Introduction

Verizon Connect fournit des Solutions destinées au Personnel Itinérant en matière de Gestion de flotte automobile et de Suivi de flotte. Nos Produits suivent la performance de votre flotte de véhicules qui peuvent avoir un impact important sur votre activité. Il s'agit de la localisation de vos véhicules, du comportement de vos conducteurs sur la route et de leur consommation de carburant. Ces informations sont ensuite placées sur des tableaux de bord faciles à comprendre afin que vous puissiez agir rapidement. Reveal est un outil essentiel pour vous aider à en faire plus en moins de temps, fournir un meilleur service client et finalement améliorer les résultats de votre entreprise. À travers nos produits de Suivi de flotte, nous avons également la capacité de gérer le cycle de vie complet des demandes de services de nos clients, dès le premier contact avec le client, la fourniture d'un devis pour le travail, la planification de la tâche, l'acheminement, l'itinéraire optimal du conducteur et le paiement.

Le présent livre électronique – eBook - répond aux Questions fréquemment posées sur les Services Reveal de suivi de Flotte (« les services » ou « Reveal ») que Verizon Connect (« VZC ») vous propose sur la plateforme Reveal et fournit un aperçu de certaines des considérations et exigences clés en matière de protection des données à caractère personnel dont vous aurez besoin avant la mise en œuvre du service, pendant et après le déploiement du service. Si le présent eBook se concentre principalement sur les questions de protection des données à caractère personnel, vous devez vous demander si d'autres exigences légales pertinentes affecteront votre mise en œuvre et votre utilisation des services. Par exemple, dans certains pays, l'application de dispositions du droit du travail sera déclenchée par l'utilisation des services dans les véhicules conduits par des employés.

Le cas échéant, il est fait référence aux lignes directrices règlementaires disponibles au moment de la publication. Les régulateurs revoient et révisent leurs lignes directrices régulièrement ; vous devez donc être attentifs aux développements dans ce domaine dans la mesure où il relèvera finalement de votre responsabilité en tant que Responsable du traitement des données à caractère personnel collectées et utilisées par le service de garantir le respect des lois applicables.

Les informations fournies dans le présent eBook ne constituent pas un conseil juridique ou professionnel. Vous devez toujours consulter un avocat dûment qualifié concernant toute problématique ou question juridique spécifique. VZC n'assume aucune responsabilité quant aux informations contenues dans le présent eBook et décline toute responsabilité sur ces informations.

Questions fréquemment posées sur Reveal

1. Quelles sont les personnes dont les données sont collectées par les services ?

Les données seront collectées essentiellement concernant les employés et les prestataires qui conduisent les véhicules dans lesquels vous déployez les services. Les données peuvent également être collectées concernant d'autres personnes (par exemple, les passagers ou d'autres personnes vivant au sein du foyer du conducteur et ayant accès au véhicule), selon les modalités et les raisons pour lesquelles vous déployez le service.

2. Comment les données sont-elles collectées pour le service ?

Le service collecte des données provenant de deux sources :

- Le dispositif embarqué installé dans vos véhicules : Celui-ci collecte des données sur les localisations et les activités de vos véhicules. Si vous savez (ou pourriez déterminer) qui est le conducteur auquel chaque véhicule est attribué, ces informations constitueront également des données à caractère personnel.

- Nous disposons de plusieurs applications mobiles sur nos plateformes, que vous pouvez installer pour utiliser notre service de façon efficace, telles que nos applications relatives au S (Work, Workforce, Field) et nos applications relatives à la Gestion de la flotte (Manager/Spotlight, Video, ELD). Pour utiliser l'application, chaque conducteur doit fournir certaines informations au cours de l'enregistrement.

Dans le présent eBook, nous désignons collectivement toutes les données à caractère personnel collectées par le service « Données personnelles Reveal ».

3. Quelles sont les données à caractère personnel collectées par le service ?

Vous déterminez la majorité des données à caractère personnel qui seront collectées par le service ; ce que vous souhaitez collecter variera selon les modalités et les raisons pour lesquelles vous déployez la solution. Vous avez le contrôle total du type de données que vous collectez. En tant que tel, il en va de votre responsabilité légale de vous assurer que vous avez besoin d'obtenir les données que vous collectez pour utiliser le service.

Les données à caractère personnel collectées par l'intermédiaire du dispositif embarqué à bord du véhicule peuvent comprendre :

- Des données de localisation (GPS) des véhicules et des personnes ;
- Des informations tachygraphiques (temps de conduite) ;
- La vitesse et le comportement du conducteur du véhicule ;
- Des données relatives aux événements du véhicule (par exemple, implication dans un accident, pénétrer ou quitter une zone délimitée géographiquement) ;
- D'autres informations sur le véhicule (par exemple, consommation de carburant, pression des pneus, données opérationnelles).

Les données à caractère personnel collectées par l'intermédiaire de l'application peuvent comprendre :

- Le nom du conducteur ;
- Le numéro de téléphone, l'adresse email et l'adresse du domicile du conducteur ;
- Les identifiants de connexion du conducteur ;
- Les dossiers du conducteur (par exemple, l'attribution d'un véhicule, le numéro du conducteur, les zones délimitées géographiquement) ;
- La géolocalisation GPS.

4. Des « catégories particulières » de données à caractère personnel ou relatives à des condamnations pénales ou des infractions sont-elles collectées par l'intermédiaire de Reveal ?

Conformément aux lois sur la protection des données personnelles, les catégories particulières de données à caractère personnel sont des données à caractère personnel relatives à la race, l'origine ethnique, les opinions politiques, la religion, l'appartenance à un syndicat, la génétique, la biométrie (quand utilisées à des fins d'identification), la santé, la vie sexuelle, l'orientation sexuelle. De même que les données à caractère personnel relative aux condamnations pénales et aux infractions, le traitement des catégories particulières de données à caractère personnel est plus limité que d'autres traitements.

Aucune catégorie particulière de données à caractère personnel ou de données à caractère personnel relative aux condamnations pénales et aux infractions ne sont demandées via le service (par exemple, les conducteurs ne se voient pas demander d'entrer des informations de cette nature dans l'application). Si des catégories particulières de données à caractère personnel peuvent être déduites à partir des données de localisation (par exemple, les données de géolocalisation pourraient identifier qu'un conducteur se rend régulièrement dans un centre religieux ou médical), cela ne déclenche pas l'application des dispositions du RGPD relatives au traitement de catégories particulières de données à caractère personnel sauf si les données de géolocalisation sont effectivement utilisées pour déduire ce type de catégories particulières de données à caractère personnel. Néanmoins, selon les modalités et les raisons pour lesquelles vous déployez le service, les données à caractère personnel relatives aux condamnations pénales et aux infractions (alléguées) pourraient être

traitées à partir des données collectées (par exemple, les données sur l'activité du véhicule pourraient indiquer qu'un conducteur a dépassé une limite de vitesse).

Ce qui constitue une infraction pénale variera en fonction des pays, de même que la catégorisation des données en « catégorie particulière » de données à caractère personnel ou données à caractère personnel relative aux condamnations pénales et aux infractions. Dans le cas où vous collectez des données qui pourraient être considérées comme des données à caractère personnel relative aux condamnations pénales et aux infractions, conformément aux lois sur la protection des données, vous devrez alors respecter, en tant que Responsable du traitement de ces données à caractère personnel, des obligations légales supplémentaires prévues par le RGPD et par les lois nationales

5. Qui a accès aux Données personnelles Reveal ?

Les Données personnelles Reveal traitées dans le cadre de la fourniture du service sont mises à la disposition des employés Verizon compétents, selon le principe du « besoin d'en connaitre ». Les Données personnelles Reveal sont également mises à la disposition de sociétés tierces qui fournissent des services à Verizon pour permettre à Verizon de gérer le service (par exemple, des tiers qui fournissent des services d'hébergement). Verizon peut également communiquer les Données personnelles Reveal à des tiers si la loi l'exige (par exemple, les instances chargées de l'application des lois).

Outre les finalités décrites ci-dessus, vous pouvez choisir de communiquer les Données personnelles Reveal pour vos propres finalités. Vous choisirez qui, au sein de votre organisation, devrait avoir accès aux Données personnelles Reveal (par exemple, vous devrez désigner des administrateurs qui peuvent accéder au portail en ligne pour visualiser la localisation du véhicule en temps réel et les données relatives à l'activité du véhicule). Vous pouvez également choisir de partager les Données personnelles Reveal à des tiers, tels que d'autres organisations au sein de votre groupe de sociétés, ou d'autres fournisseurs de plateformes (par exemple, si une autre plateforme offre des interfaces avec Reveal).

