Guide pratique

# Les EPI connectés

©T2S

SYNAMAP

Syndicat national des acteurs du marché de la prévention et de la protection

## 1. Définition d'un EPI connecté

Un EPI est un "Equipement de Protection Individuelle" visant à protéger une personne contre un ou plusieurs risques susceptibles de menacer sa santé ou sa sécurité sur son lieu de travail, lorsque la protection collective ne suffit pas.

Les EPI sont classés en trois catégories :
- Catégorie 1 : protection contre les risques mineurs
- Catégorie 2 : protection contre les risques majeurs
- Catégorie 3 : protection contre les risques irréversibles ou mortels.

**Un EPI connecté** est un équipement de protection individuelle qui est capable de communiquer avec son environnement ou un autre équipement. Certains peuvent être dotés d'un système capable de collecter des données à l'aide de capteurs afin de prévenir l'utilisateur d'un danger ou d'alerter en cas d'accident.
Le principe des EPI connectés repose sur l'intégration :
- de capteurs,
- de systèmes de géolocalisation,
- de dispositifs de communication et autres fonctionnalités intelligentes.

Ces technologies permettent de recueillir des informations pour améliorer la protection des travailleurs (surveillance en temps réel de l'environnement de travail, alerte instantanée en cas de danger, etc.) ou permettre d'augmenter la sécurité de la personne en la rendant active (LEDS par exemple).

Les EPI connectés peuvent faciliter également la communication entre les travailleurs et leur équipe de supervision ou de secours avec une connexion instantanée pour signaler un problème, demander de l'aide ou recevoir des instructions en temps réel.

***A ne pas confondre avec un EPI intelligent !*** *Celui-ci étant un équipement de protection individuelle auquel on a ajouté un composant électronique, un nouveau matériau, ou tout autre élément qui apporte une valeur ajoutée en prévention et en protection.*

## 2. Rappel réglementaire

Un EPI connecté doit protéger avant tout son porteur et respecter les exigences essentielles du règlement UE 2016/425 qui précise qu'un "EPI est un équipement conçu et fabriqué pour être porté ou tenu par une personne en vue de la protéger contre un ou plusieurs risques pour sa santé ou sa sécurité".
Cet équipement doit donc comporter le marquage CE et répondre aux normes en vigueur en tant qu'EPI. Son composant électronique doit également apposer le marquage CE qui indique que les produits sont fabriqués conformément à toutes les directives et règlements applicables.

Les caractéristiques propres à l'EPI sont toujours prioritaires :
- La solution électronique ne doit pas dégrader l'EPI.
- Un équipement dont le système électronique ne fonctionne pas est toujours considéré comme un EPI puisque ses caractéristiques de protection sont intactes

## 3. Maintenance et entretien

### 3.1 – Article neuf

Lors de la remise de l'EPI connecté, il faut s'assurer que sont présentes ;
- La notice de l'EPI certifié (cf règlement 2016/425).
- La notice de la partie connectée qui précise les instructions sur les éléments connectés amovibles ou fixes.
Le manuel d'utilisation de la partie connectée explicitera les niveaux de responsabilité de l'employeur et de l'utilisateur (ex : bonne utilisation et maintenant de la partie connectée – comme la recharge).

Avant toute première mise en circulation d'un EPI connecté, l'utilisateur pourra utiliser une procédure de mise en route de la partie connectée pour s'assurer de sa conformité. Cette procédure est mise à disposition par le fournisseur.
Le fabriquant veillera à informer et former les utilisateurs et mettra, par la suite, les consignes à disposition.

### 3.2 – Maintenance et entretien

#### A - Maintenance et entretien de la partie textile

Concernant la partie vêtement, les conditions d'entretiens sont indiquées sur les étiquettes présentes sur le vêtement et sur la notice d'utilisation remise avec le vêtement.

***Partie 1 – Les obligations des employeurs et prestataires***

L'employeur et le prestataire chargés d'entretenir le vêtement EPI doivent s'assurer de plusieurs points lors de l'entretien, selon le Règlement 2016/425, pour la partie textile non-connectée :

Les obligations de l'employeur sont les suivantes :

- Fournir des instructions d'entretien : L'employeur est généralement tenu de fournir des instructions d'entretien appropriées pour chaque type d'EPI utilisé dans l'environnement de travail. Ces instructions sont fournies par le fabricant.

