NEO DPO

La notification des violations de données personnelles

Art. 33 et 34 du RGPD

1. La notion de violation de données personnelles

✓ **<u>Définition</u>** : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données

✓ **<u>Exemples</u>, une violation de sécurité peut être consécutive à :**

- Une faille ou vulnérabilité de sécurité
- Un accident (incendie, panne matérielle, séisme, etc.)
- Une erreur de saisie, de manipulation, dans la conception de systèmes, etc.
- Une malveillance (*phishing*, vol de matériel, fraude externe ou interne, accès frauduleux, manipulation de données, bombe logique, logiciels malveillants, défiguration de sites, etc.)

2. L'obligation de notification

ST

Notifie au RT toute violation de données dans les meilleurs délais après en avoir pris connaissance afin de lui permettre de respecter son obligation de notifier, si possible, dans les 72 h

RT

Notifie à l'autorité de contrôle la violation dans les meilleurs délais, et si possible dans les 72 h de la connaissance de la violation **si la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques**

- Reçoit la notification
- Examine les éléments liés à la violation
- Conseille le RT sur les mesures à prendre
- Peut ordonner au RT de communiquer à la personne concernée la violation de données

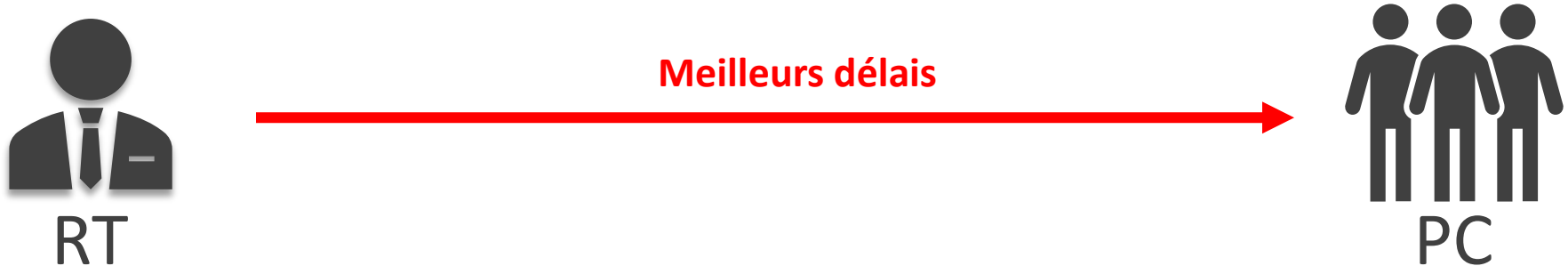
3. Contenu de la notification

✓ Via un téléservice dédié, La notification doit comprendre :

- Une description de la nature de la violation, y compris, si possible les catégories et le nombre approximatif de personnes concernées et les catégories et le nombre approximatif d'enregistrements de données personnelles concernées
- Le nom et les coordonnées du DPO ou d'un point de contact en mesure de communiquer des informations supplémentaires
- Une description des conséquences probables de la violation et des mesures prises ou que le responsable du traitement propose de prendre pour y remédier

✓ Les informations peuvent être communiquées en plusieurs fois, sans autre retard indu

4. L'obligation d'information des personnes concernées



- ✓ **PRINCIPE** : lorsqu'une violation de données à caractère personnel est susceptible d'engendrer **un risque élevé** pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais

- ✓ **EXCEPTIONS** :
  - Le RT à mis en œuvre les mesures de protection techniques et organisationnelles appropriées et si ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation. (ex : chiffrement)
  - Le RT a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser (par exemple en cas de vol de mot de passe, invalider l'ensemble des mots de passe objets de la violation)
  - Dans l'hypothèse où une notification individuelle exigerait des efforts disproportionnés, il peut être procédé à une communication publique (par exemple via une annonce sur un site internet)

5. L'obligation de documentation

✓ Le RT doit documenter **toute violation** de données à caractère personnel

✓ Cette documentation doit comporter :

- **Les faits concernant la violation des données à caractère personnel**
- **Ses effets**
- **Les mesures prises pour y remédier**

✓ Vise à permettre à l'autorité de contrôle de vérifier le respect des règles en matière de notification des violations des données

6. Synthèse

Pour les personnes concernées, la violation engendre :	Aucun risque	Un risque	Un risque élevé
Documentation en interne par le RT sous forme d'un registre interne des différentes violations dont il est victime	X	X	X
Notification à l'autorité de contrôle, c'est-à-dire la CNIL en France, si possible en 72h		X	X
Information des personnes concernées dans les meilleurs délais, hors cas particuliers			X

