Grant Thornton

Protection des données personnelles

Analyse des nouveautés phares apportées par la Loi n° 25-11

CONTEXTE ET OBJECTIFS POURSUIVIS :

Dans un contexte de renforcement continu de la protection des personnes physique dans le cadre de traitement de leurs données à caractère personnel, l'Algérie poursuit sa politique de modernisation du cadre juridique applicable afin d'aligner la législation locale sur les normes internationales.

À cet effet, la loi n° 25-11 du 24 juillet 2025, modifiant et complétant la loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, marque une évolution substantielle du dispositif algérien de protection des données personnel déjà en place.

Ce nouveau cadre législatif introduit des avancées significatives visant à consolider les garanties offertes aux personnes concernées tout en renforçant notamment les exigences de conformité pesant sur les responsables de traitement ainsi que les sous-traitants.

Il convient de noter que cette Newsletter se concentre sur les évolutions législatives récentes ayant un impact direct sur les obligations et la conformité des opérateurs économiques en Algérie.

NOUVELLES NOTIONS DÉFINITOIRES :

S'inscrivant dans une démarche de renforcement des exigences de conformité, le nouveau texte législatif enrichit le dispositif existant par l'introduction de nouvelles définitions. Celles-ci présentent une double portée : certaines revêtent un caractère essentiellement descriptif ou technique, tandis que d'autres constituent de véritables leviers de mise en conformité. Nous exposons ci-après les nouvelles définitions introduites par le nouveau texte.

a. Données biométriques : « données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique »

b. Profilage : « toute forme d'utilisation des données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts personnels, la fiabilité, le comportement, la localisation ou les déplacements de cette personne »

c. Pseudonymisation : traitement des données à caractère personnel de telle manière qu'elles ne puissent désormais être attribuées à une personne concernée sans recourir à des informations supplémentaires »

d. Autorité compétente : toute autorité publique compétente en matière de prévention et de détection des infractions, d'investigations, d'enquête et de poursuites, ainsi que d'exécution et d'application des peines, ou tout organisme ou entité jouissant des prérogatives de puissance publique et exerçant des pouvoirs de la force publique à des fins de prévention et de détection des infractions, d'investigations, d'enquête, de poursuites pénales, d'exécution et d'application des peines »

e. Violation des données à caractère personnel : « toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, la modification, la divulgation ou l'accès non autorisés aux données à caractère personnel transmises, conservées ou traitées d'une autre manière »

f. Organisation internationale : « toute entité et ses organes affiliés régis par le droit international public, ou tout autre organisme créé par un accord entre deux Etats ou plus, ou en vertu d'un tel accord. »

ORGANISATION DECENTRALISEE DE L'AUTORITE NATIONALE

L'article 27 bis de la nouvelle Loi dispose que « L'Autorité nationale est dotée de pôles régionaux chargés du contrôle et de l'audit auprès des institutions et des personnes traitant des données à caractère personnel. »

Cette disposition consacre une organisation décentralisée de l'autorité nationale de protection des ddonnées a ccaractère personnel « ANPDP », à travers la création de pôles régionaux chargés des missions de contrôle et d'audit. Elle traduit une volonté de renforcer l'effectivité des contrôles appelant ainsi les responsables de traitement à une vigilance accrue en matière de conformité.

EXIGENCES RENFORCÉES À FORT IMPACT OPÉRATIONNEL :

a. Obligation de désignation d'un délégué à la protection des données personnels « DPO »

Le délégué à la protection des données personnels constitue une passerelle entre l'ANPDP et le responsable de traitement celui-ci est désigné en pratique via un procès-verbal.

Il convient de noter que le délégué à la protection des données personnels est désigné notamment sur la base de ses connaissances spécialisées du droit et des pratiques relatives à la protection des données.

Il est possible de procéder à la mutualisation du délégué à la protection des données à caractère personnel entre plusieurs responsables de traitement ou autorités compétentes, selon les caractéristiques organisationnelles et dimensionnelles des entités concernées.

