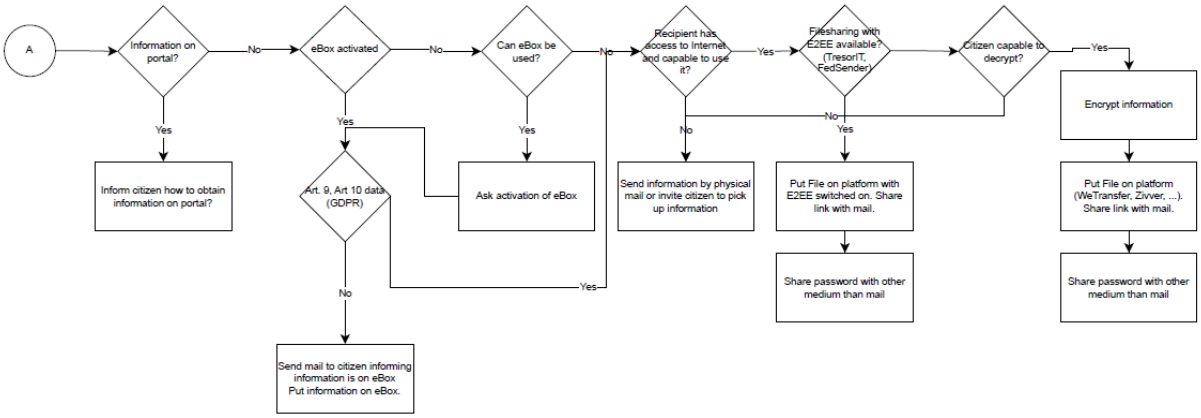
La présente recommandation peut être adaptée aux besoins et exigences spécifiques de votre institution. Il est important d'organiser régulièrement des campagnes de sensibilisation et des formations sur cette recommandation afin de s'assurer que tous les utilisateurs en sont informés et la respectent.

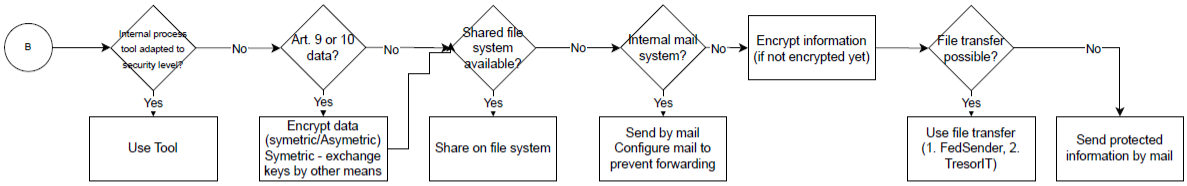
L'utilisation interne de la messagerie électronique et de Teams peut être établie depuis longtemps, en particulier dans les institutions publiques qui gèrent des dossiers (de citoyens), par exemple. Il est dès lors recommandé de créer une roadmap pour pouvoir satisfaire à ces recommandations dans le temps et/ou identifier exceptionnellement certains risques et leur impact et les accepter ou non (appétit pour le risque).

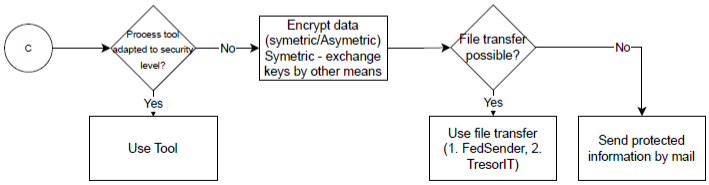
Annexes

Pour aider les institutions à déterminer les moyens de partager l'information, un arbre/tableau de décision qui recommande les différents moyens en fonction du destinataire, de la sensibilité de l'information et du type de communication sera créé et tenu à jour.









Remarque : Les articles 9 et 10 portent sur les données à caractère personnel sensibles telles que les données médicales ou les condamnations judiciaires. En raison du risque que l'accès à ces informations fait courir à la personne concernée, celle-ci doit bénéficier d'une protection supplémentaire.