- Veiller à la conformité : L'employeur doit s'assurer que les EPI sont entretenus conformément aux spécifications du fabricant et aux normes applicables.

- Évaluer les risques : L'employeur doit évaluer les risques liés à l'utilisation des EPI et déterminer la fréquence et la nature de l'entretien en fonction de ces évaluations.

- Formation des travailleurs : L'employeur doit former les travailleurs sur l'importance de l'entretien des EPI, sur la manière de les entretenir correctement, et sur la reconnaissance des signes d'usures ou de défaillances.

Les EPI peuvent être entretenus par un prestataire qui doit vérifier les points suivants :

- Conformité aux spécifications du fabricant : Le prestataire en charge de l'entretien doit suivre les spécifications du fabricant pour l'entretien des EPI connectés et est responsable de la conformité de la partie non-connectée. Il est aussi responsable de la partie connectée présente à demeure sur le vêtement (pax exemple leds, fils de connexion…).

- Documentation adéquate : Il est essentiel que le prestataire en charge de l'entretien s'assure de suivre un protocole conforme aux spécifications du fabricant.

- Formation du personnel : Le personnel chargé de l'entretien doit être formé, avoir à disposition des instructions permettant un entretien approprié des EPI, et également des EPI connectés.

***Partie 2 – Déterminer que la partie connectée est fonctionnelle***

Guide sur la conformité de la partie connectée de l'EPI après entretien :

- Vérifier que les instructions de lavage sont fournies avec les spécifications concernant la partie connectée-hardware (éléments compatibles avec le lavage, retirer les parties non-lavables…).

- Définir le process de prélèvement, entretien et remise à disposition de l'EPI connectés, notamment la gestion des éléments connectés amovibles et non-lavables, avec l'éventuel prestataire d'entretien retenu et les obligations du porteur pour la partie connectée amovible.

- S'assurer des procédures de vérification de la conformité/ bon fonctionnement des EPI connectés après entretien. Définir le responsable de cette vérification (interne à l'entreprise ou éventuel prestataire d'entretien).

Guide sur la conformité des EPI connectés soumis à un protocole de réparation :

- S'assurer de la mise à disposition du protocole de réparation fourni par le fabricant pour la partie EPI soumise au règlement 2016/425 (cf guides du SYNAMAP) et qui n'engendre pas un disfonctionnement de la partie connectée. Préciser les actes de réparations qui pourraient avoir un impact sur la partie connectée.

- En cas de défaillance de la partie connectée (hardware), amovibles ou non-amovibles, s'assurer de la mise à disposition du protocole de réparation proposé par le fabricant et qui n'altère pas les propriétés de protection de l'EPI connecté. La réparation pourra être réalisée par le fabricant ou sous-traitée au prestataire d'entretien, si accord avec ce dernier.

- En cas de défaillance du software, vérifier les dispositions prises par le fabricant pour assurer la continuité de service et que cette dernière n'altère par les propriétés de protection de l'EPI.

- S'assurer des procédures de vérification de la conformité / bon fonctionnement des EPI connectés après réparation. Définir le responsable de cette vérification (interne ou éventuel prestataire d'entretien).

©ROSTAING

## B - Maintenance de la partie hardware

La partie Hardware désigne le matériel et les composants physiques de l'EPI connecté. Il peut s'agir de fils, de leds, de capteurs, d'un boîtier de commande simple ou d'un élément communicant intégrant une batterie, une mémoire de stockage, une carte électronique, des puces communicantes…

### *Partie 1 – Liste d'obligations, règlementations*

Pour mettre son article sur le marché, il est nécessaire que le fabricant réponde aux obligations suivantes :

- Conformité CE : Le fabricant doit déclarer la conformité de son produit avec les exigences essentielles des directives et règlements européens applicables et apposer le marquage CE. Cela s'applique à diverses directives, notamment la directive EMC (Compatibilité électromagnétique), la directive LVD (Basse tension), et d'autres pertinentes pour le produit.

- Directive RoHS (Restriction of Hazardous Substances) : Le produit doit être conforme à la directive RoHS, qui limite l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques.