6. Verizon transfère-t-elle les Données personnelles Reveal en-dehors de l'Espace économique européen (« EEE ») ?

Verizon héberge les Données personnelles Reveal dans des centres de données situés à la fois au sein et en-dehors de l'EEE. Une liste de ces pays est disponible ici : https://www.verizon.com/about/privacy/data-processing-activities. Si Verizon partage les Données personnelles Reveal en-dehors de l'EEE au sein du groupe Verizon, ces transferts sont effectués selon les Règles d'entreprise contraignantes approuvées par l'Union européenne pour le Responsable du traitement & le Sous-traitant (BCRs).

7. Combien de temps Verizon conserve-t-elle les Données personnelles Reveal ?

Les Données personnelles Reveal seront conservées aussi longtemps que convenu dans les clauses du contrat et conformément aux paramètres de conservation que vous sélectionnez dans le produit. Cela variera en fonction de votre obligation légale à conserver les données ou toute exigence de reporting que vous pouvez demander. Il en va de votre responsabilité en tant que Responsable du traitement de vous assurer que vous comprenez la durée pendant laquelle vous êtes légalement tenu de conserver les Données personnelles Reveal. A la résiliation des services, Verizon Connect effacera les Données personnelles Reveal de façon sécurisée.

8. Verizon utilise-t-elle les Données personnelles Reveal pour ses propres finalités ?

Les Données personnelles Reveal sont collectées par Verizon pour vous fournir le service Reveal que vous avez demandé. Verizon est un sous-traitant pour ces finalités.

Dans la mesure permise par la loi, Verizon fait une certaine utilisation secondaire des données anonymisées collectées par le système Reveal à ses propres fins et pour améliorer les produits et services. Cela comprend des analyses pour optimiser la solution Reveal et la communication à des compagnies d'assurance. Aucune personne ni organisation utilisant Reveal ne peut être identifiée à partir des données anonymisées.

9. Comment Verizon garantit-elle que les Données personnelles Reveal sont conservées de façon sécurisée ?

Veuillez-vous référer au document Annexe de sécurité du Système d'information interne Verizon (Verizon Internal Systems Information Security Exhibit) pour une description des mesures de sécurité techniques et organisationnelles que Verizon met en œuvre pour satisfaire à ses obligations conformément au RGPD à ***https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit.***

Exigences en matière de protection des données à caractère personnel

La présente section explique comment les exigences en matière de protection des données à caractère personnel s'appliquent à votre utilisation de Reveal.

A la fin de la présente section, nous avons inclus une liste de vérification des articles du Règlement Général sur la Protection des Données Personnelles et de la section dans laquelle ils sont abordés dans le présent eBook. Cela vous permettra de vérifier si une disposition particulière du RGPD est pertinente pour Reveal et où elle est traitée dans ce eBook Nous avons également inclus une liste de sources d'informations complémentaires.

A. Analyse d'impact relative à la protection des données

Une analyse d'impact relative à la protection des données (« AIPD ») est un processus pour décrire et évaluer le traitement des données à caractère personnel et pour identifier et gérer les risques que le traitement des données présente pour les personnes concernées.
Collectivement, les autorités de contrôle de la protection des données considèrent que les AIPD doivent être menées quand une organisation traite des données à caractère personnel pour évaluer les performances, la localisation ou le mouvement des employés[1]. Il est probable que votre utilisation du service nécessite que vous meniez une AIPD. Toutefois, chaque autorité de contrôle a publié ses propres critères relatifs aux AIPD. Vous devez consulter les critères établis par votre autorité de contrôle compétente pour identifier si une AIPD est requise.

Votre AIPD doit :

- Décrire le traitement de Données personnelles Reveal qui sera mis en place ;
  - Les informations dans le présent eBook sur la nature des données collectées, la façon dont elles sont collectées et dont elles sont traitées vous aideront.
- Décrire les finalités du traitement - et, si la base juridique de votre utilisation du service est que le traitement est nécessaire à une finalité qui est dans vos intérêts légitimes, préciser quel est cet intérêt.
- Évaluer si le traitement est un moyen nécessaire et proportionné pour atteindre ces objectifs ;
  - Cela signifie de considérer s'il est raisonnablement possible d'atteindre les objectifs d'une

[1] Groupe de travail Article 29 *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679* (WP248) p. 10.

autre façon qui implique de traiter moins de données à caractère personnel.
    - Par exemple, si une société souhaite suivre les heures travaillées par une personne, est-ce que cela pourrait être réalisé par un processus alternatif plutôt que de suivre sa localisation pendant toute la durée de sa période de travail, dans la mesure où cela serait clairement disproportionné.
- Évaluer les risques que le traitement présente pour les personnes concernées et comment ces risques peuvent être gérés ;
    - Par exemple, si un employé est autorisé à utiliser un véhicule pour son usage privé, suivre le véhicule alors que l'employé ne travaille pas serait intrusif et ne serait pas nécessaire pour atteindre les finalités poursuivies par l'employeur. Ce risque pourrait être atténué en autorisant l'employé à désactiver le service en-dehors des heures de travail, en activant le mode « *Privacy Switch* » (mode Vie Privée) et en s'assurant que les employés connaissent l'existence de cette option.
- Décrire les mesures de sécurité ; et
- Décrire les autres mesures pour garantir la protection des données à caractère personnel et pour démontrer la conformité.
    - L'AIPD doit traiter les autres sujets exposés dans le présent eBook.
    - En particulier, l'AIPD doit exposer comment les droits de la personne concernée sont respectés.

Au cours de la réalisation de votre AIPD, vous devez consulter votre Délégué à la protection des données (DPO) (si vous en avez un). Le cas échéant, vous devez également consulter les personnes dont les données seront traitées, ou leurs représentants - par exemple, par la Consultation de l'Employé, du Syndicat ou du Comité d'entreprise - et refléter les résultats de cette consultation dans l'AIPD.

Si votre AIPD conclut que l'utilisation des Données personnelles Reveal pour les finalités que vous envisagez entraîne des risques élevés et non atténués pour les personnes concernées, vous devez consulter votre autorité de contrôle compétente (au Royaume Uni, il s'agit de l'*Information Commissioner's Office*,

Vous devrez continuer à examiner toute AIPD et à évaluer périodiquement votre déploiement du service et votre utilisation des Données personnelles Reveal par rapport à celle-ci.

Notices d'information

Comme pour tous les traitements de données à caractère personnel que vous réalisez, il vous incombe de vous assurer que vous fournissez aux personnes concernées une informations claire et compréhensible concernant votre collecte et l'utilisation que vous faites de leurs Données personnelles Reveal.

La présente section décrit les informations que vous êtes obligé d'inclure dans votre notice d'information pour satisfaire aux exigences en matière de protection des données à caractère personnel. Cependant, vous devez vérifier si d'autres obligations légales pertinentes affecteront le contenu de votre notice d'information et la façon dont vous mettez en œuvre le service. Par exemple, dans certains pays, le droit du travail exigera d'inclure des informations additionnelles dans votre notice d'information ou dans d'autres documents internes.

Le RGPD requiert d'inclure les informations suivantes dans votre notice d'information:

- Votre identité et vos coordonnées (et celles de votre délégué à la protection des données, si vous en avez désigné un) ;
- Les finalités et les bases juridiques du traitement (et, si vous traitez des Données personnelles Reveal aux fins de vos « intérêts légitimes », quels sont ces intérêts) ;
    - Les sections sur les finalités et la base juridique dans le présent eBook vous aideront à envisager et à décrire ces points.
- Les catégories de Données personnelles Reveal traitées (et les sources), si elles ne sont pas obtenues directement auprès de la personne concernée ;
    - La section 3 ci-dessus « Quelles sont les données à caractère personnel collectées par le service ? » vous aidera à les décrire.

- Les destinataires des Données personnelles Reveal et tout pays non membre de l'EEE auquel les Données personnelles Reveal sont transférées (incluant le détail des garanties appropriées mises en place)

- La durée de conservation des Données personnelles Reveal ;
- Si la fourniture de Données personnelles Reveal est obligatoire et les conséquences éventuelles de la non-fourniture de ces données ;
- L'existence de prise de décision individuelle automatisé (y compris le profilage), avec des informations utiles concernant la logique impliquée, ainsi que l'importance et les conséquences éventuelles d'un tel traitement pour la personne concernée ;
- Une description des droits de la personne concernée (y compris le droit de retirer son consentement, si vous traitez des Données personnelles Reveal si la personne a donné son consentement) et la possibilité de déposer une plainte auprès d'une autorité de contrôle.

La notice d'information fournie doit également satisfaire aux exigences supplémentaires prévues par l'art. 12 du RGPD (par ex., les informations que vous fournissez aux personnes concernées doivent être concises, transparentes, compréhensibles et aisément accessibles, en des termes clairs et simples).

