Niveau 4

Gouvernance 2.0 : nouveau traitement – reclamation – amelioration continue

Mots clés : analyse d'impact - amélioration continue - archivage - données de mineurs - conservation - garanties suffisantes - guichet unique - mesures correctrices (sanction) - minimisation des données - traitement ultérieur - réclamation directe - réclamation (CNPD)

Luxembourg House of Cybersecurity

CNPD National Commission for Data Protection Grand-Duchy of Luxembourg

Co-funded by the European Union

Mise à jour : 4 Juin 2024

Amélioration continue (PDCA)

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire (Art. 24 RGPD).

NOUVEAUX TRAITEMENT, AYEZ LES BONS REFLEXES !

Finalité et traitement ultérieur

Conformément à l'article 5.1, b) du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

Ceci signifie qu'avant toute collecte de données, le responsable du traitement devra définir, de manière précise, la ou les finalités qu'il souhaite effectivement poursuivre en collectant ces données et ne pourra pas l'utiliser ensuite à d'autres fins. Par conséquent, un employeur qui décide d'installer un système de géolocalisation dans l'unique but d'assurer la protection de ses véhicules contre le vol, ne pourra pas ensuite l'utiliser pour contrôler le temps de travail de ses salariés. En effet, ceci constituerait une autre finalité pour laquelle les données n'ont pas été collectées et utilisées initialement et qui n'a notamment pas été portée à la connaissance des salariés.

Un traitement de données pour une finalité autre que celle pour laquelle les données ont été collectées ne peut avoir lieu que si la nouvelle finalité est compatible avec celle qui avait été initialement envisagée, conformément au principe de limitation des finalités.

Afin de déterminer si une finalité est ou non compatible, vous devez tenir compte des éléments suivants (si le traitement initial n'était pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit national pris en exécution de l'article 23 du RGPD):

- De l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé;
- Du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et vous;
- De la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9 du RGPD, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10 du RGPD;
- Des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées;
- De l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Quid du consentement des enfants ?

Si vous recueillez des données liées à des enfants, en particulier via votre site web commercial (p.ex. jeux en ligne, réseaux sociaux), il est nécessaire d'obtenir l'accord de leurs parents ou tuteurs légaux. L'information à l'égard des utilisateurs doit être facile à comprendre et formulée en des termes simples et clairs.

Principe de minimisation des données

Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Egalement appelé principe de nécessité et de proportionnalité, la minimisation des données signifie que vous devez traiter uniquement les données qui sont nécessaires (et non seulement utiles) à la réalisation des finalités

Pour en savoir plus :

Les grands principes

Traitement de données de mineurs

Le consentement de la personne concernée constitue une des bases juridiques ou « conditions de licéité » sur lesquelles peut se fonder un traitement de données à caractère personnel.

Les dispositions concernant les conditions applicables au consentement ont été approfondies par le RGPD, en insistant sur le caractère « libre, spécifique, éclairé et univoque » de celui-ci. La personne concernée doit donc avoir un véritable choix.

Par ailleurs, la personne concernée a le droit de retirer son consentement à tout moment, ce retrait ne compromettant pas la licéité du traitement fondé sur le consentement effectué avant ce retrait.

Pour en savoir plus :

Recommendations de l'EDPB

Analyse d'impact relative à la protection des données

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD, en anglais, Data Protection Impact Assessment ou DPIA).

L'analyse d'impact relative à la protection des données permet :

- D'élaborer un traitement de données personnelles ou un produit respectueux de la vie privée,
- D'apprécier les impacts sur la vie privée des personnes concernées,
- De démontrer que les principes fondamentaux du règlement sont respectés.

L'enjeu est d'apprécier les risques sur la protection des données du point de vue des personnes concernées.

Conformément à l'article 35.4 du RGPD, la CNPD a élaboré une liste de types d'opérations de traitement pour lesquels elle estime qu'une analyse d'impact sur la protection des données est obligatoire dans tous les cas.