- Directive RED (Equipements hertziens et équipements terminaux de télécommunications) : Si le produit intègre des technologies sans fil, comme le Bluetooth, il doit être conforme à la directive RED. Cela inclut la conformité aux normes harmonisées et la déclaration de conformité.

- Directive Batteries : Si le produit intègre une batterie, il doit être conforme à la directive relative aux piles et accumulateurs et aux déchets de piles et d'accumulateurs. Cela concerne la sécurité des piles et l'impact environnemental de leur élimination.

- Directive WEEE (Waste Electrical and Electronic Equipment) : La directive WEEE concerne la gestion des déchets électriques et électroniques. Le fabricant peut avoir des responsabilités en matière de collecte, de traitement et de recyclage des déchets générés par son produit.

- Normes harmonisées et conformité technique : Le fabricant doit souvent se conformer à des normes spécifiques liées à son produit. Les normes harmonisées fournissent des spécifications techniques pour faciliter la conformité. La documentation technique doit être préparée et conservée pour démontrer la conformité.

- Étiquetage et documentation : Le fabricant doit fournir des informations d'étiquetage et une documentation appropriée accompagnant le produit. Cela peut inclure des manuels d'utilisation, des avertissements de sécurité, etc.

- Responsabilité du fabricant : Le fabricant assume la responsabilité totale de la conformité de son produit. Cela inclut la documentation technique, la surveillance du marché, et la gestion des mises à jour si nécessaire.

### *Partie 2 – Vérification des éléments fournis avec l'EPI*

- Présence du marquage CE, respect de la réglementation de mise sur le marché en vigueur sur tous les sous-ensembles du produit (équipements connectés amovibles ou fixes).

- Présence de la documentation technique avec les manuels d'utilisations, les avertissements de sécurité, les protocoles de réparation autorisée…

- Présence des éléments permettant le bon fonctionnement de l'équipement (chargeur, piles, moyen de communication par exemple).

- Information en cas de défaillance et remplacement de l'équipement pour assurer la continuité de service de l'élément connecté.

- S'assurer qu'en cas de défaillance de la partie hardware, l'EPI connecté pourra toujours assurer la protection du porteur pour les risques identifiés selon le Règlement UE 2016/425.

- Information sur la gestion des mises à jour.

- Information sur un possible contrôle régulier de l'état du matériel et de sa pérennité de fonctionnement.


### C - Maintenance de la partie software

Guide pour la partie applicative (software ou application mobile) de la solution EPI connectée :

- S'assurer d'un contrat de mise à jour de la partie software.

- S'assurer qu'en cas de défaillance de la partie software, l'EPI connecté pourra toujours assurer la protection du porteur pour les risques identifiés selon le Règlement UE 2016/425.

- Information et formation des utilisateurs lorsqu'une mise à jour majeure (ajout d'une fonctionnalité par exemple) a été effectuée dans les plus brefs délais (à définir avec le fabricant).

## 3.3 – La réforme des EPI connectés

Un EPI connecté en fin de vie doit être réformé et ne peut plus être remis en circulation. Il est important de noter que c'est l'état de l'EPI qui protège le porteur, à savoir la partie non-connectée établie selon le Règlement UE 2016/425, qui doit être prise en considération en premier. La priorité est d'assurer la sécurité des travailleurs en veillant à ce que les EPI connectés soient en bon état de fonctionnement au moment de leur utilisation. Divers facteurs peuvent être pris en compte pour évaluer la réforme ou le remplacement d'un EPI comme son état, les recommandations du fabricant, les résultats des inspections pendant son utilisation ou après entretien, les résultats des évaluations des risques…

## A - Cas d'usage où le vêtement doit être réformé

Voici quelques indications (liste non-exhaustive) indiquant le moment où un EPI devrait être réformé selon le Règlement UE 2016/425 :

- Usure ou dommages visibles sur tous les EPI qui sont exclus du protocole de réparation : lorsqu'un EPI présente des signes évidents d'usure, de dégradation ou de dommages qui ne peuvent être réparés selon le protocole donné par le fabricant, il doit être retiré de l'utilisation et réformé. La partie connectée amovible peut être potentiellement réutilisée sur un autre EPI connecté selon les préconisations du fabricant.

- Usure ou dommages visibles de la partie connectée non-amovibles qui peut entraîner une altération de la fonction protection assurée par l'EPI par rapport aux risques identifiés et qui ne peut être réparée ou changée.