Utilisateurs du service en France

Outre les exigences du RGPD énumérées ci-dessus, la Loi Informatique et Libertés impose d'informer les personnes concernées de leur droit à définir des directives relatives au sort de leurs données à caractère personnel après leur décès.

Notice d'information dans le véhicule

Étant donné que la collecte des Données personnelles Reveal est un mode de collecte de données moins visible pour les personnes concernées, mais qui peut avoir des conséquences significatives, vous devez fournir un effort particulier pour porter l'utilisation du service à l'attention des conducteurs. Outre la notice d'information compréhensible décrite ci-dessus, les lignes directrices d'ordre réglementaire indiquent que vous devez également informer clairement les conducteurs qu'un dispositif de suivi a été installé dans le véhicule qu'ils conduisent et que leurs mouvements (et leur comportement de conduite, si la technologie concernée est déployée) font l'objet d'un suivi. Idéalement, cette information doit être affichée de façon proéminente dans chaque véhicule concerné, à la vue du conducteur.[2]

Utilisateurs du service en Pologne

Outre le contenu énuméré ci-dessus, si le déploiement du service constitue une surveillance des employés, l'information dans le véhicule doit également indiquer :

- Quelles sont les données collectées et enregistrées ;
- Où et combien de temps ces données sont stockées ; et
- Qui a accès aux données[3].

Politiques de mis en application

Si les Données personnelles Reveal seront utilisées pour faire appliquer vos règles et normes, vous devez vous assurer qu'une telle utilisation est légale et que les employés connaissent les règles concernées et que vous procéderez à un suivi pour voir si elles sont satisfaites, via le service.

C. Registre des activités de traitement

[2] Groupe de travail Article 29 *Avis 2/2017 sur le traitement des données sur le lieu de travail* (WP249), p. 20

[3] Bureau (polonais) de protection des données, *Protection des données sur le lieu de travail. Directives pour les employeurs,* p. 37

En tant que responsable du traitement des données, vous devez tenir un Registre des activités de traitement (« Registre »), tel que prévu par l'art. 30 du RGPD. Vous devez vous assurer que le traitement des Données personnelles Reveal est inclus dans votre Registre. Vous devez inclure les informations suivantes :

- Le nom et les coordonnées de votre organisation (et, le cas échéant, le nom et les coordonnées de votre délégué à la protection des données, représentant et/ou responsable conjoint du traitement) ;
- La finalité pour laquelle vous utilisez les Données personnelles Reveal ;
- Une description des catégories de Données personnelles Reveal et des catégories des personnes dont les données sont traitées ;
    - La section 3 ci-dessus « Quelles sont les données à caractère personnel collectées par le service ? » vous aidera à le remplir.
- Les catégories de destinataires auxquels les Données personnelles Reveal seront communiquées ;
    - La section 5 ci-dessus « Qui a accès aux Données personnelles Connect ? » vous aidera à le remplir. Vous devez lister également les destinataires auxquels vous donnez accès aux Données personnelles Reveal
- Transferts des Données personnelles Reveal vers des pays situés hors de l'EEE ;
    - La section 6 ci-dessus « Verizon transfère-t-elle les Données personnelles Connect en-dehors de l'EEE ? » explique où les données sont transférées et quelles sont les garanties appropriées utilisées pour protéger les Données personnelles Reveal
- Les durées de conservation
    - La section 7 ci-dessus « Combien de temps Verizon conserve-t-elle les Données personnelles Reveal ? » explique ce point.
- Informations sur les mesures de sécurité, lorsque cela est possible.
    - Veuillez-vous référer au *document Annexe de sécurité du Système d'information interne Verizon (Verizon Internal Systems Information Security Exhibit)* pour une description des mesures de sécurité techniques et organisationnelles que Verizon met en œuvre pour satisfaire aux obligations qui s'imposent à elle en vertu du RGPD disponible à l'url suivant : https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit

Verizon a mis à votre disposition des informations pour vous aider à mettre en œuvre cette obligation au lien suivant : https://www.verizon.com/about/privacy/data-processing-activities

Utilisateurs du service au Royaume Uni

Si vous traitez des données de condamnations pénales et d'infractions et si votre base juridique pour le traitement est l'une des conditions visées à l'Annexe 1 de la Loi sur la protection des données de 2018 (*Data Protection Act 2018*), vous serez alors tenu d'ajouter des colonnes supplémentaires dans le Registre (portant sur la base juridique et les conditions du traitement, et sur la conservation/suppression des données concernées conformément au à la Politique appropriée, si requis).

D. Finalités

Vous devrez identifier la ou les finalités pour lesquelles vous souhaitez déployer le service et utiliser les Données personnelles Reveal, par exemple :

- Détecter et prévenir la perte des biens de votre organisation ;
- Améliorer la productivité des employés ;
- Optimiser les itinéraires et les ressources et économiser du carburant ;
- Fournir aux clients des informations de suivi en temps réel ;
- Assurer la sûreté et la sécurité de vos employés, en s'assurant, par exemple, que les pauses et les repas sont observés.

Il est important que vous soyez clair dès le départ sur les finalités pour lesquelles le service est déployé.

- Vous avez besoin d'une « base juridique » pour chaque finalité distincte pour laquelle vous traitez les Données personnelles Reveal ;
- Vous devez vous assurer que vous ne traitez pas plus de Données personnelles Reveal que ce qui est raisonnablement nécessaire pour cette finalité ;
- Vous devez dire aux personnes concernées quelles sont ces finalités.

Une fois que vous avez collecté les Données personnelles Reveal pour ces finalités, vous ne pouvez alors utiliser les Données personnelles Reveal que pour ces finalités, ou pour d'autres finalités qui sont compatibles avec ces finalités. Parfois, le droit applicable autorise des exceptions à ce principe.

Utilisateurs du service en France

Les dispositifs de géolocalisation ne peuvent être installés dans des véhicules utilisés par des employés que pour les finalités suivantes[4] :

- Suivre, justifier et facturer les services de transport de passagers ;
- Assurer la sûreté et la sécurité des salariés, des biens et des véhicules (notamment, localiser des véhicules volés) ;
- Optimiser la répartition des ressources si des services sont fournis dans des zones géographiques étendues, particulièrement dans le contexte des services d'urgence ;
- Suivre le temps de travail (mais uniquement si aucun moyen alternatif de suivi du temps de travail n'est disponible) ;
- se conformer aux obligations légales et réglementaires ;
- S'assurer que les règles prévues par l'employeur concernant l'utilisation des véhicules de travail sont respectées.

À l'inverse, l'utilisation d'un dispositif de géolocalisation installé dans les véhicules des salariés est interdite[5] :

- Pour contrôler le respect des limites de vitesse ;
- Pour suivre les salariés en permanence ;
- Pour suivre le temps de travail lorsque des moyens alternatifs sont disponibles ;
- Dans le véhicule d'un salarié qui dispose d'une liberté dans l'organisation de ses déplacements et de son travail (par exemple, un commercial) ;
- Pour suivre l'utilisation privée du véhicule si une utilisation privée est autorisée (par exemple, pendant les pauses ou par des salariés qui peuvent librement organiser leurs déplacements) ; ou
- Pour suivre des représentants de syndicats ou agissant de façon similaire dans l'exercice de leurs fonctions.

Utilisateurs du service en Allemagne

Les systèmes de suivi, par lesquels les employés peuvent être surveillés de façon permanente, ne sont généralement pas autorisés.[6]

Utilisateurs du service en Pologne

Si et dans la mesure où le déploiement du service constitue une surveillance des employés, les organisations ne peuvent traiter les Données personnelles Reveal qu'aux fins légitimes de « s'assurer que les employés font un bon usage de leur temps de travail et une utilisation correcte de leur équipement et outils ». L'autorité de contrôle polonaise suggère que cette finalité légitime est assez large et peut autoriser :

- La localisation d'un véhicule en cas de vol ;

[4] Directives de la CNIL sur la géolocalisation des véhicules des salariés, 2018

[5] Directives du CNIL sur la géolocalisation des véhicules des employés, 2018

[6] Commissaire à la protection des données et à la liberté d'information Rhénanie-Palatinat, *Sur la licéité d'un suivi GPS des employés* ; Commissaire à la protection des données et à la liberté d'information Baden-Württemberg, *Protection des données en matière d'emploi*, 2018, pp. 36- 37.

- La recherche de la responsabilité d'un employé concernant un dommage causé à un véhicule ; ou
- L'optimisation des itinéraires et des ressources et l'économie de carburant.