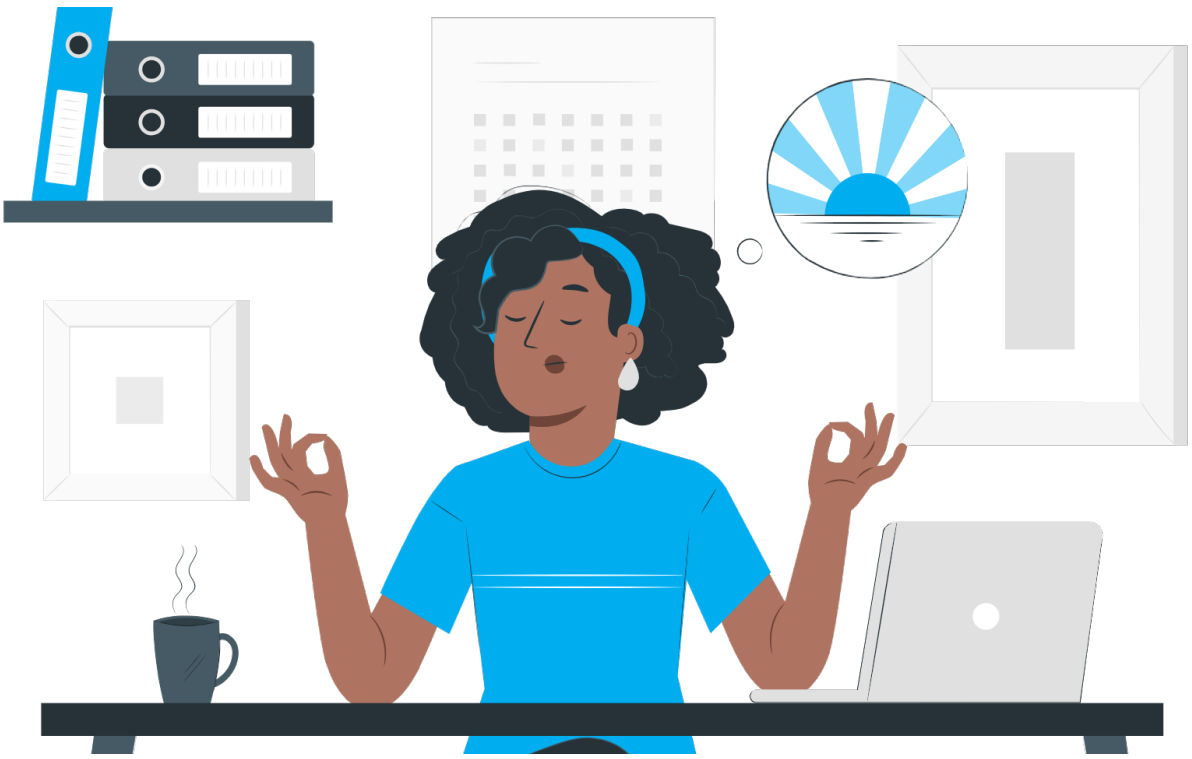
Rappel (Art. 35 et Art. 36 du RGPD):

- L'AIPD doit être exécutée avant la mise en œuvre du traitement ;
- Le responsable de traitement doit effectuer une consultation préalable au traitement auprès de la CNPD pour avis sur l'AIPD si le traitement présente encore un risque résiduel élevé pour les droits et libertés des personnes après la mise en place de mesures pour atténuer le risque.

Il convient de souligner que la liste actuelle n'est pas une liste exhaustive de tous les types d'opération de traitement nécessitant la réalisation d'une AIPD. Ainsi l'absence d'un type d'opération de traitement sur cette liste ne signifie pas nécessairement qu'une AIPD n'est en pas requise. La liste se limite aux activités de traitement qui nécessiteront toujours la réalisation d'une AIPD. Pour les activités de traitement ne figurant pas sur cette liste, les responsables du traitement des données devraient s'appuyer sur l'article 35 (1) du RGPD et sur les lignes directrices WP248 du groupe de travail de l'article 29 pour évaluer la nécessité d'une AIPD.