- Fin de la durée de vie utile : Certains EPI ont une durée de vie utile spécifiée par le fabricant. Si cette durée de vie est atteinte, l'EPI doit être réformé, même s'il ne montre pas de signes évidents de dommages.

- Changements dans les conditions d'utilisation : Si les conditions d'utilisation de l'EPI changent de manière significative, par exemple, si l'entreprise évalue des risques plus importants que ceux pour lesquels l'EPI est prévu, il peut être nécessaire de le réévaluer et éventuellement de le remplacer par un équipement plus approprié.

- Résultats d'inspections régulières (pendant son utilisation ou après entretien) : Les inspections régulières doivent être effectuées conformément aux instructions du fabricant et aux exigences réglementaires. Si une inspection révèle des problèmes ou des signes de défaillance potentielle, l'EPI doit être réformé.

- Changements dans la réglementation : Si des modifications réglementaires sont apportées, il peut être nécessaire de mettre à jour ou de remplacer les EPI pour garantir la conformité aux nouvelles exigences.

- Recommandations du fabricant : Les fabricants peuvent fournir des recommandations spécifiques sur le moment où un EPI doit être réformé. Il est important de suivre ces recommandations.

©ANSELL

## B - Réutilisation de la partie connectée suite à la réforme de l'EPI

Certains EPI sont réformés après un certain nombre de lavage, durée prédéterminée (durée de vie donnée par le fabricant) ou suite à une non-conformité de la partie EPI « vêtement ». Cependant La partie «connectée» peut être encore fonctionnelle.

Guide pour déterminer le devenir de la partie connectée encore fonctionnelle :

- Définir dans le cadre d'un EPI connecté mis en réforme, comment se passe le recyclage ou la réutilisation de la partie connectée si encore fonctionnelle.

- Définir dans le cadre d'une réutilisation de la partie connectée, quelle est la procédure pour s'assurer de la conformité de la partie connectée.

- S'assurer de la mise à disposition d'une procédure de formation ou d'une documentation suite à la réutilisation de la partie connectée.

## C - Traitement des EPI connectés en fin de vie

Informations sur les conditions de réforme :

- De la partie EPI présente sur la notice d'utilisation.

- De la partie connectée présente sur le manuel d'utilisation.

- Information sur le circuit préconisé pour la gestion des EPI connectés en fin de vie (gestion de la partie textile et de la partie électronique).

- Partie textile avec éléments non-amovibles.

- Partie électronique amovibles.

- Déchets d'équipements électriques et électroniques (DEEE).

## 4. Sécurité des données

**BON A SAVOIR**
Les notions de cybersécurité et RGPD doivent être mentionnées dans les CGV du fabricant et mises à la disposition des clients.

### 4.1 – PIA (Privacy Impact Assessment)

**L'Etude d'Impact sur la vie privée ou PIA** *(Privacy Impact Assessment)* est une obligation introduite par le règlement européen 2016/679 (RGPD) du 27 avril 2016, relatif à la protection des données à caractère personnel.
Il s'agit d'un document clé dans le cadre de la gestion **des risques liés au traitement des données à caractère personnel**.
Une Etude d'Impact est requise lorsqu'il existe un risque élevé pour les personnes concernées, par exemple, lorsqu'un traitement concerne des personnes dites "vulnérables" ou implique des **données sensibles**.
L'étude d'impact sur la vie privée s'inscrit dans une logique **de responsabilisation des acteurs**. Il s'agit également d'un **vecteur de confiance** dans la relation des acteurs à leurs partenaires et à leurs clients.

Le PIA permet de justifier, à tout moment, les grands principes de la règlementation informatique et libertés :

- Licéité, loyauté transparence
- Limitation des finalités
- Minimisation des données
- Exactitude
- Limitation de la conservation
- Intégrité et confidentialité des données.

Il s'agit d'une **analyse de mesures juridiques mais également de solutions techniques (sécurité physique et logique)** permettant de traiter des données personnelles (pseudonymisation, minimisation, chiffrement, éloignement des sources de risques…).

Les responsables de traitement et leurs sous-traitants doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut.

Le responsable de traitement doit effectuer une Etude d'Impact lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer **un risque élevé pour les droits et libertés des personnes physiques**.