Utilisateurs du service au Portugal

Les services ne peuvent pas être utilisés pour surveiller le comportement des salariés, et peuvent uniquement être déployés dans les véhicules utilisés par les employés pour les finalités autorisées suivantes : [7]

- **La gestion de la flotte lorsque des services externes sont fournis :**
  - Les services d'assistance technique ;
  - La distribution de biens ;
  - Le transport de passagers ;
  - Le transport de biens, et
  - La sécurité privée.
- **La protection des biens**
  - Le transport de matières dangereuses, etc.
  - Le transport de matériaux de grande valeur

E. Bases juridiques

Vous devrez identifier une base juridique conformément à l'art. 6 du RGPD pour chaque finalité pour laquelle vous utilisez les Données personnelles Reveal. Selon votre situation, vous pouvez utiliser les Données personnelles Reveal parce que cela est nécessaire pour :

- **Respecter une obligation légale :** par exemple, si vous êtes légalement tenu de surveiller l'utilisation/les heures de conduite des véhicules en fixant un tachygraphe à un véhicule ;
- **Exécuter un contrat avec la personne concernée :** par exemple, si une bonne conduite est une condition de travail ;
- **Poursuivre une finalité qui est dans vos intérêts légitimes :** par exemple, maintenir vos conducteurs (et autres usagers de la route) saufs, faire appliquer des habitudes de bon conducteur, surveiller la flotte, améliorer l'efficacité du carburant et de la maintenance, se défendre en cas d'accidents et de fausses déclarations, assurer la santé & la sûreté du personnel, et contribuer aux primes d'assurance.

Il est impératif que vous vous assuriez de disposer d'une base juridique légitime pour traiter les données et que vous soyez en mesure de la justifier auprès d'un Autorité de contrôle de la protection des données à caractère personnel, si cela est requis.

Vous devrez démontrer que le traitement des Données personnelles Reveal est « nécessaire ». « Nécessaire » signifie que le traitement des Données personnelles Reveal doit être un moyen ciblé et proportionné d'atteindre votre objectif ; le traitement doit être « plus que souhaitable, mais moins qu'indispensable ou absolument nécessaire »[8]. Votre évaluation doit être factuelle en prenant en compte l'objectif poursuivi et toutes les options moins intrusives pour atteindre le même but. S'il existe des alternatives moins intrusives et que celles-ci sont réalistes, alors le traitement n'est pas « nécessaire ».[9]

Si vous invoquez des intérêts légitimes, vous devrez effectuer un « test de mise en balance » et le documenter pour vous assurer que vos intérêts légitimes ne sont pas supplantés par les intérêts, les droits et les libertés

[7] Directives du CNPD et code du travail.

[8] *South Lanarkshire Council v Scottish Information Commissioner* [2013] UKSC 55

[9] Comité européen de la protection des données (CEPD), *Directives 2/2019 sur le traitement des données à caractère personnel aux termes de l'article 6(1)(b) du RGPD dans le contexte de la fourniture de services en ligne aux personnes concernées, adoptées le 9 avril 2019*, p. 7.

des personnes concernées. Le traitement doit être nécessaire à la finalité (c'est-à-dire proportionné aux besoins de l'activité) et des garanties doivent être incluses pour la vie privée des personnes concernées. Si les intérêts des personnes concernées prévalent sur vos intérêts, alors le traitement ne doit pas être poursuivi.

Consentement **:** Vous pouvez également traiter des Données personnelles Reveal si la personne concernée a donné son consentement à cette fin. Cependant, le consentement n'est valable que s'il est donné librement. Les personnes doivent également être libres de révoquer leur consentement - sans préjudice. Cela rend difficile l'obtention d'un consentement valide dans le contexte de l'emploi.[10]
De nombreuses autorités de de protection des données ont commenté les bases juridiques dans le contexte de la télématique. Par exemple :

- Au Royaume Uni et en Pologne, lorsque qu'un véhicule peut être utilisé à des fins privées, surveiller les mouvements quand il est utilisé à titre privé, sans le consentement de l'utilisateur donné librement, sera rarement justifié.[11]
- Au Portugal, le consentement ne constitue pas une base juridique valable pour traiter des données dérivées de la géolocalisation.[12]
- Les dispositifs de suivi de véhicule ne doivent pas être considérés comme des dispositifs pour suivre ou surveiller le comportement ou les localisations des conducteurs ou autres employés, par exemple en envoyant des alertes concernant la vitesse du véhicule.[13]
- Le traitement des données de localisation peut être justifié si cela est réalisé pendant le suivi du transport de personnes ou de biens, l'amélioration de la répartition des ressources, ou pour la sécurité de l'employé , du véhicule, ou des biens transportés, mais peut s'avérer excessif si les employés sont libres d'organiser leurs déplacement comme ils le souhaitent ou si cela est réalisé dans l'unique but de surveiller le travail d'un employé alors qu'il peut être surveillé par d'autres moyens.[14]
  Envoyer des informations excessives à un client sur le conducteur livrant ses produits, par exemple une photographie de passeport (en plus du nom et de la localisation du conducteur) pour permettre à un client de vérifier l'identité du livreur à son arrivée n'est pas susceptible d'avoir une base juridique (il y aurait un « intérêt légitime » à fournir la photographie à des fins d'identification mais cela est considéré disproportionné dans le cadre du test de mise en balance).[15]

Données de condamnations pénales et d'infractions

Si les Données personnelles Reveal que vous traitez comprennent des données de condamnations pénales et d'infraction (au regard des lois locales et de l'interprétation locale des « infractions »), alors l'art. 10 du RGPD limite le traitement de ces données à caractère personnel. Les données de condamnations pénales et d'infractions ne peuvent être traitées que sous le contrôle d'une « autorité officielle » ou si cela est autorisé

[10] Par exemple, les consentements des employés sont régulièrement considérés invalides en Allemagne (Commissaire à la protection des données et à la liberté d'information (LDi) NRW, *24e Rapport sur la protection des données et la liberté d'information 2017-2018*, p. 65, 66) et le consentement n'est pas une base juridique valable pour traiter des données à caractère personnel dans le contexte de l'emploi au Portugal (Directive du CNPD sur l'utilisation des outils de géolocalisation dans le contexte de l'emploi et interprétation stricte des dispositions du code du travail)

[11] Bureau du Commissaire à l'information, *Code des pratiques en matière d'emploi*, p. 76 ; Bureau (polonais) de protection des données, *Protection des données sur le lieu de travail, Directives pour les employeurs*, p. 38

[12] Directive du CNPD sur l'utilisation des outils de géolocalisation dans le contexte de l'emploi et interprétation stricte des dispositions du code du travail

[13] Groupe de travail Article 29 *Avis 13/2011 sur les services de géolocalisation sur les dispositifs mobiles intelligents*

[14] Groupe de travail Article 29 *Avis 5/2005 sur l'utilisation des données de localisation en vue de fournir des services à valeur ajoutée*

[15] Groupe de travail Article 29 *Avis 2/2017 sur le traitement des données au travail*

par les législations européennes ou nationales applicables. Vous devrez alors consulter les lois locales pour identifier les exigences pertinentes en la matière, par exemple :

Utilisateurs du service en France

Conformément à la Loi Informatique et Libertés, la collecte des données à caractère personnel relatives au comportement d'une personne qui peut ou est susceptible d'être qualifié d'infraction ou de crime est interdite. En conséquence, il est interdit de collecter les dépassements de limites de vitesse ou des informations relatives au comportement d'une personne qui peut révéler des violations des règles de circulation.

Utilisateurs du service en Allemagne

La position actuelle en Allemagne est que le traitement normal des Données personnelles Reveal ne constitue pas un traitement de données de condamnations pénales et d'infractions. L'utilisation des services dans le but spécifique de détecter des infractions pénales serait en revanche limitée par la section 26(1) BDSG (par exemple, si les mouvements du véhicules sont suivis pour détecter un vol, une fraude ou un trafic de drogue par des employés - veuillez noter que les excès de vitesse ne constituent pas en ce sens des actes criminels). Cela ne serait pas un cas d'utilisation « normale » de Reveal, et par conséquent, il est probable que le traitement pour cette finalité n'ait lieu que très exceptionnellement (par exemple, si un employeur enquête sur des cas dans lesquels il suspecte qu'un employé a commis un acte criminel), mais si vous utilisez les services à cette fin, alors la section 26(1) BDSG doit être consultée.

Utilisateurs du service en Italie

De manière générale, le traitement des Données personnelles Reveal ne constitue pas un traitement de données de condamnations pénales et d'infractions tel qu'entendu en Italie (seules les infractions qui seraient punissables par une amende administrative). Cependant, vous devez vérifier si un changement dans le droit local serait susceptible d'introduire une infraction pénale par laquelle les Données personnelles Reveal pourraient être concernées.

