Le RGPD impose aux responsables de traitement :

* De documenter en interne les violations de données
* De notifier à la CNI les violations de données personnelles présentant un risque pour les droits et libertés des personnes
* De notifier aux personnes concernées les violations de données personnelles susceptible d’engendrer un risque élevé pour les droits et libertés d’une personne physique

Pour qu’il y ait violation de données personnelles 2 conditions doivent être réunis :

* L’organisme a effectué un traitement de données personnelles
* Ces données ont fait l’objet d’une perte de disponibilité, d’intégrité ou de confidentialité de manière accidentelle ou illicite

Il faut documenter l’incident :

* La nature de la violation
* Les conséquences probables de la violation de données
* Si possible, les catégories et le nombre approximatif de personnes concernées par la violation
* Les mesures prises ou envisagées pour éviter que cet incident ne se reproduise ou pour atténuer les éventuelles conséquences négatives
* Les catégories et le nombre approximatif d’enregistrements de données personnelles concernés

En cas d’incident qui peut constituer un risque élevé pour la vie privée des personnes, il faut en informer les personnes concernées.