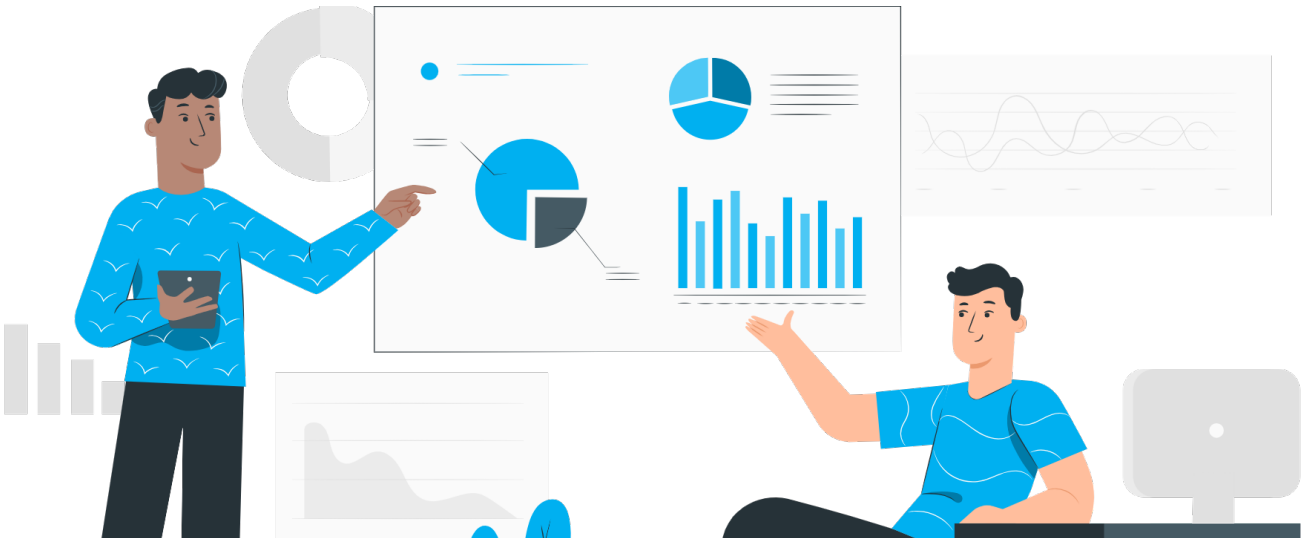
Pour en savoir plus :

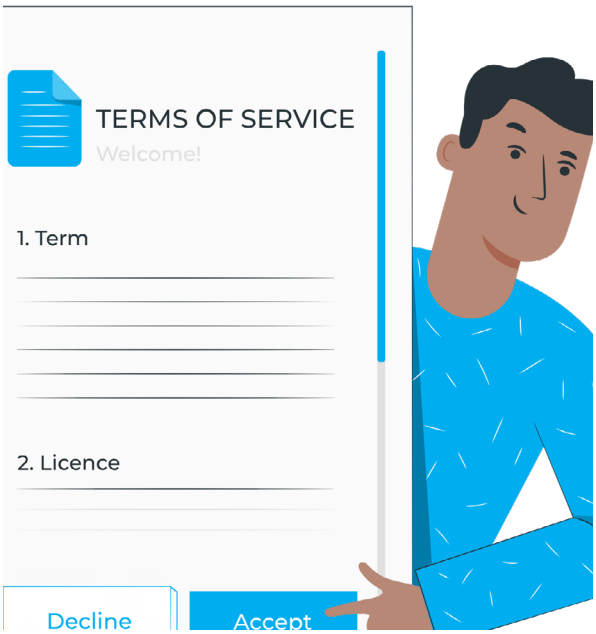
Sur le DPIA



Liste de traitements pour lesquels une analyse- d'impact sur la protection des données est obligatoire

1. Les opérations de traitement portant sur des données génétiques telles que définies à l'article 4 (13) du RGPD, en combinaison avec au moins un autre critère figurant dans les lignes directrices du Comité européen de la protection des données (ci-après : CEPD »), à l'exception des professionnels de santé qui fournissent des services de santé ;
2. Les opérations de traitement qui incluent des données biométriques telles que définies à l'article 4 (14) du RGPD aux fins d'identification des personnes concernées en combinaison avec au moins un autre critère des lignes directrices du CEPD ;
3. Les opérations de traitement impliquant la combinaison, la correspondance ou la comparaison de données à caractère personnel collectées à partir d'opérations de traitement ayant des finalités différentes (provenant du même ou de différents responsables du traitement) - à condition qu'elles produisent des effets juridiques à l'égard de la personne physique ou aient une incidence significative et similaire sur la personne physique ;
4. Les opérations de traitement qui consistent en ou qui comprennent un contrôle régulier et systématique des activités des employés - à condition qu'elles puissent produire des effets juridiques à l'égard des employés ou les affecter de manière aussi significative ;
5. Les opérations de traitement de fichiers susceptibles de contenir des données à caractère personnel de l'ensemble de la population nationale, à condition qu'une telle DPIA n'ait pas déjà été réalisée dans le cadre d'une analyse d'impact générale dans le contexte de l'adoption de cette base juridique ;
6. Les opérations de traitement à des fins de recherche scientifique ou historique ou à des fins statistiques au sens des articles 63 à 65 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données ;
7. Les opérations de traitement qui consistent en un suivi systématique de la localisation de personnes physiques ;
8. Les opérations de traitement reposant sur la collecte indirecte de données à caractère personnel en conjonction avec au moins un autre critère des lignes directrices du CEPD lorsqu'il n'est ni possible / ni réalisable de garantir le droit à l'information