Cette obligation est renforcée lorsque le responsable de traitement procède à **l'évaluation systématique et approfondie d'aspects personnels** concernant des personnes physiques, qui est fondée sur un **traitement automatisé**, y compris **le profilage**, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire.

Pour mieux prendre en compte l'évolution de l'économie numérique, le règlement européen a défini **la notion de profilage**, il s'agit de "*toute forme de **traitement automatisé** de données à caractère personnel consistant à utiliser ces 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, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique*."

Le PIA permet d'identifier les risques Privacy, d'analyser les écarts pour être en règle au RGPD et de mettre un plan d'action pour sécuriser les données personnelles.

## 4.2 – Cybersécurité

État d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace.
La cybersécurité est assurée par la cyberprotection et, dans le cas d'un Etat, par la cyberdéfense.

C'est l'ensemble des technologies, processus et pratiques visant à protéger les réseaux, les appareils, les programmes informatiques ou les données contre les cyberattaques.
On parle aussi parfois de sécurité informatique. Le but est de préserver l'intégrité, la confidentialité et la disponibilité des systèmes et réseaux informatiques et des données qu'ils renferment.
Pour une entreprise, l'objectif principal est de protéger sa propriété intellectuelle contre les menaces internes et externes.

## 4.3 – EPI connecté et les différents niveaux de cybersécurité

- Sécurité de réseau : protéger un réseau informatique contre les intrus, y compris les connexions filaires et sans fil (Wi-Fi).
Comme l'EPI connecté en temps différé qui stocke des données et si nécessaire pourra les transférer (via un ordinateur ou sans fil par Wi-Fi, GSM...)
Exemple : un gilet de signalisation avec un système anticollision.

- Sécurité des applications : protéger les applications fonctionnant sur site et dans le cloud.
La sécurité doit être intégrée aux applications dès leur conception, en tenant compte de la manière dont les données sont traitées, de l'authentification des utilisateurs... Comme l'EPI connecté en temps réel, qui doit obligatoirement transmettre & recevoir pour fonctionner via Wi-Fi, GSM...
Exemple : des lunettes de protection en réalité augmentée.

- Sécurité du cloud : les données du cloud au repos (dans le stockage), en mouvement (lorsqu'elles se déplacent vers, à partir et dans le cloud) et en cours d'utilisation (pendant le traitement) pour le respect de la confidentialité des informations des clients, des exigences commerciales et des normes de conformité aux réglementations.
Exemple : tous les EPI connectés sont concernés.

La cybersécurité passera aussi par :

- La formation des administrateurs et des utilisateurs : Sensibilisation de l'ensemble de l'organisation à la sécurité, afin de renforcer la sécurité des points de terminaison.
Exemple : supprimer les pièces jointes suspectes des courriers, éviter d'utiliser des périphériques USB inconnus...

- La sécurité des informations : RGPD.

- La planification de la reprise après sinistre/de la continuité des opérations : Outils et procédures permettant de réagir à des événements imprévus, tels que des catastrophes naturelles, des pannes de courant ou des incidents de cybersécurité, en perturbant le moins possible les opérations essentielles.

- La sécurité du stockage : par le chiffrement et les copies de données inaltérables et isolées.
Elles demeurent dans le même pool afin de pouvoir être rapidement restaurées pour soutenir la reprise, réduisant ainsi l'impact d'une cyberattaque. Le haut niveau de sécurité du datacenter qui abrite les données primordiales. Un centre de données doit être sécurisé à tous les niveaux : normes de sécurité, certifications, accès aux bâtiments restreints...

- La sécurité mobile : gérer et sécuriser le personnel mobile itinérant.

Dans le cadre des EPI, il existe aussi des EPI non connectés avec un fonctionnement autonome et sans lien avec l'informatique
Exemple : une paire de talkie-walkie avec la fonction Protection du Travailleur Isolé.

L'ensemble des points ci-dessus, sont applicables si vous êtes propriétaire ou si vous êtes locataire de la solution EPI connectée.

SYNAMAP

Syndicat national des acteurs du marché
de la prévention et de la protection

75, rue de Lourmel
75015 PARIS
01 46 94 61 17
info@synamap.fr
www.synamap.fr