Aperçu non exhaustif des missions du Délégué à la protection des données :

- Informer et de conseiller le responsable du traitement et les personnels en charge du traitement des obligations qui leur incombent en vertu de la présente loi ;
- Contrôler le respect de la présente loi ainsi que des procédures internes du responsable du traitement en matière de protection des données à caractère

personnel, y compris la répartition des responsabilités, la sensibilisation et la formation des personnels participant aux opérations de traitement et aux opérations d'audits pertinentes ;

- Fournir des conseils, sur demande, en ce qui concerne l'analyse de l'impact du traitement sur la protection des données à caractère personnel et de surveiller sa mise en œuvre, conformément aux dispositions loi 25-11 susmentionnée.

b. Registres obligatoires :

1. Registre des activités de traitements :
   Le responsable de traitement ainsi le sous-traitant doivent tenir un registre des activités de traitement. Ce registre recense notamment les coordonnées des acteurs, les finalités et catégories de données, les destinataires, les délais de conservation et les mesures de sécurité mises en œuvre. Tenus sur support papier ou électronique, ces registres doivent pouvoir être communiqués à l'ANPDP sur demande.

2. Carnet automatisé des opérations de traitement:
   Le responsable du traitement et le sous-traitant doivent tenir un carnet automatisé des opérations de traitement, consignant toutes les opérations réalisées sur les données, leurs motifs, dates et identités des utilisateurs ou destinataires. Ce carnet sert au contrôle interne, à la vérification de la légalité des traitements, à la sécurité des données et, le cas échéant, aux procédures pénales, et doit être mis à disposition de l'ANPDP sur demande.

c. Etude d'impact

L'article 45 bis 6 instaure l'obligation de réaliser une étude d'impact préalable lorsqu'un traitement de données est susceptible de présenter des risques élevés pour les droits et libertés des personnes physiques. Cette étude doit permettre d'identifier les risques, de prévoir les mesures de protection appropriées et de démontrer la conformité du traitement aux exigences légales prévue par la loi en question.

d. Gestion des violations de données

Les articles 45 bis 8 à 45 bis 10 instaurent un dispositif complet de gestion des violations de données à caractère personnel, renforçant significativement les obligations pesant sur les responsables de traitement et les sous-traitants.

1. Notification rapide à l'autorité nationale :
   En cas de violation de données, le responsable du traitement est tenu de notifier l'autorité nationale dans un délai maximal de cinq jours (05) à compter de la découverte de l'incident. Toute notification tardive doit être dûment justifiée. Le sous-traitant est, quant à lui, soumis à une obligation d'alerte immédiate envers le responsable du traitement.

Contenu et modalités de la notification :

La notification doit décrire :

- La nature de la violation ;
- Les conséquences potentielles ;
- Les mesures correctives mises en œuvre ou envisagées.

Lorsque toutes les informations ne sont pas immédiatement disponibles, la loi autorise une communication échelonnée, favorisant une gestion pragmatique des incidents.

2. Traçabilité et accountability :
   Le responsable du traitement doit documenter l'ensemble des violations, leurs impacts et les mesures prises. Cette documentation constitue un élément central de preuve de conformité, permettant à l'autorité nationale d'exercer ses missions de contrôle.

3. Information des personnes concernées :
   Lorsque la violation est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques, les personnes concernées doivent être informées de manière claire et intelligible, avec une description des conséquences de l'incident.

Note aux lecteurs :
Les analyses et commentaires présentés dans la présente communication sont fondés sur textes en vigueur en Algérie à la date de sa rédaction. Ils sont fournis à titre strictement informatif et ne sauraient constituer une prise de position définitive ou un avis juridique engageant.

En conséquence, nous ne pouvons garantir que les interprétations ou appréciations formulées seront maintenues en cas d'évolution de la législation, de la jurisprudence, des pratiques administratives ou des positions des autorités compétentes.

Il est par ailleurs rappelé que notre intervention s'inscrit dans un rôle de conseil et d'accompagnement.

Nous vous prions d'agréer l'expression de notre considération distinguée.

Nous mettons à votre disposition les compétences de nos experts en la matière pour vous accompagner dans toutes les démarches et vous fournir les conseils adaptés à votre cas.

Veuillez accepter nos sincères remerciements.

Registered office: 01 Rue Ahmed El Affer, Lot Zedek, Ben Aknou, Alger, Algérie

Email : contact@dz.gt.com