Les garanties suffisantes du sous-traitant

Afin que les exigences du règlement général sur la protection des données soient respectées dans le cadre d'un traitement réalisé par un sous-traitant pour le compte du responsable du traitement, lorsque ce dernier confie des activités de traitement à un sous- traitant, il ne devrait faire appel qu'à des sous-traitants présentant des garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux exigences du présent règlement, y compris en matière de sécurité du traitement.

Il convient de préciser que la nécessité de revoir les contrats de sous-traitance ainsi que les garanties suffisantes se présentent, en particulier, en cas de changement de prestataire.

En outre, l'application par un sous-traitant d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à démontrer le respect des obligations incombant au responsable du traitement.

Conservation et Archivages des données

- Conservation en base active

Il s'agit de la durée nécessaire à la réalisation de l'objectif (finalité du traitement) ayant justifié la collecte/enregistrement des données. Par exemple, dans une entreprise, les données d'un candidat non retenu seront conservées pendant 2 ans maximum (sauf s'il en demande l'effacement) par le service des ressources humaines.

En pratique, les données seront alors facilement accessibles dans l'environnement de travail immédiat pour les services opérationnels qui sont en charge de ce traitement (ex : le service des ressources humaines pour les opérations de recrutement) ;

- Archivage intermédiaire

Les données personnelles ne sont plus utilisées pour atteindre l'objectif fixé (« dossiers clos ») mais présentent encore un intérêt administratif pour l'organisme (ex : gestion d'un éventuel contentieux, etc.) ou doivent être conservées pour répondre à une obligation légale (par exemple, les données de facturation doivent être conservées dix ans en application du Code de commerce, même si la personne concernée n'est plus cliente). Les données peuvent alors être consultées de manière ponctuelle et motivée par des personnes spécifiquement habilitées ;

- Archivage définitif

En raison de leur « valeur » et intérêt, certaines informations sont archivées de manière définitive et pérenne.

À la différence de la conservation en base active, les deux dernières étapes ne sont pas systématiquement mises en place. Leur nécessité doit être évaluée pour chaque traitement, et, pour chacune de ces phases, un tri sera opéré entre les données.

LES RECLAMATIONS, QUI ? QUOI ? COMMENT ?

A qui adresser les réclamations ?

Les responsable de traitement doivent permettre à la personne concernée de savoir à qui elle doit adresser leur réclamations en vertu des droits prévus par le RGPD.

A cette fin, les entreprises doivent fournir les informations relatives à l'exercice des droits dans un langage simple et clair au moment même de la collecte des données ou, au plus tard, endéans un mois suivant la collecte.

En cas de traitement de données à caractère personnel, les informations suivantes doivent être communiquées par le responsable du traitement à la personne concernées :

- L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement;
- Le cas échéant, les coordonnées du délégué à la protection des données (DPO).

Les réclamations directes

Les personnes concernées par un traitement de données peuvent faire valoir leurs droits d'accès, d'effacement et de rectification à tout moment directement auprès du responsable du traitement dès la collecte, l'enregistrement, l'utilisation ou le traitement des données vous concernant.

Le renseignement demandé doit être obtenu gratuitement. Le responsable du traitement peut demander des informations supplémentaires nécessaires pour confirmer l'identité du réclamant, s'il a des doutes raisonnables quant à celle-ci.

Pour en savoir plus :

Sur le droit d'information

Les démarches préalables par le réclamant

L'article 4 de la procédure Réclamation de la CNPD prévoit :

« Si la demande a pour objet l'exercice des droits de la personne concernée lui conférés par les articles 12 à 22 du RGPD ainsi que par les articles 11 à 15 de laloi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et que le réclamant n'a pas cherché lui-même à exercer ses droits directement auprès du responsable du traitement en cause, la CNPD lui adresse un courrier électronique ou postal l'informant des démarches qu'il lui appartient d'engager, préalablement à toute saisine de la CNPD. »

Par conséquent, avant de faire une réclamation auprès de la CNPD, cette dernière invite les personnes concernées à effectuer une première démarche auprès du responsable de traitement pour faire respecter leurs droits (accès, rectification, effacement, portabilité…).

