Introducción

Movildata proporciona Soluciones para Equipos de Trabajo Móviles en el entorno de Gestión de Flotas y Gestión de Servicios de Campo. Nuestros Productos supervisan el rendimiento de su flota de vehículos, rendimiento que puede tener un gran impacto en su negocio. Se trata de información sobre el lugar donde se encuentran sus vehículos, cómo se comportan sus conductores en la carretera y cuánto combustible utilizan. Esta información se introduce a continuación en paneles de control asimilables para que pueda actuar con rapidez. Reveal es una herramienta fundamental para ayudarle a hacer más en menos tiempo, proporcionar un mejor servicio al cliente y, en última instancia, mejorar los resultados en toda su empresa. A través de nuestros productos de Servicio de Campo también tenemos la capacidad de gestionar todo el ciclo de vida de las solicitudes de servicio de nuestros clientes, desde el primer contacto con el cliente, mediante la entrega de un presupuesto para el trabajo, la programación del trabajo, el envío, la ruta óptima de un conductor y la aceptación del pago.

El presente eBook responde a las preguntas más frecuentes sobre los Servicios de Seguimiento de Flotas de Reveal ("los servicios" o "Reveal") que Movildata le vende en la plataforma Reveal, y presenta una visión general de algunas de las consideraciones y requisitos fundamentales de protección de datos que deberá tener en cuenta antes, durante y después de la implementación del servicio. Aunque este eBook se centra principalmente en cuestiones de protección de datos, deberá tener en cuenta la posibilidad de que otros requisitos legales relevantes afecten a su implementación y al uso de los servicios. Por ejemplo, en algunos países el uso de los servicios en vehículos conducidos por empleados activará determinados requisitos desde un punto de vista de la legislación laboral.

Cuando ha procedido, hemos hecho referencia a las directrices normativas disponibles en el momento de la publicación. Los reguladores examinan y revisan periódicamente sus directrices; por ello, deberá estar atento a la evolución en este sentido, ya que, en última instancia, será responsabilidad suya, como Responsable del Tratamiento de los datos personales recogidos y utilizados a través del servicio, garantizar el cumplimiento de la legislación aplicable.

La información proporcionada en este eBook no constituye asesoramiento legal o profesional alguno. Deberá consultar en todo momento a un abogado debidamente cualificado ante cualquier problema o cuestión legal específica. Movildata no asume ni aceptará responsabilidad alguna por la información contenida en este eBook.

Preguntas Frecuentes sobre Reveal

1. ¿De quién es la información que se recoge a través de los servicios?
Principalmente, se recogerá información sobre los empleados y contratistas que conducen los vehículos en los que usted presta los servicios. También se puede recoger información sobre otras personas (por ejemplo, pasajeros u otras personas del entorno familiar de un conductor con acceso al vehículo), dependiendo de cómo y por qué se implemente el servicio.

2. ¿Cómo se recoge la información para el servicio?
El servicio recoge información de dos fuentes:

- El dispositivo de a bordo instalado en sus vehículos: Este dispositivo recoge información sobre las ubicaciones y actividades de sus vehículos. Si usted conoce (o podría determinar) el conductor al que está asignado cada vehículo, esta información también será considerada como datos personales.
- Tenemos varias aplicaciones móviles en nuestras plataformas que puede instalar para utilizar nuestro servicio de forma efectiva, tales como nuestras aplicaciones relacionadas con el Servicio de Campo (Work, Workforce, Field) y nuestras aplicaciones relacionadas con la Gestión de Flotas (Manager\Spotlight, Video, ELD). Para utilizar la aplicación, cada conductor deberá proporcionar determinada información durante el proceso de registro.

En este eBook hacemos referencia de forma colectiva a cualquier dato personal recogido a través del servicio como "Datos Personales de Reveal".

3. ¿Qué datos personales se recogen a través del servicio?
Usted determinará la mayoría de los datos personales que se recogerán a través del servicio. Lo que desee recoger variará en función de cómo y por qué implementa la solución. Usted tiene el control total del tipo de datos que recoge. En este sentido, será su responsabilidad legal asegurarse de que los datos que recoge son necesarios para poder utilizar el servicio.
Los datos personales recogidos a través del dispositivo de a bordo del vehículo pueden incluir:

- Datos de localización (GPS) de vehículos y personas;
- Información sobre tacógrafos (tiempos de conducción);
- Velocidad y comportamiento del conductor del vehículo;
- Datos de eventos del vehículo (por ejemplo, implicación en un accidente, entrada o salida de un área geo-cercada (geofencing));
- Otra información sobre el vehículo (por ejemplo, consumo de combustible, presión de los neumáticos, datos de funcionamiento).