Utilisateurs du service en Pologne

Certaines exigences spécifiques s'appliquent au traitement des données de condamnations pénales et d'infractions concernant les employés, conformément au code polonais du travail de 1974, à savoir que vous ne pouvez pas invoquer le consentement de l'employé pour le traitement de ses données de condamnations pénales et d'infractions. Une base juridique alternative est requise ; il est très probable que les données soient traitées pour se conformer à une obligation légale ou pour l'établissement, l'exercice ou la défense de de droits en justice.

Utilisateurs du service au Portugal

Le traitement des données de condamnations pénales et d'infractions pour la prévention ou la détection d'un acte illégal (tel qu'éventuellement, la commission d'excès de vitesse ou d'infractions au code de la route) est autorisé dans certaines circonstances et si cela est nécessaire aux fins ou dans le cadre de procédures juridiques, de conseils juridiques ou pour établir, exercer ou défendre des droits en justice. Les données à caractère personnel doivent, cependant, être pseudonymisées dans les sept jours de la collecte.

Utilisateurs du service en Espagne

De manière générale, le traitement des Données personnelles Reveal ne constitue pas un traitement données de condamnations pénales et d'infractions tel qu'entendu en Espagne (uniquement l'infraction à des règles de circulation routière). Cependant, vous devez surveiller qu'aucun changement dans le droit local n'introduise une infraction pénale par laquelle les Données personnelles Reveal pourraient être concernées car le traitement des données de condamnations pénales et d'infractions en Espagne est limité - les seules

(éventuelles) circonstances pertinentes dans lesquelles le traitement des données de condamnations pénales et d'infractions pourrait avoir lieu dans ce contexte sont si (i) la finalité est la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou les mesures d'application de la loi, (ii) le traitement est couvert par une règle ayant force exécutoire ou par une loi européenne.

Utilisateurs du service au Royaume Uni

Au Royaume Uni, vous devrez vous assurer qu'en sus d'une base juridique, une condition pour le traitement est remplie, soit conformément à l'article 9 du RGPD soit conformément à l'Annexe 1 de la loi sur la protection des données de 2018. Par exemple, eu égard aux données de condamnation pénales et d'infractions, la loi sur la protection des données de 2018 permet le traitement des données à caractère personnel pour la prévention ou la détection d'un acte illégal (tel qu'éventuellement, la commission d'un excès de vitesse ou d'une infraction au code de la route) dans certaines circonstances et si cela est nécessaire aux fins ou dans le cadre de procédures juridiques, de conseils juridiques ou pour établir, exercer ou défendre des droits en justice.

F. Minimisation des données

Vous devez vous assurer que vous utilisez uniquement les Données personnelles Reveal qui sont adéquates, pertinentes et limitées à ce qui est nécessaire (au regard de vos finalités). Cela signifie finalement que vous devez identifier et utiliser le minimum de Données personnelles Reveal dont vous avez besoin pour remplir vos objectifs.

Si vous permettez aux employés de faire un usage privé des véhicules, il n'y a alors généralement pas besoin de collecter des données sur l'endroit où le véhicule est utilisé en-dehors des heures de travail. Le service a la fonctionnalité de garantir que les employés ne sont pas suivis en-dehors des heures de travail. Il s'agit du « *Privacy Switch* » (mode vie privée) et il s'agit d'un moyen simple et économique pour vous permettre de garantir votre conformité. Dans certains pays (comme la France, l'Allemagne et le Portugal), permettre aux employés d'utiliser le « *Privacy Switch* » (mode vie privée) est requis par les lignes directrices d'ordre règlementaire.[16]

G. Exactitude des données

Vous devez vous assurer que les Données personnelles Reveal que vous utilisez ne sont pas incorrectes ou fallacieuses. Dans le contexte des Données personnelles Reveal, il est particulièrement important que vous preniez des mesures pour garantir l'exactitude des données à caractère personnel (par exemple, en s'assurant que les registres des véhicules attribués aux employés soient tenus avec précision) et que vous examiniez soigneusement toute contestation relative à l'exactitude des données à caractère personnel (par exemple, un conducteur contestant sa localisation à un moment particulier).

H. Conservation des Données personnelles Reveal

Les Données personnelles Reveal doivent être conservées pendant une durée qui n'excède pas la durée nécessaire pour atteindre votre finalité spécifique. Vous devrez examiner si des obligations légales de conservation des données s'appliquent (par exemple, pour conserver les registres de temps de travail), qui devront être évoquées dans votre politique de conservation des données.

[16] Commissaire bavarois à la protection des données, 27e Rapport d'activité 2016, p. 241 ; Lignes directrices de la CNIL sur la géolocalisation des véhicules des salariés, 2018 ; Délibération du CNPD 7680/2014

I. Sécurité des Données personnelles Reveal

Vous devrez mettre en œuvre des mesures « techniques et organisationnelles appropriées » pour garantir la confidentialité, l'intégrité et la disponibilité des Données personnelles Reveal conformément à l'art. 32 du RGPD. Une évaluation des risques peut être utilisée pour identifier les problématiques particulières posées par votre déploiement de Reveal et votre utilisation des Données personnelles Reveal afin de déterminer le niveau de sécurité « approprié » (compte tenu de l'état des connaissances et des coûts de mise en œuvre). Une fois mises en œuvre, vous devez tester régulièrement vos mesures techniques et organisationnelles pour vous assurer qu'elles continuent à être appropriées. Si vous partagez les Données personnelles Reveal avec une autre organisation qui agit en tant que Sous-traitant des données pour votre compte, vous devrez vous assurer que le Sous-traitant des données présente des garanties suffisantes (et accepte contractuellement) de mettre également en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données personnelles.

Dans le cas d'une violation de sécurité impliquant des données à caractère personnel, vous devrez respecter les art. 33 et 34 du RGPD. Nous vous en informerons dans les meilleurs délais. Vous pouvez alors être tenu de notifier l'autorité de contrôle compétente 72 heures au plus tard après avoir pris connaissance de de l'incident (à moins que vous considériez que cet incident n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées). Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, vous devrez également en informer les personnes affectées dans les meilleurs délais. Vous devez examiner la manière dont vous serez en mesure d'identifier la survenance d'une violation impliquant les Données personnelles Reveal, quelles mesures doivent être prises pour atténuer la violation et comment évaluer une violation pour déterminer si une notification est requise.

Utilisateurs du service en France

Selon les lignes directrices de la CNIL sur la géolocalisation des véhicules des salariés[17], vous devez notamment mettre en œuvre :

- une politique d'autorisation d'accès ;
- des mesures pour des transferts de données sécurisés ; et
- un journal des logs d'accès et de traitement des données.

Utilisateurs du service en Espagne

Quand les données à caractère personnel sont en cours de rectification ou de suppression, la Loi Espagnole sur la Protection des Données requiert que les responsables du traitement « bloquent » les données dans le cadre des mesures techniques et organisationnelles qu'ils mettent en œuvre pour se conformer à l'art. 32 - cela signifie que les données à caractère personnel concernées doivent être extraites et stockées dans une base de données séparée et que des mesures techniques et organisationnelles doivent être adoptées pour empêcher le traitement des données (y compris tout accès et visualisation). Les données à caractère personnel concernées doivent être maintenues dans une base de données séparée et protégée afin de pouvoir répondre aux demandes qui peuvent être reçues des organismes publics compétents (tels que les juridictions, les procureurs, les autorités de contrôle de la protection des données, etc.) ou dans le cas où le transfert des données vers ces organismes publics soit nécessaire pour l'exercice ou la défense de de droits en justice. Pour calculer la période pendant laquelle les données à caractère personnel doivent être conservées « bloquées », les délais de prescription pour les différentes réclamations en justice qui pourraient découlées du traitement des données concernées doivent être examinés. Les données à caractère personnel peuvent être effacées complètement une fois que les délais de prescription concernés sont arrivés à expiration.

[17] Directives de la CNIL sur la géolocalisation des véhicules des salariés, 2018

En tant que Responsable du Traitement des Données Personnelles Reveal, vous devez vous assurer que vous pouvez vous conformer à cette obligation. Verizon vous assiste dans le respect de cette obligation en vous permettant de télécharger des copies de certaines Données Personnelles Reveal vis le tableau de bord Reveal.

J. Droits des personnes concernées

Vous devrez identifier la manière dont vous pourrez vous conformer à votre obligation de répondre aux demandes des personnes. Conformément au RGPD, les personnes concernées ont les droits suivants concernant leurs données à caractère personnel :

- Le droit d'accès ;
- Le droit de rectification ;
- Le droit à l'effacement ;
- Le droit à la limitation du traitement ;
- Le droit à la portabilité des données ;
- Le droit d'opposition ;
- Des droits relatifs à la prise de décision automatisée et au profilage.

Vous devez informer les personnes concernées que ces droits existent dans votre avis de confidentialité.

