7 ANNEXE 3 - PROCEDURE DE GESTION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

Cette procédure s'applique à tous les agents de l'administration de la Polynésie française.

7.1 **Contexte**

En tant qu'agent de l'administration, vous êtes susceptible de soupçonner ou constater une violation de données à caractère personnel.

Une violation de données à caractère personnel est un incident de sécurité, qui se caractérise par la perte, l'altération et/ou la divulgation non autorisée (accidentelle ou malveillante) de données à caractère personnel. Tout traitement de données à caractère personnel comporte un risque de violation de données à caractère personnel. Par exemple, un pirate informatique réussit à s'infiltrer dans le système d'information, des informations sur un usager sont envoyées par erreur à la mauvaise personne, etc.

Il est primordial d'agir rapidement et de manière appropriée d'afin de limiter les conséquences pour les personnes concernées et de respecter le délai de notification éventuelle, prévu par la réglementation (72 heures maximum à compter de la découverte).

7.2 Déroulement

Étape	Rôle	Action
1	Tout agent	Constatation ou soupçon d'une violation.
2	Agent (ayant constaté/soupçonné)	Information immédiate du supérieur hiérarchique direct, du RIL du service, du chef de service et du DPO.
3	RIL	Inscription et suivi de la violation (dans l'outil Dastra).
4	RIL, en collaboration avec l'agent (ayant constaté/soupçonné)	Documentation de la violation (dans l'outil Dastra).
5	DPO	Analyse des risques de la violation puis émission d'un avis à destination du chef de service sur la nécessité de notifier la violation et les mesures de remédiation de la violation.
6	Chef de service	Mise en place des mesures de remédiation de la violation et, avant l'expiration d'un délai de soixante-douze (72) heures à compter de la découverte de l'incident, décision de notifier la violation (à la CNIL et aux personnes concernées).
7	RIL	Suivi des mesures de remédiation de la violation.