Los datos personales recogidos a través de la aplicación pueden incluir:

- Nombre del conductor;
- Número de teléfono, dirección de correo electrónico y domicilio del conductor;
- Credenciales de inicio de sesión del conductor;
- Registros del conductor (por ejemplo, asignación del vehículo, número de conductor, ubicaciones de las zonas cercadas (geofence);
- Geolocalización GPS.

4. ¿Se recoge a través de Reveal categorías especiales de datos o sobre infracciones penales?
Según las leyes de protección de datos, las categorías especiales de datos están formadas por los datos relacionados con la raza, el origen étnico, las opiniones políticas, la religión, la pertenencia a un sindicato, la genética, la biometría (cuando se utiliza con fines de identificación), la salud, la vida sexual y la orientación sexual. Junto con la información sobre infracciones penales, el tratamiento de esta información es más restringido.

A través del servicio no se solicitan categorías especiales de datos ni información sobre infracciones penales (por ejemplo, no se pide a los conductores que incluyan ninguna información de esta naturaleza en la aplicación). Aunque pueden deducirse datos de categorías especiales a partir de la información de localización (por ejemplo, la información de geolocalización puede identificar que un conductor visita regularmente un centro religioso o médico en particular), esto no activa los requisitos del RGPD relacionados con el tratamiento de categorías especiales de datos, a menos que la información de localización se utilice, de hecho, para deducir este tipo de datos. Sin embargo, dependiendo de la forma y los motivos por los que se implemente el servicio, a partir de la información recogida, podría tratarse información sobre (presuntas) infracciones penales (por ejemplo, la información sobre la actividad del vehículo podría indicar que un conductor ha superado un límite de velocidad).

Los elementos constitutivos un delito varían de un país a otro, al igual que la categorización de la información como "categoría especial" o información sobre infracciones penales. En el supuesto de que los datos que se recojan pudieran ser considerados información sobre infracciones penales, de acuerdo con la(s) ley(es) de protección de datos, tendrá obligaciones adicionales establecidas por el RGPD y por la legislación nacional como Responsable del Tratamiento.

5. ¿Quién tiene acceso a los Datos Personales de Reveal?
Los Datos Personales de Reveal tratados en el curso de la prestación del servicio están disponibles para los correspondientes empleados de Verizon en función de la "necesidad de saber". Los Datos Personales de Reveal también se ponen a disposición de empresas de terceros que brindan servicios a Verizon, para permitir que Verizon administre el servicio (por ejemplo, terceros que prestan servicios de hosting). Verizon también puede comunicar Datos Personales de Reveal a terceros cuando así lo exija la ley (por ejemplo, a los órganos encargados de hacer cumplir la ley).

Además de las finalidades descritas anteriormente, usted puede optar por comunicar Datos Personales de Reveal para sus propias finalidades. Las personas que, dentro de su organización, deberían tener acceso a

Datos Personales de Reveal serán designadas por usted (por ejemplo, tendrá que asignar administradores que puedan acceder al portal online para ver en tiempo real la ubicación del vehículo y la información de actividad). También puede optar por compartir los Datos Personales de Reveal con terceros, como pueden ser otras empresas dentro de su grupo societario, u otros proveedores de plataformas (por ejemplo, cuando otra plataforma interactúe con Reveal).

6. ¿Verizon transfiere Datos Personales de Reveal fuera del Espacio Económico Europeo (EEE)?
Verizon aloja Datos Personales de Reveal en centros de datos ubicados tanto dentro como fuera del EEE. Podrá encontrar un listado de esos países en el siguiente enlace: https://www.verizon.com/about/privacy/data-processing-activities. Cuando Verizon transfiere Datos Personales de Reveal fuera del EEE dentro del grupo Verizon, estas transferencias se realizan de acuerdo con las Normas Corporativas Vinculantes para Responsables y Encargados aprobadas por la UE.

7. ¿Cuánto tiempo conserva Verizon los Datos Personales de Reveal?
Los Datos Personales de Reveal serán guardados durante el tiempo acordado en los términos del contrato y de acuerdo con las configuraciones de retención que usted seleccione dentro del producto. Esto variará dependiendo de los requisitos legales de conservación de datos que le apliquen, o de cualquier requisito de información que pueda solicitar. Como Responsable del Tratamiento, será su responsabilidad asegurarse de que conoce el tiempo durante el cual tiene obligación legal de conservar los Datos Personales de Reveal. Una vez finalizados los servicios, Movildata suprimirá de forma segura los Datos Personales de Reveal.

8. ¿Verizon utiliza Datos Personales de Reveal para sus propias finalidades?
Verizon recoge los Datos Personales de Reveal para proporcionarle el servicio Reveal que usted ha solicitado a Reveal. En este caso, Verizon será considerado como Encargado del Tratamiento.