L'applicabilité de ces droits peut être limitée (par exemple, le droit à la portabilité des données ne s'applique que si les données à caractère personnel sont traitées sur la base juridique de la nécessité contractuelle ou du consentement) et vous pouvez être en mesure d'appliquer des exceptions (par exemple, si la communication d'informations porterait atteinte aux droits d'autrui, ce qui pourrait inclure la protection du secret des affaires).
En principe, vous devez répondre à ces demandes dans un délai d'un mois et vous assurer que votre réponse soit conforme aux exigences supplémentaires prévues par l'art. 12 du RGPD (c'est-à-dire, les informations que vous fournissez aux personnes concernées doivent être concises, transparentes, intelligibles et aisément accessibles, en des termes clairs et simples).

Lorsqu'il est raisonnablement possible de le faire, Verizon peut vous aider à vous conformer aux demandes qui portent sur le service.

<u>Utilisateurs du service en France</u>
Selon la Loi Informatique et Libertés, les personnes ont le droit de définir des directives concernant le sort de leurs données à caractère personnel après leur décès. Vous devez vous assurer que vous êtes en mesure de répondre à ce type de demande.

K. Partager les Données personnelles Reveal

Outre les demandes d'accès des personnes à leurs propres données, vous devrez déterminer comment vous devez répondre aux demandes d'accès aux Données personnelles Reveal provenant de tiers. Cela peut comprendre, par exemple, des demandes provenant des organes en charge de l'application des lois et des assureurs, si un véhicule a été impliqué dans un accident.

Tout partage de Données personnelles Reveal (y compris, par exemple, avec d'autres organisations au sein de votre groupe de sociétés ou à un autre prestataire de services) devra satisfaire à toutes les obligations en matière de protection des données détaillées dans le présent eBook (par exemple, le partage doit être légitime, proportionné, transparent, etc.). Vous devrez déterminer si des contrats ou d'autres arrangements doivent être mis en place avec l'organisation (par exemple, si l'autre organisation agit comme Sous-traitant

des données pour votre compte ou comme Responsable Conjoint du traitement avec vous). Lorsque ce partage implique un transfert des Données personnelles Reveal en-dehors de l'Espace économique européen (« **EEE** »), vous devrez vous assurer que le transfert est permis par le RGPD.

Utilisateurs du service en France

Selon les lignes directrices de la CNIL, vous devez limiter l'accès aux informations portant sur (ou provenant de) les dispositifs de géolocalisation aux personnes suivantes (le cas échéant) : (i) votre propre personnel autorisé, (ii) l'employeur de la personne que les données de géolocalisation concerne ; et (iii) le personnel autorisé d'un client auquel vous fournissez les services concernés. En principe, le nom du conducteur ne doit pas être partagé sauf si cette information est particulièrement pertinente et nécessaire.

L. Prise de décision automatisée

La loi sur la protection des données interdit aux organisations de prendre des décisions basées uniquement sur un traitement automatisé des données à caractère personnel lorsque la décision produirait des effets juridiques ou l'affectant de manière significative de façon similaire. Vous devrez identifier de telles utilisations du service. Cela pourrait être pertinent lorsque :

- Le salaire d'un conducteur est calculé automatiquement au moment où il commence/finit de conduire un véhicule ;
- Un conducteur se voit délivrer automatiquement un avertissement pour avoir pénétré dans une zone délimitée géographiquement ;
- L'éligibilité d'un conducteur à une prime est calculée automatiquement sur la base du nombre de tâches attribuées et accomplies par ce dernier, telles qu'enregistrées par le service.

S'il y a une intervention humaine permettant d'examiner la décision avant qu'elle ne soit prise, ces restrictions ne s'appliquent pas.

Les organisations sont autorisées à prendre ce genre de décisions exclusivement automatisées lorsque la décision est :

- Nécessaire à l'exécution ou la signature d'un contrat ;
- Autorisée par la législation de l'Union européenne ou d'un Etat membre, à laquelle le Responsable du Traitement est soumis et qui établit également des mesures appropriées pour protéger les droits, les libertés et les intérêts légitimes des personnes concernées ; ou
- Basée sur le consentement explicite de la personne concernée.

Lorsque des décisions individuelles sont prises de manière automatisée, vous devez fournir une information claire sur celle-ci aux personnes concernées (voir « Notice d'information » ci-dessus) et donner aux personnes concernées le droit d'obtenir une intervention humaine dans le processus de prise de décision, d'exprimer leur point de vue et de contester la décision.

Utilisateurs du service au Portugal

L'utilisation des données de géolocalisation et de télémétrie du véhicule destinées à une prise de décision exclusivement automatisée n'est pas permise.[18]

M. Consultation des employés/Conseil Economique et Social/syndicat

Vous pouvez être tenu par le droit du travail de consulter vos employés, le Conseil Economique et Social ou les syndicats sur la mise en œuvre du service ou sur d'autres utilisations que vous choisissez de faire des Données

[18] Directive du CNPD sur l'utilisation des outils de géolocalisation dans le contexte de l'emploi et interprétation stricte des dispositions du code du travail

personnelles Reveal. De manière alernative, vous pouvez être tenu de consulter les syndicats ou les représentants du personnel selon les termes de tout accord volontaire qui est en place. Même si cela n'est pas requis, vous pourriez estimez qu'il est approprié de consulter le personnel concernant le déploiement du service et l'utilisation des Données personnelles Reveal dans le cadre du processus AIPD.

Si vous trouvez un accord contraignant avec le Conseil Economique et Social, cet accord constituera une « règle plus spécifique » permettant d'assurer la protection des droits des employés conformément à l'article 88 (1) du RGPD. Cela signifie qu'un tel accord peut, dans certaines circonstances, fournir une sécurité juridique sur la façon dont Reveal peut être utilisée dans votre organisation.

Afin de respecter les obligations applicables pour les « règles plus spécifiques » conformément à l'article 88(1) du RGPD, l'accord doit être contraignant conformément au droit du travail local and doit intégrer de manière appropriée les intérêts en matière de protection des données à caractère personnel des employés (voir article 88(2) of the GDPR). En cas de doute, veuillez demander des conseils juridiques.

Utilisateurs du service en France
Selon l'art. L2312-38 du code français du travail, vous devez informer et consulter le Conseil Economique et Social avant de mettre en œuvre tout système ou moyen qui permet de surveiller l'activité des employés, comme le suivi de la géolocalisation.

Utilisateurs du service en Allemagne
Selon la section 87(6) de la loi sur l'organisation sociale des entreprises (*Bundesverfassungsgesetz - BetriebsVG*), le comité d'entreprise, s'il en existe un au sein de votre organisation, a le droit de co-déterminer l'introduction et l'utilisation de l'équipement technique destiné à surveiller le comportement ou les performances des employés. Le « contrôle » permanent du comportement et des performances des employés par l'intermédiaire de la surveillance n'est pas permis - si vous êtes l'employeur, vous êtes tenu d'exclure tout « contrôle » permanent des employés au moyen d'accords avec le comité d'entreprise ou de règlements unilatéralement contraignants.[19]

Section 26(4) de la Loi Fédérale sur la Protection des Données Personnelles prévoit explicitement que les traitements de données à caractère personnel peuvent être permis sur la base de conventions collectives ou d'accords d'entreprise si ces conventions collectives ou accords d'entreprise sont conformes aux exigences de l'article 88(2) du RGDP.

Utilisateurs du service en Italie
Vous pourriez être obligé de consulter le ou les syndicats de votre organisation, le cas échéant, ou d'obtenir l'autorisation du Bureau du travail compétent sur la mise en œuvre du service et votre utilisation des Données personnelles Reveal pour se conformer à l'art. 4(2) de la loi n° 300/1970 (Statuts du travailleur italien), sauf si les Données personnelles Reveal que vous traitez se limitent aux données strictement nécessaires au respect d'obligations légales.

Utilisateurs du service en Pologne
Vous devez exposer la finalité, le périmètre et les méthodes de surveillance dans votre Règlementation du travail (une politique interne obligatoire pour les employeurs ayant plus de 50 employés en Pologne) ou dans la Convention Collective de Travail de l'Entreprise. Si votre organisation compte des syndicats, les changements apportés à la Règlementation du travail ou à la Convention Collective de Travail de l'Entreprise

[19] Commissaire à la protection des données et à la liberté d'information Baden Württemberg, *Protection des données en matière d'emploi*, 2018 ; Centre indépendant pour la protection des données Schleswig-Holstein, Rapport d'activité 2017-2018, 103

demanderont une coopération avec les syndicats.

Tant que des employés existants sont concernés, vous devez les informer de votre intention de mettre en œuvre un système de surveillance. Cela doit être fait au plus tard deux semaines avant la mise en œuvre du système de surveillance.

