CLUBEBIOS

COMMENT MENER UN PIA AVEC EBIOS RISK MANAGER ?

CONTEXTE

- Vous créez un traitement « *susceptible d'engendrer un risque élevé sur les droits et libertés des personnes physiques* ».
  - Il rencontre au moins 2 des 9 critères de « sensibilité » (voir exemples de traitements).
  - Et il ne fait pas l'objet d'une exception (voir exemples de traitements).
- Vous devez donc mener un PIA (*Privacy Impact Assessment,* appelé AIPD dans le RGPD).
- Pour ce faire, vous souhaitez utiliser la méthode EBIOS Risk *Manager* (Voir aussi les guides et le logiciel PIA de la CNIL).

ATELIER 1 : CADRAGE ET SOCLE DE SÉCURITÉ

1. Décrivez le traitement (fonctionnalités et système support) (ex : création de titres d'identité)
2. Évaluez les mesures que vous vous êtes engagés à respecter (ex : PSSI) et utilisez le « Socle pour la protection de la vie privée » (finalité, information, droits des personnes, *etc*, exemple au verso)
3. Imaginez ce qu'il pourrait arriver aux personnes concernées si, au regard des données traitées :
   - des personnes non autorisées y accédaient (ex : détournement d'une allocation, usurpation d'identité) ;
   - elles étaient modifiées de manière non désirée (ex : attribution d'un diagnostic, remboursement, délit, *etc.* à la mauvaise personne) ;
   - elles disparaissaient (ex : perte de chance en cas de prise en charge médicale, obligation de refaire les démarches).
4. Déterminez les mesures agissant sur le socle de sécurité ou ces événements redoutés (ex : utiliser des gabarits et non des données brutes, prévoir un mécanisme « brise-glace » en cas d'usurpation)

MESURES

ATELIER 2 : SOURCES DE RISQUES

1. Identifiez les principales sources de risques et leurs objectifs (ex : escroc à des fins de fraude)
2. Déterminez les mesures agissant contre ces couples (ex : rendre l'usage de la carte inutilisable par un fraudeur)

ATELIER 5 : TRAITEMENT DU RISQUE

1. Déterminez le plan d'actions (qui doit faire quoi ? quand ? quelles ressources ?)
2. Présentez et évaluez les risques résiduels
3. Consulter la CNIL si les risques résiduels sont encore élevés

ATELIER 4 : SCÉNARIOS OPÉRATIONNELS

1. Déterminez les principaux chemins permettant aux scénarios de se réaliser (ex : vol de cartes par un gardien corrompu)
2. Déterminez les mesures agissant sur ces scénarios opérationnels (ex : contrôles d'accès tracés)

ATELIER 3 : SCÉNARIOS STRATÉGIQUES

1. Identifier les tiers (sous-traitants, fournisseurs, partenaires, *etc.*)
2. Déterminez les principaux chemins dans l'écosystème permettant aux 3 événements redoutés de survenir (accès non autorisé, modification non désirée et disparition de données)
3. Déterminez les mesures agissant sur l'écosystème ou ces scénarios stratégiques (ex : renforcer la sécurité physique du producteur de titres)

Avec le soutien de l'ANSSI

CLUBEBIOS

COMMENT MENER UN PIA AVEC EBIOS RISK MANAGER ?

FOCUS SUR LE SOCLE POUR LA PROTECTION DE LA VIE PRIVÉE

Exemple : création de titres d'identité

PRINCIPES FONDAMENTAUX	ANALYSE DE CE QUI EST PRÉVU	CONCLUSION
Finalité(s)	Créer des titres d'identité, afin de permettre l'authentification (et non l'identification)	🟢 ○ ○
Fondement(s)	Traitement mis en œuvre pour le compte de l'État	🟢 ○ ○
Minimisation	Nécessaires au traitement : état civil, images de la photographie et de 2 empreintes digitales, signature	○ 🟠 ○
Destinataires	Forces de l'ordre, services de renseignement, autres traitements définis	🟢 ○ ○
Qualité des données	Vérification en mairie	🟢 ○ ○
Conservation	Durées fixées, en fonction du titre et de l'âge	🟢 ○ ○
Information	Décret et affichage en mairie	🟢 ○ ○
Consentement	Non applicable	⚫ ⚫ ⚫
Droit d'accès	Oui, auprès de l'autorité de délivrance	🟢 ○ ○
Droit à la portabilité	Non applicable	⚫ ⚫ ⚫
Droit de rectification	Oui, auprès de l'autorité de délivrance	🟢 ○ ○
Droit d'effacement	Non applicable	⚫ ⚫ ⚫
Droit de limitation	Non prévu	○ ○ 🔴
Droit d'opposition	Non applicable	⚫ ⚫ ⚫
Sous-traitance	Obligations fixées dans les contrats avec les partenaires	🟢 ○ ○
Transferts	Aucun transfert hors de l'Union européenne	🟢 ○ ○

🟢 Conforme 🟠 Présente un risque 🔴 À corriger ⚫ Non applicable

DERNIERS CONSEILS

Pour mener un PIA, il conviendrait d'impliquer les parties prenantes suivantes :

- le métier ou la maîtrise d'ouvrage, pour initier le PIA ;
- la maîtrise d'œuvre, pour déterminer les scénarios et mesures techniques ;
- le délégué à la protection des données (DPO), ou équivalent, pour orchestrer le PIA et son avis ;
- le responsable de la sécurité des systèmes d'information (RSSI), ou équivalent, pour son conseil ;
- le responsable de traitement, pour valider le PIA ;
- la CNIL si le PIA indique finalement que le risque est encore élevé malgré les mesures prévues.

Comité de rédaction :
Yaël COHEN HADRIA (experte individuelle), Matthieu GRALL (SODIFRANCE), Jean OLIVE (CGI BUSINESS CONSULTING), Maricela PELEGRIN-BOMEL (ANSSI), Josué PRISER (EDF) , Franck YVELIN (expert individuel)

Conception graphique : Creads

CLUBEBIOS
contact@club-ebios.org
@club_ebios
Club EBIOS
www.club-ebios.org

Avec le soutien de l'ANSSI