Pour en savoir plus :

Sur la procédure de réclamation

Réclamation auprès de la CNPD

Si la réclamation auprès du responsable du traitement est restée sans suite (ou si une telle réclamation s'avère difficile, voire impossible compte tenu des circonstances), la personne concernée peut s'adresser directement à la CNPD. Le traitement des réclamations émanant des personnes concernées compte parmi ses missions.

Celle-ci peut interdire un traitement de données en cas de non-respect de la loi. Elle peut aussi ordonner la suppression de données et saisir le procureur d'État. Des sanctions pourront être prononcées en cas d'infraction.

Il est vivement recommandé aux personnes concernées de soumettre la réclamation en utilisant le formulaire en ligne de la CNPD. L'utilisation de ce formulaire permettra un traitement accéléré de leur réclamation.

Le service Réclamations de la CNPD examine, au regard des textes légaux en matière de protection des données, si la CNPD est matériellement et territorialement compétente pour traiter la réclamation.

Au cours de la procédure de réclamation, la CNPD examine si une réclamation est justifiée, c'est-à-dire qu'elle vérifie si les faits allégués par le réclamant relatifs à un traitement de données à caractère personnel sont susceptibles de constituer ou non une violation de la législation applicable en matière de protection des données. Lorsque la CNPD estime que le traitement de données litigieux serait effectivement contraire à la législation, elle s'efforcera de remédier à la situation sans avoir à recourir à des mesures contraignantes dont elle dispose dans le cadre de ses pouvoirs lui conférés par la loi.

