Le Règlement Général de Protection des Données

Règlement européen : Faut-il encore effectuer des déclarations à la CNIL ? **NON**.

Le système de biométrie mesure certaines caractéristiques morphologiques de la personne à enregistrer : la forme et la taille de sa main, son empreinte digitale ou sa reconnaissance faciale ou son réseau veineux de la paume de la main ... Ces mesures mémorisées sont appelées des gabarits.

Description des gabarits	Finalités du traitement
Le gabarit de type 1 Maîtrise exclusive par la personne	- Le seul à détenir le gabarit est l'utilisateur, ces données biométriques sont stockées dans un badge ou carte à puce. - Pour valider son droit d'accès, il s'identifie à la fois par son badge et ces caractéristiques biométriques concernés, par exemple son empreinte digitale … - Aucune base de données centralisée du gabarit.
Le gabarit de type 2* Maîtrise partagée	- Les gabarits sont stockés dans une base de données collective, mais les données sont cryptées. - Elles ne pourront être lues que sur intervention du salarié concerné, via la présentation d'un badge ou le renseignement d'un mot de passe.
Le gabarit de type 3 Maîtrise exclusive par l'employeur	- Les gabarits de tous les utilisateurs sont contenus dans une base centralisée, et l'utilisateur n'a pas à présenter de badge ou de code d'accès pour s'authentifier. - L'utilisateur doit seulement présenter sa caractéristique biométrique (morphologie de la main, empreinte digitale, reconnaissance faciale, réseau veineux de la main).

Le logiciel BiomAccess3 et la mise en conformité au RGPD

La mise en place d'un logiciel de contrôle d'accès ne garantit pas la conformité au RGPD mais constitue une aide à la mise en œuvre d'une bonne gestion des données personnelles, afin d'adopter au minimum les mesures suivantes ou des mesures dont il démontre l'équivalence :

- Cloisonner les données lors de leur transmission et leur conservation.
Zalix : Aucune donnée n'est accessible par tous au logiciel BiomAccess3.

- Chiffrer les données biométriques, dont les gabarits, à l'aide d'un algorithme cryptographique.
Zalix : Les données biométriques sont cryptées selon un algorithme qui est propre à chaque constructeur de lecteur et à chaque technologie.

- Associer un code d'intégrité aux données (par exemple, signature ou hachage).
Zalix : le cryptage des données, la manière de contrôler l'intégrité des données est propre à chaque constructeur de lecteur. Zalix rajoute un contrôle d'intégrité des données biométriques, afin d'éviter leurs substitutions. **

- Intégrer une mesure technique ou organisationnelle de détection de fraude (ex : mesure de détection de faux doigts).
Zalix : Les terminaux à empreinte digitale (V2) répondent à ces exigences à la reconnaissance des doigts vivants.

- Interdire tout accès externe à la donnée biométrique.
Zalix : L'accès aux données se fait uniquement par l'intermédiaire du logiciel BiomAccess3.

- Effectuer le contrôle d'accès par une comparaison entre l'échantillon calculé et le gabarit d'enrôlement enregistré.
Zalix : On compare un gabarit enregistré et stocké (carte, base de données) avec le gabarit capturé au moment de l'accès, on n'enregistre alors aucun gabarit (gabarit 1).

- Interdire la transmission de tout gabarit stocké.
Zalix : L'utilisation des données gabarits biométriques reste confinée au système BiomAccess3 pour laquelle elle a été prévue, en d'autres termes, les données biométriques ne sortent pas de ce cadre-là et ne peuvent être communiquées en dehors de celui-ci.

- Veiller à l'effectivité de l'effacement des données à l'issue de la durée de conservation.
Zalix : Cette procédure est automatique et programmable, par exemple, 6 mois à compter de la fin de la relation contractuelle.

- Supprimer la donnée biométrique en cas d'accès non autorisé au terminal de lecture-comparaison ou au serveur distant.
Zalix : Oui, l'option se fait de manière logicielle par l'intermédiaire de la remontée des évènements. ***

- Supprimer toute donnée non utile au traitement ultérieur lors de la fin de vie du dispositif biométrique.
Zalix : En «fin de vie» ou lors de tout remplacement des terminaux (V2), les données stockées sur les lecteurs sont supprimées et les paramètres réinitialisés (dispositif anti-arrachement).
Client : Ajouter procédure pour fin de vie pour tout client de devoir effacer le contenu du lecteur.

Les Terminaux De Technologie Biométrique

- Nous, ZALIX BIOMETRIE, certifions que les terminaux à empreinte digitale (V2), reconnaissance faciale (V2) et réseau veineux de la paume de la main** que nous commercialisons extraient minutieusement les points de données des gabarits et créent un modèle à partir de ces données et ne conserve pas l'image brute du gabarit dans le périphérique ou le serveur.
- Les modèles peuvent être de différents types : «ISO 19794-2 : 2005, ANSI-378 (les deux étant des normes internationales).
- Afin de sécuriser la protection des modèles, des outils cryptographiques et des méthodes de cryptage sont utilisés, tels que l'AES 128 bits ou AES 256 bits (sur le serveur), ce qui rend inaccessible à l'accès aux données biométriques.
- La communication TCP (Transmission Control Protocol) entre les périphériques et le serveur central peut être définie comme « Communication sécurisée » avec l'utilisation de TLS 1.2 (y compris SSL / HTTPS).

Les fichiers relatifs à ces dispositifs n'ayant plus à être déclarés à la CNIL depuis le 25 mai 2018, date d'entrée en application du RGPD, pour vous conformer aux règles de protection des données personnelles, vous devez :

- Demander conseil et assistance à votre Délégué à la protection des données (DPO) si vous en avez un.
- Effectuer une analyse d'impact sur la protection des données (PIA).
- Inscrire votre fichier dans le Registre des activités de traitement tenu par votre société.
- Informer vos clients des conditions dans lesquelles vous traitez leurs données.
- Prévoir des mesures de sécurité adaptées au regard des risques.

Conformément aux dispositions de délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la 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.
https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf

*Pas disponible actuellement. **En cours. *** option à venir pour les lecteurs le permettant.