En la medida legalmente permitida, Verizon hace un uso secundario de la información anonimizada recogida a través de Reveal para sus propias finalidades y para mejorar los productos y servicios. Lo anterior incluye análisis para optimizar la solución Reveal y comunicaciones a compañías de seguros. Ninguna persona física o jurídica que utilice Reveal podrá ser identificada a partir de la información anonimizada.

9. ¿Cómo se asegura Verizon de que los Datos Personales de Reveal se mantengan seguros?
Consulte el Documento sobre Seguridad de la Información de los Sistemas Internos de Verizon para obtener una descripción de las medidas de seguridad técnicas y organizativas que Verizon implementa para cumplir con sus obligaciones al amparo del RGPD, en https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit.

Requisitos de Protección de Datos

Esta sección explica cómo se aplican los requisitos de protección de datos al uso que hace de Reveal.

Al final de esta sección hemos incluido una listado de los Artículos del Reglamento General de Protección de Datos y de su referencia en este eBook. Esto le permitirá comprobar cuando una disposición concreta en el RGPD es relevante para Reveal y dónde se trata en este eBook. También hemos incluido una lista de fuentes de información adicional.

A. Evaluación de Impacto Relativa a la Protección de Datos

Una evaluación de impacto relativa a la protección de datos ("EIPD") es un proceso que se realiza para describir y evaluar el tratamiento de datos personales y para identificar y gestionar los riesgos que el tratamiento de datos supone para las personas físicas.

En conjunto, las autoridades de control de protección de datos consideran que las EIPD deben realizarse

cuando una organización trate datos personales con el fin de evaluar el rendimiento, la ubicación o el desplazamiento de los empleados[1]. Es probable que el uso del servicio requiera realícela realización de una EIPD por su parte, si bien cada autoridad de control ha publicado sus propios criterios de EIPD. Deberá consultar los criterios de su autoridad de control competente para identificar si se requiere una EIPD.

Su EIPD debería:

- Describir qué tipo de tratamiento de Datos Personales de Reveal se llevará a cabo;
    - La información contenida en este eBook sobre qué datos se recogen, cómo se recogen y cómo se tratan le será de ayuda en este sentido.
- Las finalidades del tratamiento - y, en caso de que se use el servicio amparado en su interés legítimo como base de legitimación, cuál es dicho interés
- Evaluar si el tratamiento es una forma necesaria y proporcionada de cumplir estas finalidades;
    - Esto significa valorar si es razonablemente posible cumplir las finalidades de otra manera que implique un menor tratamiento de datos personales.
    - Por ejemplo, si una empresa desea hacer un seguimiento de las horas trabajadas por una persona, ¿podría hacerlo mediante un proceso alternativo en lugar de hacer un seguimiento de su paradero a lo largo de todo el turno, ya que esto sería claramente desproporcionado?
- Evaluar los riesgos que presenta el tratamiento para los interesados y cómo se pueden mitigar estos riesgos;
    - Por ejemplo, si se permite que un empleado haga un uso privado de un vehículo, realizar un seguimiento del vehículo mientras el empleado no está trabajando sería intrusivo e innecesario para las finalidades del empleador. Este riesgo podría mitigarse permitiendo al empleado desactivar el servicio fuera de las horas de trabajo habilitando el "Privacy Switch" ("interruptor de privacidad") disponible y asegurándose de que los empleados estén al tanto de esta opción.
- Describir las medidas de seguridad; y
- Describir el resto de medidas que garanticen la protección de los datos personales y demostrar su cumplimiento.
    - La EIPD debe abordar el resto de temas establecidos en este eBook.
    - En concreto, la EIPD debería establecer cómo se respetan los derechos de los interesados.

Durante el proceso de elaboración de la EIPD, deberá consultar a su Delegado de Protección de Datos (si dispone de uno). Si procede, también deberá consultar a las personas cuyos datos vaya a ser tratados, o a sus representantes -por ejemplo, a través de Consulta a los Empleados, a los Sindicatos o al Comité de Empresa- y reflejar el resultado de esta consulta en la EIPD.

Si su EIPD llega a la conclusión de que el uso de Datos Personales de Reveal para las finalidades previstas supone un riesgo elevado y absoluto para los interesados, deberá realizar una consulta a su autoridad de control competente (en el Reino Unido, se trata de la Oficina del Comisionado de Información).

Deberá revisar periódicamente toda EIPD que realice, así como evaluar cada cierto tiempo la implementación del servicio y el uso de Datos Personales de Reveal frente a la misma.

B. Aviso de Privacidad

Al igual que con todo el tratamiento de datos personales que realice, está obligado a asegurarse de que proporciona a los interesados información clara y completa sobre la recogida y tratamiento de sus Datos Personales de Reveal.

