DECLARATION

20/11/2019

AU 52
Biométrie : Contrôle d’accès sur les lieux de travail avec maîtrise de la personne sur son gabarit

BIOMÉTRIE : CONTRÔLE D'ACCÈS SUR LES LIEUX DE TRAVAIL AVEC MAÎTRISE DE LA PERSONNE SUR SON GABARIT

(Déclaration N° 52)

Suite à l'entrée en application du RGPD, les autorisations uniques adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

L'autorisation unique n°AU-052 concerne les dispositifs biométriques mis en œuvre pour contrôler l'accès aux locaux, appareils et applications informatiques utilisés sur les lieux de travail. Ces dispositifs doivent garantir à la personne concernée de garder la maîtrise de son gabarit. Cela suppose de stocker le gabarit biométrique

- sur un support détenu par la seule personne concernée
- ou en base de données sous une forme inexploitable car illisible sans un secret détenu par la seule personne concernée.

Ces systèmes intègrent donc par défaut des mécanismes permettant de respecter la vie privée des personnes. Ils doivent être privilégiés lorsqu'un contrôle d'accès biométrique est mis en place dans un contexte professionnel.

L'AU-052 abroge et remplace les autorisations uniques adoptées par la CNIL en matière de biométrie :

- l'AU-027 (Contrôle d'accès par empreinte digitale aux ordinateurs portables professionnels)
- l'AU-019 (Réseau veineux de la main sur les lieux de travail)
- l'AU-008 (Empreinte digitale sur le lieu de travail)
- l'AU-007 (Contrôle d'accès par contour de la main aux lieux de travail).

Les organismes ayant effectué un engagement de conformité à ces autorisations uniques et qui ne respectent plus les conditions fixées par la présente norme disposent d'un délai de deux ans à compter de son adoption pour se mettre en conformité et effectuer un nouvel engagement de conformité, ou demander une autorisation spécifique auprès de la Commission.

TEXTE OFFICIEL

Délibération n° 2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise de la personn

RESPONSABLES DE TRAITEMENT CONCERNES

- Tout organisme privé (exception : établissement accueillant des mineurs) ;
- Les organismes publics, sauf l'Etat et les établissements accueillant des mineurs.

OBJECTIF(S) POURSUIVI(S) PAR LE TRAITEMENT (FINALITES)

- le contrôle des accès à l'entrée et dans les locaux limitativement identifiés par l'organisme comme devant faire l'objet d'une restriction de circulation, à l'exclusion de tout contrôle des horaires des employés ;
- le contrôle des accès à des appareils et applications informatiques professionnels limitativement identifiés de l'organisme, à l'exclusion de tout contrôle du temps de travail de l'utilisateur.

FINALITES EXCLUES DU CHAMP DE LA NORME

Le contrôle des horaires, l'authentification biométrique proposée en dehors de tout contexte professionnel

DONNEES PERSONNELLES CONCERNEES

Les données concernent toute personne spécifiquement habilitées par le responsable du traitement à accéder aux locaux, appareils ou applications informatiques protégées par le contrôle d'accès biométrique.

Elles portent sur :

- **l'identité** : nom, prénom, photographie et gabarit de la caractéristique biométrique, clé biométrique résultat du traitement des mesures par un algorithme (et non une image ou une photographie de cette caractéristique), numéro d'authentification ou numéro de support individuel, coordonnées ;
- **la vie professionnelle :** numéro de matricule interne, corps ou service d'appartenance, grade, nom de l'employeur ;
- **le déplacement des personnes :** porte utilisée, zones et plage horaire d'accès autorisées, date et heure d'entrée et de sortie ;
- **en cas d'accès à un parking** : numéro d'immatriculation du véhicule, numéro de place de stationnement ;

Les caractéristiques biométriques sont conservées sous la forme d'un gabarit chiffré ne permettant pas de recalculer la donnée biométrique d'origine.

Le gabarit doit être conservé sur un support individuel de stockage détenu par la seule personne concernée.

S'il n'est pas possible de confier des supports de stockage individuels aux personnes concernées, le responsable du traitement peut conserver le gabarit en base de données ou dans la mémoire interne du terminal de lecture comparaison :

- en justifiant cette impossibilité ;
- en conservant les gabarits biométriques que sous forme chiffrée par une clé de chiffrement/déchiffrement uniquement détenue par la personne concernée.

DUREE DE CONSERVATION DES DONNEES

- Le gabarit biométrique ne peut être conservé que le temps de l'habilitation de la personne concernée et doit être supprimé à son départ.
- Les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservées cinq ans après le départ de la personne disposant d'une habilitation d'accès de longue durée, et 3 mois après le départ des personnes disposant d'une habilitation d'accès ponctuelle.
- Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de 3 mois.

DESTINATAIRES DES DONNEES

- **Les personnes habilitées du service du personnel peuvent avoir connaissance des données suivantes :** identité (à l'exception du gabarit de la biométrie utilisé et du code d'authentification), vie professionnelle, déplacement des personnes et informations en relation avec la gestion du parking.
- **Les personnes habilitées du service gérant la sécurité des locaux données peuvent avoir connaissance des données suivantes : i**dentité (à l'exception du gabarit de la biométrie utilisée et du code d'authentification), plages horaires autorisées, déplacement des personnes, vie professionnelle et informations en relation avec la gestion du parking ou des locaux.
- **Les personnes habilitées du service ou de l'organisme gérant le restaurant d'entreprise ou administratif peuvent avoir connaissance des données suivantes :** identité (à l'exception du gabarit du contour l'organisme gérant le restaurant d'entreprise de la main et du code d'authentification) et informations en relation avec la gestion de la restauration.

Toutes ces personnes ne peuvent avoir accès au gabarit de l'empreinte digitale que de façon temporaire et pour les stricts besoins de l'enrôlement de la personne concernée ou de la suppression du gabarit. Il leur est impossible d'accéder directement, de modifier, ou de copier sur un autre support, les gabarits enregistrés.

INFORMATION DES PERSONNES ET RESPECT DES DROITS "INFORMATIQUE ET LIBERTES"

Lors de la collecte des données, le responsable du traitement doit informer les personnes :

- de son identité,
- de la finalité du traitement,
- du caractère obligatoire ou facultatif des informations qu'il collecte,
- des destinataires de ces informations,
- de l'existence de droits pour les personnes fichées et du service auprès duquel les faire valoir,
- des transmissions envisagées.

Préalablement à la mise en place du dispositif de contrôle d'accès, les instances représentatives du personnel sont informées et consultées.

L'information préalable des employés est effectuée par remise d'une notice explicative. Elle précise notamment la manière d'exercer les droits d'accès, de rectification et d'opposition pour motif légitime.

SECURITE ET CONFIDENTIALITE

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées et notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

Ces mesures doivent porter sur les données (chiffrer et cloisonner les données lors de leurs transmissions, y associer un code d'intégrité, la supprimer en cas d'accès non autorisé, etc.), sur l'organisation du responsable du traitement (formation des personnes habilitées à utiliser les matériels, mise en place d'un dispositif de secours, test du dispositif, informer les personnes concernées en cas d'accès non autorisé à leurs données, etc.), sur les matériels (traçabilité du cycle de vie du matériel, matériel dédié, etc.), sur les logiciels utilisés pour effectuer la comparaison (mise à jour, détection de logiciels malveillants, etc.), et sur les canaux informatiques.