Utilisateurs du service au Portugal
Selon l'art. 21 du code portugais du travail, vous devez informer et consulter le Comité d'entreprise (*Comissão de Trabalhadores*) avant de mettre en œuvre tout système ou moyen qui permet de surveiller l'activité des employés, comme le suivi de la géolocalisation.

Utilisateurs du service en Espagne
Selon l'art. 64(1) du Statut du travailleur espagnol, vous devrez informer les représentants des travailleurs avant la mise en œuvre de toute mesure qui pourrait affecter les travailleurs, ce qui s'entend comme incluant la mise en œuvre de dispositifs de géolocalisation ou de toute autre solution de surveillance.

À l'appui de ce qui précède, l'art. 90(2) de la loi organique 3/2018 du 5 décembre sur la protection des données à caractère personnel et l'attribution de droits numériques prévoit qu'avant la mise en œuvre de dispositifs de géolocalisation, les représentants des employés et des travailleurs doivent être informés de l'existence et des caractéristiques de ces dispositifs.

N. Atténuation du risque et protection des données dès la conception et par défaut

Vous devez vous assurer que toutes les mesures nécessaires pour atténuer les risques pour les personnes (tels qu'identifiés pendant le processus d'AIPD) et pour satisfaire aux exigences de « protection des données dès la conception et par défaut » ont été prises. La protection des données dès la conception signifie que les questions relatives à la vie privée doivent être prises en compte et traitées dès le commencement d'une activité de traitement de données (c'est-à-dire la phase de conception) et pendant la durée de vie de cette activité de traitement. La protection des données par défaut requiert que vous vous assuriez que le minimum de données nécessaire pour atteindre votre/vos objectif(s) est traité (par exemple, au lieu de permettre un accès large aux Données personnelles Reveal, l'accès doit être limité à des personnes spécifiques selon le principe du « besoin d'en connaitre ».

Les directives émises par les autorités de contrôle de la protection des données fournissent des exemples d'atténuation du risque dans le contexte de la télématique et de la surveillance des employés :

- Les conducteurs doivent être autorisés à désactiver temporairement le suivi de localisation dans certaines circonstances (par exemple, quand ils se rendent dans une clinique médicale), si les employés sont autorisés à faire un usage personnel des véhicules de l'organisation.[20]
- S'il existe un besoin de suivre la localisation d'un véhicule en-dehors des heures de travail d'un employé (par exemple, pour prévenir le vol de véhicule), la mise en œuvre doit être proportionnée aux risques, par exemple, la localisation du véhicule n'est pas enregistrée (ou visible pour vous) en-dehors des heures de travail sauf s'il quitte un cercle défini largement (par exemple, une région).[21]
- Le personnel ayant accès aux Données personnelles Reveal doit être limité. Le personnel doit être formé de façon adéquate et soumis à des obligations de confidentialité et de sécurité.[22] Déterminez quel personnel est le plus approprié pour avoir accès aux Données personnelles Reveal (cela pourrait ne pas être les supérieurs hiérarchiques par exemple).[23]

[20] Groupe de travail Article 29 *Avis 2/2017 sur le traitement des données sur le lieu de travail* (WP249), p. 20
[21] Groupe de travail Article 29 *Avis 2/2017 sur le traitement des données sur le lieu de travail* (WP249), p. 20
[22] Bureau du Commissaire à l'information, *Code des pratiques en matière d'emploi*, p. 67
[23] Bureau du Commissaire à l'information, Code des pratiques en matière d'emploi, p. 67

O. Désignation d'un Délégué à la protection des données (DPD/DPO)

Plusieurs facteurs entrainant la désignation d'un délégué à la protection des données (« DPO ») sont prévus par l'art. 37 du RGPD. Vos activités de traitement actuelles pourraient ne pas requérir que vous désigniez un DPO. Cependant, votre utilisation des services peut nécessiter que vous soyez obligé de désigner un DPO au regard de l'art. 37(1)(B), qui requiert de désigner un DPO si les activités de base d'une organisation consistent en un suivi régulier et systématique à grande échelle des personnes concernées. L'utilisation des services pour suivre les conducteurs et leurs comportements routiers est susceptible d'entrer dans le champ d'application de l'art. 37(1)(b), auquel cas vous serez tenu de désigner un DPO. D'autres dispositions du RGPD (art. 38 et 39) imposent des obligations quant à la fonction et aux missions du DPO - vous devrez également vous conformez à celles-ci si la désignation d'un DPO est requise.

Utilisateurs du service en Allemagne

Conformément à la section 38 de la loi fédérale sur la protection des données (BDSG), vous êtes tenu de désigner un DPO si vous employez de façon permanente au moins 20 personnes pour le traitement automatisé de données à caractère personnel ou si le traitement de données à caractère personnel que vous réalisez requiert que vous meniez une AIPD. Vous êtes susceptibles d'avoir besoin de désigner un DPO si vous utilisez les services en Allemagne.

Informations complémentaires

Législation

- Règlement général sur la protection des données (UE) 2016/679 (« RGPD »)
- Loi sur la protection des données 2018 (Royaume Uni)
- Loi 58/2019, 8 août 2019 (Portugal)
- Code du travail (Portugal)
- Loi constitutionnelle 3/2018, 5 décembre 2018, sur la protection des données à caractère personnel et la garantie de droits numériques (Espagne)
- Loi fédérale sur la protection des données (*Bundesdatenschutzgesets - BDSG*) 2018 (Allemagne)
- Loi sur l'organisation sociale des entreprises (*Bundesverfassungsgesetz -BetriebsVG*) (Allemagne)
- Décret législatif n° 196/2003 (Code italien sur la protection des données) (Italie)
- Loi n° 300/1970 (Statuts du travailleur italien) (Italie)
- Décret législatif n° 101/2018 (Italie)
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés – « Loi Informatique et Libertés »(France)
- Code français du travail (France)

Jurisprudence

South Lanarkshire Council v Scottish Information Commissioner [2013] UKSC 55 (Royaume Uni)

Lignes directrices réglementaires

UE

- Groupe de travail Article 29 *Avis 5/2005 sur l'utilisation des données de localisation en vue de fournir des services à valeur ajoutée* (WP115)

- Groupe de travail Article 29 *Avis 13/2011 sur les services de géolocalisation sur des dispositifs mobiles intelligents (WP 185)*
- Groupe de travail Article 29 *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679* (WP248)
- Groupe de travail Article 29 *Avis 2/2017 sur le traitement des données sur le lieu de travail* (WP249)
- Groupe de travail Article 29 *Avis* 2016/679 *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement* (WP251)
- Comité européen de la protection des données (CEPD), *Directives 2/2019 sur le traitement des données à caractère personnel aux termes de l'article 6(1)(b) du RGPD dans le contexte de la fourniture de services en ligne aux personnes concernées (version pour consultation publique)*

France

- Directives de la CNIL sur la géolocalisation des véhicules des salariés, 2018

Allemagne

- Commissaire à la protection des données et la liberté d'information Rhénanie-Palatinat, *Sur la légalité d'un suivi GPS des employés*
- Commissaire à la protection des données et la liberté d'information Baden-Württemberg, *Protection des données en matière d'emploi* 2018
- Conférence sur la protection des données des autorités fédérales et étatiques (*Länder*) chargées de la protection des données (*Datenschutzkonferenz - DSK*), bref exposé n° 14 : *Protection des données en matière d'emploi* (17 décembre 2018)
- Commissaire bavarois à la protection des données, *27e Rapport d'activité* 2016
- Conférence sur la protection des données des autorités fédérales et étatiques (*Länder*) chargées de la protection des données (*Datenschutzkonferenz - DSK*), bref exposé n° 17 : Catégories particulières de données à caractère personnel (27 mars 2018)
- Conférence sur la protection des données des autorités fédérales et étatiques (*Länder*) chargées de la protection des données (*Datenschutzkonferenz - DSK*), bref exposé n° 19 : *Information et engagement des employés à se conformer aux exigences de protection des données selon le RGPD* (29 mai 2018)
- Commissaire à la protection des données et la liberté d'information Rhénanie-du-Nord-Westphalie (LDi NRW), 24e Rapport sur la protection des données et la liberté d'information 2017-2018, *Positionnement par satellite pour déterminer la position des véhicule de société - pas un moyen admissible pour surveiller les employés*
- Commissaire berlinois à la protection des données et la confidentialité, liberté d'information, *Rapport annuel 2018*
- Centre indépendant pour la protection des données Schleswig-Holstein, Rapport d'activité 2017-2018
- Le Commissaire à la protection des données Basse Saxe, 24e Rapport d'activité 2017-2018, *Surveillance par GPS des véhicules de société*

Pologne

- Bureau de protection des données, *Protection des données sur le lieu de travail. Directives pour les employeurs*

Portugal

- Délibération du CNPD 7680/2014 (Directive sur l'utilisation de la géolocalisation dans le contexte de l'emploi).