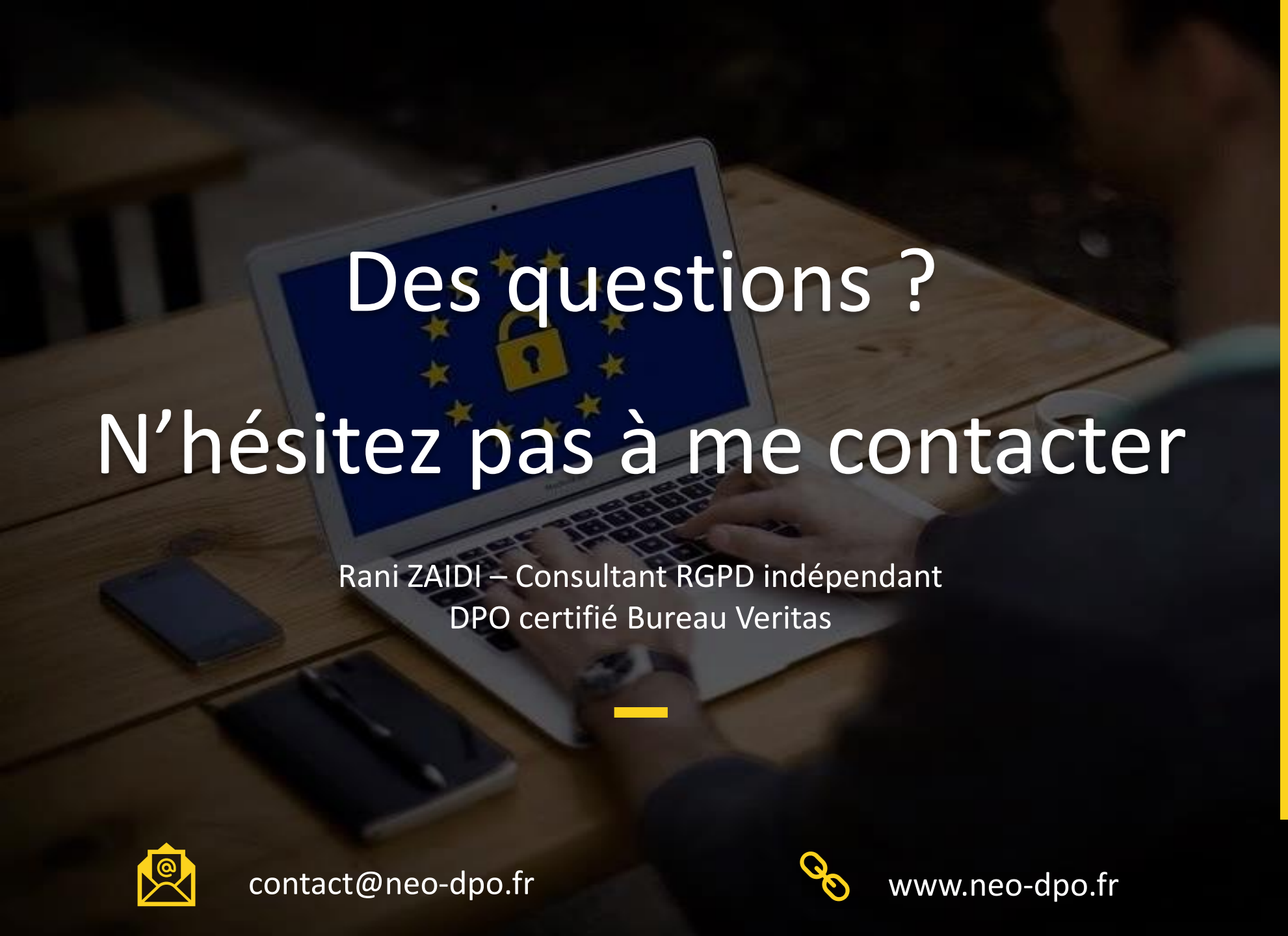
7. Pour aller plus loin

- ✓ Le CEPD (EX G29) a publié des lignes directrices au sujet de la notification des violations de données à caractère personnel :

https://www.cnil.fr/sites/default/files/atoms/files/wp250rev01_fr.pdf

- ✓ Le CEPD (EX G29) a également publié des lignes directrices spécifiques fournissant de nombreux exemples de violations de données personnelles afin d'aider à remplir ses obligations :

https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf



Des questions ?

N’hésitez pas à me contacter

Rani ZAIDI – Consultant RGPD indépendant
DPO certifié Bureau Veritas

contact@neo-dpo.fr

www.neo-dpo.fr

NEO DPO