BTS SIO2
bloc 1

B1-Act3-TD1 – Évaluation des risques EBIOS RM (0h30)

Introduction

Le travail porte sur l'utilisation de la méthode EBIOS[1] pour évaluer les risques sur la vie privée de personnes concernées par un traitement de données à caractère personnel. Seuls ces risques sont étudiés.

Le contexte est celui d'une entreprise française dont l'employeur souhaite équiper les véhicules de fonction de ses commerciaux de dispositifs de géolocalisation[2]. Son but est essentiellement d'optimiser leurs déplacements pour réduire les coûts associés, dans la mesure où il a la charge d'organiser leurs déplacements[3] de manière individuelle.

En effet, l'employeur a constaté les limites des dispositifs de planification standards individuels. Ils ne permettent pas de planifier des itinéraires complexes d'un seul véhicule, et encore moins d'un parc complet. Il n'est donc pas possible d'optimiser les déplacements des commerciaux dans leur ensemble. En outre, ils ne mesurent que la position du véhicule et ne considèrent pas la durée d'utilisation du véhicule, le kilométrage parcouru ou les vitesses de circulation, ce qui limite les possibilités d'optimisation. Le service associé doit donc permettre cette optimisation d'itinéraires.

Il est prévu que le traitement repose sur un boîtier GPS embarqué dans les véhicules. Ce boîtier communiquerait par GSM avec un serveur hébergé chez un prestataire, qui stockerait également les données collectées dans une base de données. On note que le boîtier lui même peut stocker temporairement des données (quelques jours au maximum) pour palier aux soucis de captation du réseau (tunnel, zone peu couverte) ou aux soucis de sur-taxation de la communication (zones frontalières). L'employeur accéderait à une application du prestataire via Internet, afin de gérer le lien entre les véhicules et les commerciaux, de paramétrer le boîtier (horaires, alertes sur zone géographique…) et de visualiser les données. Des tableaux de bord lui seraient envoyés une fois par mois par courrier électronique.
L'accès à l'application web du prestataire (et donc à la base de données) serait contrôlé par un identifiant et un mot de passe.

L'étude des risques a pour objectif de déterminer des modalités de mise en œuvre respectueuses de la vie privée de ses employés. En effet, l'enjeu de l'employeur réside dans l'acceptation du traitement par les commerciaux, qui pourraient contester la proportionnalité du dispositif ou estimer qu'ils doivent avoir une liberté dans leurs déplacements.

L'employeur : *Comment faire en sorte que mes commerciaux ne se sentent pas « fliqués » ? Comment prouver à mes employés que seules des données professionnelles sont collectées ?*
Un commercial : *Puis-je me faire licencier pour avoir utilisé mon véhicule de fonction à des fins personnelles ? Qu'en est-il de ma liberté de déplacement ?*
La CNIL : *Le dispositif n'est-il pas disproportionné ?*

Travail demandé

Le début de l'analyse a été réalisé (atelier 1 de la méthode EBIOS). On vous demande de poursuivre cette analyse, de prévoir les mesures à mettre en place, et de compléter la matrice des scénarios des risques (avant et après la mise en place des mesures).

---

[1] Expression des besoins et identification des objectifs de sécurité. Méthode de gestion des risques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

[2] Lorsqu'on parle de géolocalisation il serait plus juste de parler de « chronogéolocalisation ». Ce qui est recherché n'est pas seulement où était la personne mais où était la personne tel jour à telle heure. Si elle n'est pas forcément recherchée en temps réel, il s'agit bien d'un suivi dans le temps et dans l'espace des déplacements (traces).

[3] On rappelle qu'il est interdit de géolocaliser un employé disposant de manière certaine d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP…)

Les risques : des atteintes potentiellement graves à la vie privée des commerciaux – À COMPLÉTER

ATELIER 1				ATELIER 2	ATELIER 3	ATELIER 4
Risques	**Événements redoutés jugés comme <u>les plus graves</u>** (impacts sur les personnes concernées)	**Mesures réduisant la gravité**	**Gravité**	**Pertinence du risque**	**Scénarios Chemins d'attaques**	**Vraisemblance**
R1 – Accès illégitime à des données par l'employeur	La vie privée des commerciaux est atteinte par « flicage » en dehors du temps de travail (déjeuners, soirées, week-end, vacances).	Aucune				
R2 – Accès illégitime à des données par un concurrent ou un tiers intervenant sur les véhicules	Un concurrent ou un tiers récupère les données (professionnelles et personnelles) pour « voler » la clientèle de l'entreprise.	Aucune				
R3 – Accès illégitime à des données par un administrateur informatique du prestataire	Un administrateur du prestataire récupère les données pour les vendre ou faire du chantage.	Aucune				
R4 – Disparition accidentelle de données	Le dispositif n'envoie plus de données de géolocalisation.	Aucune				
R5 – Disparition délibérée de données	Les commerciaux sont accusés d'avoir manipulé le dispositif.	Aucune				
R6 – Modification non désirée de données	Un bug fait que le dispositif ne permet par aux commerciaux d'optimiser leur itinéraire.	Aucune				

Les mesures à mettre en place (ATELIER 5) – À COMPLÉTER

Les principales mesures doivent non seulement permettre de traiter les risques, mais aussi de respecter les principes fondamentaux de la protection de la vie privée : finalité déterminée, explicite et légitime ; données adéquates, pertinentes et non excessives ; durées de conservation limitées ; information des personnes ; droits d'accès, de rectification, etc. L'objectif visé est notamment d'éviter que :

- les commerciaux ne soient pas convenablement informés (affichage au siège de l'entreprise alors que les commerciaux n'y vont jamais, dispositif installé sans préciser pourquoi, information orale, ou pas individuelle…), et donc géolocalisés à leur insu ;
- des données non pertinentes ou excessives par rapport à la finalité soient collectées (ex : enregistrement de la vitesse instantanée ou maximale) ;
- les données soient utilisées pour une autre finalité que celle prévue (ex : licenciement), en permettant à l'employeur de détourner l'usage de l'application pour corréler les données prévues avec d'autres informations telles que les zones géographiques et les limitations de vitesse associées ;
- les forces de l'ordre exploitent les données pour sanctionner des excès de vitesse
- etc.

Listez ici les mesures principales à mettre en place.

La matrice des scénarios des risques – À COMPLÉTER

Placez sur la matrice ci-dessous les risques R1 à R6 avant et après la mise en place des mesures.