<u>Royaume Uni</u>

- Bureau du Commissaire à l'information, *Code des pratiques en matière d'emploi* et *Orientations supplémentaires*

Liste de contrôle du RGPD

Article du RGDPR	Sujet	Pertinence par rapport à Reveal	Référence dans le eBook
Art. 1, 2 ou 3	Objet et objectifs ; champ d'application matériel ; et champ d'application territorial	Aucune pertinence particulière	N/A
Art. 4	Définitions	Définit les notions de « données à caractère personnel » et de « catégories particulières » de données à caractère personnel	« Questions fréquemment posées sur Reveal », sections 3 et 4
Art. 5	Principes et « *accountability* » c'est-à-dire responsabilité	Le traitement des Données personnelles Reveal doit être conforme aux principes de protection des données à caractère personnel et le Responsable du traitement doit être en mesure de démontrer cette conformité	« *Aborder les exigences de protection des données à caractère personnel* », en général
Art. 6 et 7	Licéité du traitement et conditions applicables au consentement	Une base juridique doit exister pour chaque finalité du traitement des Données personnelles Reveal	« *Aborder les exigences en matière de protection des données à caractère personnel* », section E
Art. 8	Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information	Aucune pertinence particulière	N/A
Art. 9 et 10	Traitement portant sur des catégories particulières de données à caractère personnel et sur des données à caractère personnel relatives aux condamnations pénales et aux infractions	Une condition doit exister pour chaque finalité de traitement des Données personnelles Reveal, quand les données à caractère personnel sont des données de catégorie particulières de données à caractère personnelle ou des données à caractère personnel relatives aux condamnations pénales	« *Questions fréquemment posées sur Reveal* », section 4, et « *Aborder les exigences en matière de protection des données à caractère personnel* », section E

		et aux infractions	
Art. 11	Traitement ne nécessitant pas l'identification	Aucune pertinence particulière	N/A
Art. 12	Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée	Toute information fournie aux personnes dont les Données personnelles Reveal sont traitées doit être concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.	« *Aborder les exigences de protection des données* à caractère personnel», sections B et J
Art. 13 et 14	Informations à fournir à la personne concernée	Une information sur la protection des données doit être fournie aux personnes dont les Données personnelles Reveal sont traitées	« *Aborder les exigences de protection des données* », section B
Art. 15	Droit d'accès	Un accès aux Données personnelles Reveal doit être fourni aux personnes sur demande (sauf exceptions)	« *Aborder les exigences de protection des données* », section J
Art. 16	Droit à rectification	Les Données personnelles Reveal doivent être rectifiées sur demande des personnes concernées	« *Aborder les exigences de protection des données* », section J
Art. 17	Droit à l'effacement	Les Données personnelles Reveal doivent être effacées sur demande des personnes concernées, si le droit s'applique	« *Aborder les exigences de protection des données* », section J
Art. 18	Droit à la limitation	Le traitement des Données personnelles Reveal doivent être limitées sur demande des personnes concernées, si le droit s'applique	« *Aborder les exigences de protection des données* », section J
Art. 19	Obligation de notification en ce qui concerne la rectification, l'effacement ou la limitation	Si une demande de rectification, d'effacement ou de limitation relative aux Données personnelles Reveal est reçue, les tiers à qui les données	« *Aborder les exigences de protection des données* », section J

		ont été communiquées doivent être informés de la demande	
Art. 20	Droit à la portabilité des données	Les Données personnelles Reveal doivent être transférées aux personnes concernées (ou à des tiers désignés) sur demande des personnes concernées, si le droit s'applique	« *Aborder les exigences de protection des données* », section J
Art. 21	Droit d'opposition	Les Données personnelles Reveal ne doivent plus être traitées sur demande des personnes concernées, si le droit s'applique	« *Aborder les exigences de protection des données* », section J
Art. 22	Décision individuelle automatisée, y compris le profilage	Les décisions prises exclusivement sur un traitement automatisé concernant les personnes, qui produisent des effets juridiques les concernant ou les affectant de manière significative de façon similaire ne peuvent être prises que conformément à l'art. 22	« *Aborder les exigences de protection des données* », section L
Art. 23	Limitations	Aucune pertinence particulière	N/A
Art. 24	Responsabilité du responsable du traitement	Des mesures techniques et organisationnelles appropriées doivent être mises en œuvre pour s'assurer (et démontrer) que le traitement est réalisé en conformité avec le RGPD	« *Aborder les exigences de protection des données* », en général
Art. 25	Protection des données dès la conception et protection des données par défaut	Les questions relatives à la protection des données à caractère personnel doivent être traitées dès le début et	« *Aborder les exigences de protection des données* », sections F et N

		pendant la durée de vie du traitement des Données personnelles Reveal et le minimum de données à caractère personnel nécessaire pour atteindre votre objectif doit être traité.	
Art. 26	Responsables conjoints du traitement	Aucune pertinence particulière	N/A
Art. 27	Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union	Aucune pertinence particulière	N/A
Art. 28	Sous-traitant	Seuls les sous-traitants présentant des garanties suffisantes doivent être recrutés pour traiter des Données personnelles Reveal et des obligations doivent être imposées aux sous-traitants par un contrat	« *Aborder les exigences de protection des données* », section I
Art. 29	Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant	Aucune pertinence particulière	N/A
Art. 30	Registre des activités de traitement	Le traitement des Données personnelles Reveal doit figurer dans le registre des activités de traitement	« *Aborder les exigences de protection des données* », section C
Art. 31	Coopération avec l'autorité de contrôle	Aucune pertinence particulière	N/A
Art. 32	Sécurité du traitement	Des mesures techniques et organisationnelles appropriées doivent être mises en œuvre pour protéger la sécurité des Données personnelles Reveal	« *Aborder les exigences de protection des données* », section I
Art. 33 et 34	Notification d'une violation de données (à l'autorité de contrôle et à la personne concernée)	Dans le cas d'une violation de données à caractère personnel impliquant les Données personnelles Reveal, une notification doit être faite aux autorités	« *Aborder les exigences de protection des données* », section I

		de contrôle et aux personnes affectées si des conditions sont remplies	
Art. 35 et 36	Analyse d'impact relative à la protection des données et consultation préalable	Une analyse d'impact relative à la protection des données doit être effectuée pour traiter des Données personnelles Reveal et une consultation des autorités de contrôle peut être requise si le traitement présente des risques élevés et non atténué pour les personnes concernées	« *Aborder les exigences de protection des données* », section A
Art. 37, 38 et 39	Délégué à la protection des données	Un délégué à la protection des données doit être désigné si les activités de base du responsable du traitement consistent en un suivi « régulier et systématique » à grande échelle des personnes concernées ou au traitement à grande échelle de données de catégorie particulière de données ou de données à caractère personnel relatives à des condamnations pénales et des infractions	« *Aborder les exigences de protection des données* », section Q
Art. 40, 41, 42 et 43	Codes de conduite, certification et accréditation	Aucune pertinence particulière	N/A
Art. 44 - 50	Transferts	Tout transfert de Données personnelles Reveal hors de l'EEE vers des pays qui ne sont pas « adéquats » (par exemple, vers d'autres fournisseurs de plateforme ou des sociétés d'un groupe) ne doit être réalisé que si un mécanisme de transfert est en place ou	« *Questions fréquemment posées sur Reveal* », section 6, et « *Aborder les exigences de protection des données* », section K

		si une dérogation existe	
Art. 51 - 59	Autorité de contrôle et compétence, missions et pouvoirs, et rapports d'activité	Aucune pertinence particulière	N/A
Art. 60 - 67	Coopération et cohérence	Aucune pertinence particulière	N/A
Art. 68 - 76	Comité européen de la protection des données	Aucune pertinence particulière	N/A
Art. 77	Droit d'introduire une réclamation auprès d'une autorité de contrôle	Aucune pertinence particulière	N/A
Art. 78	Droit à un recours juridictionnel effectif contre une autorité de contrôle	Aucune pertinence particulière	N/A
Art. 79 - 82	Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant, et droit à réparation	Aucune pertinence particulière	N/A
Art. 83 - 84	Amendes administratives et sanctions	Aucune pertinence particulière	N/A
Art. 85 - 91	Dispositions relatives à des situations particulières de traitement	Aucune pertinence particulière	N/A
Art. 92 - 93	Actes délégués et actes d'exécution	Aucune pertinence particulière	N/A
Art. 94 - 99	Dispositions finales	Aucune pertinence particulière	N/A