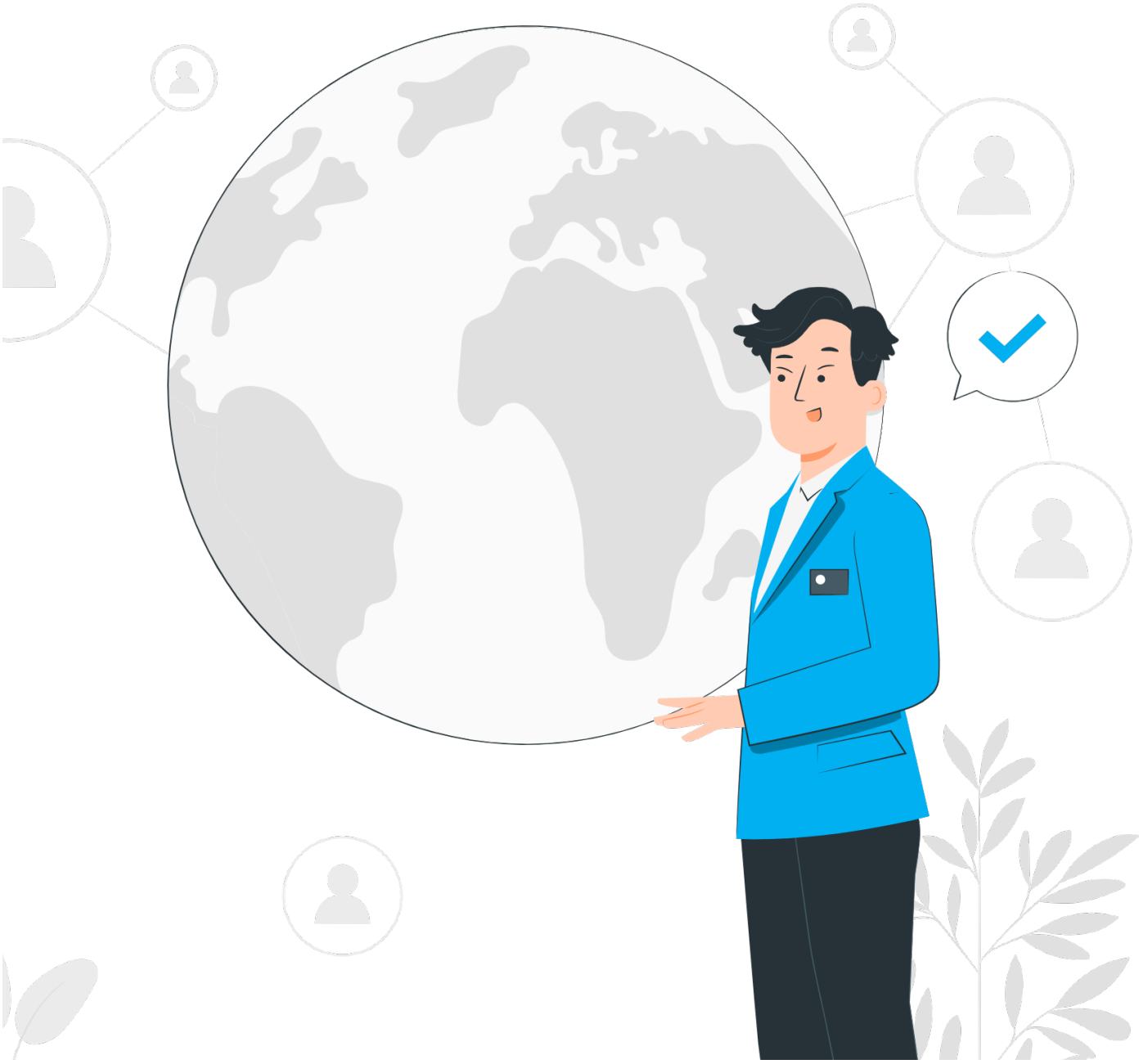
Le Guichet Unique

(réclamations européenne)

Sous le RGPD, les autorités de contrôle ont le devoir de coopérer dans les affaires ayant une composante transfrontalière afin de garantir une application cohérente du RGPD. Dans le cadre de ce mécanisme du “guichet unique” (en anglais “OSS” ou “One-Stop- Shop mecanism”), l’autorité de contrôle chef de file est en charge de préparer les projets de décision et travaille avec les autres autorités de contrôle concernées pour parvenir à un consensus.

Pour en savoir plus :

Site de la CNPD



NOUVEAUX TRAITEMENT, AYEZ LES BONS REFLEXES !

LES MESURES CORRECTRICES

Chaque autorité de contrôle (dont la CNPD) dispose du pouvoir d'adopter toutes les mesures correctrices suivantes:

a) avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement;

b) rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement;

c) ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement;

d) ordonner au responsable du traitement ou au sous- traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé;

e) ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel;

f) imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;

g) ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19;

h) retirer une certification ou ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites;

I) imposer une amende administrative en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas;

j) ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

Source : art. 58.2 RGPD

TRAITER LES PHOTOS DANS LE RESPECT DES LOIS APPLICABLES !

Base légale au sens de l'article 6 RGPD

La plupart du temps, le traitement de photos sera fondé sur le consentement de la personne concernée. Le consentement doit être « libre, spécifique, éclairé et univoque » de celui-ci. La personne concernée doit donc avoir un véritable choix. Pour les mineurs, les représentants légaux doivent donner leur consentement.

Le traitement de photos peut également être basé sur des autres conditions de licéité (par exemple : intérêt public, exécution d'un contrat).

Par exemple, un photographe peut se baser sur la condition de licéité relative à l'exécution d'un contrat quand il prend des photos d'identité ou quand il est engagé pour un photo shooting.

Les autorités publiques peuvent invoquer l'intérêt public ou l'intérêt vital de la personne concernée quand elles publient les photos, comme par exemple de personnes disparues.

Les autres lois applicables

Le "droit à l'image" n'est pas réglé seulement par le RGPD mais par une série d'autre lois et par la jurisprudence :

- Art. 8, 10, 17 Convention Européenne des Droits de l'Homme
- Art. 7, 8, 54 Charte des Droits de l'Homme
- Art. 16 Traité Fonctionnel de l'Union Européenne
- Art. 6, 85 RGPD
- Art. 11(3), 24 Constitution luxembourgeoise
- Loi du 11 août 1982 concernant la protection de la vie privée
- Loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias
- Loi modifiée du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données
- Loi modifiée du 10 août 1992 relative à la protection de la jeunesse (mineurs : art. 38)
- Art. 383, 383bis, 385 Code pénal
- Art. 1382 et s. C. civ. / action en cessation
- La jurisprudence : Il est de jurisprudence constante que « toute personne a sur son image et l'utilisation qui en est faite un droit exclusif et peut s'opposer à une diffusion non autorisée par elle ». Ainsi, il a été jugé que « le droit de l'homme sur son image privée est total et que chacun peut s'opposer à la publication de ses traits sans autorisation ».

La jurisprudence en la matière retient qu'une personne qui donne son consentement pour la prise de photos ne le donne pas nécessairement pour la publication ou la diffusion. Il y a donc lieu de collecter un double consentement.

Pour en savoir plus :

Guidance de la CNPD