Esta sección describe la información que debe incluir en su aviso de privacidad para cumplir con los requisitos de protección de datos. No obstante, deberá valorar si algún otro requisito legal relevante va a afectar al contenido de su aviso de privacidad y a la forma en la que implementa el servicio. Por ejemplo, en algunos países las leyes laborales requieren que se incluya información adicional en el aviso de privacidad u otros

[1] *Directrices del GT29 sobre la Evaluación de Impacto relativa a la Protección de Datos (EIPD) y para determinar si es "el tratamiento entraña probablemente un alto riesgo" a efectos del Reglamento 2016/679* (GT248), p.10

documentos internos.

El RGPD requiere que se incluya la siguiente información en el aviso de privacidad:

- Su identidad y datos de contacto (y los de su delegado de protección de datos, si ha designado uno);
- Las finalidades y bases de legitimación del tratamiento (y, en el caso de que trate los Datos Personales de Reveal para satisfacer sus "intereses legítimos", cuáles son dichos intereses);
    - Las secciones sobre finalidades y bases de legitimación en este eBook le ayudarán a valorarlos y describirlos.
- Las categorías de Datos Personales de Reveal tratados (y las fuentes), cuando no se hayan obtenido directamente del interesado;
    - La sección 3 anterior sobre "Qué datos personales se recogen a través del servicio" le ayudará a describirlo.
- Los destinatarios de los Datos Personales de Reveal, y los países no pertenecientes al EEE a los que se transfieren los Datos Personales de Reveal (junto con una descripción de las medidas de seguridad establecidas);
- El plazo de conservación de los Datos Personales de Reveal;
- Si la provisión de cualesquiera Datos Personales de Reveal es obligatoria, y las posibles consecuencias de la falta de suministro de dichos datos;
- La existencia de cualquier tratamiento basado en decisiones automatizadas sobre personas físicas (incluida la elaboración de perfiles), junto con información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado;
- Una descripción de los derechos de los interesados (incluido el derecho a revocar el consentimiento, cuando trate Datos Personales de Reveal en los casos en que el interesado haya dado su consentimiento) y la posibilidad de presentar una reclamación ante una autoridad de control.

El aviso de privacidad proporcionado también deberá cumplir con requisitos adicionales conforme al Art. 12 del RGPD (por ejemplo, que la información proporcionada a los interesados sea concisa, transparente, inteligible y de fácil acceso, y en un lenguaje claro y sencillo).

Usuarios del servicio en Francia
Además de los requisitos del RGPD mencionados anteriormente, la Ley de Protección de Datos francesa le exige se informe a los interesados sobre su derecho a definir las directrices relativas al tratamiento de sus datos personales después de su fallecimiento.

Aviso en el vehículo

Dado que la recogida de Datos Personales de Reveal es un tipo de recogida de datos poco visible para los interesados, pero que puede tener consecuencias significativas, deberá hacer un esfuerzo especial para llamar la atención de los conductores sobre el uso del servicio. Además del detallado aviso de privacidad descrito anteriormente, las directrices normativas establecen que también deberá informar claramente a los conductores de que se ha instalado un dispositivo de seguimiento en el vehículo que están conduciendo y de que se está realizando un seguimiento de sus movimientos (y de su comportamiento al volante, en caso de que se cuente con la tecnología correspondiente). Lo ideal es que esta información se muestre de forma destacada en cada uno de los correspondientes vehículos, a la vista del conductor.[2]

Usuarios del servicio en Polonia
Además del contenido mencionado anteriormente, cuando la utilización del servicio sea equivalente a la supervisión de los empleados, la notificación a bordo del vehículo deberá, asimismo, indicar:

- Qué datos se recogen y registran;
- Dónde y durante cuánto tiempo se almacenan estos datos; y
- Quién tiene acceso a los datos[3].

[2] *Dictamen 2/2017 del* GT29 *sobre tratamiento de datos en el trabajo* (GT249), p.20

[3] Oficina de Protección de Datos (Polonia), *Protección de datos en el centro de trabajo. Directrices para empleadores,* p. 37

Cumplimiento de Políticas

Si los Datos Personales de Reveal se utilizan para hacer cumplir sus normas y principios, deberá asegurarse de que dicho uso es legal, así como de que los empleados conocen las correspondientes normas y deberá controlar si se cumplen, a través del servicio.

C. Registro de Actividades de Tratamiento

Como Responsable del Tratamiento de Datos, deberá mantener un Registro de las Actividades de Tratamiento ("RAT"), conforme se establece en el artículo 30 del RGPD. Tendrá que asegurarse de que su RAT cubre el tratamiento de los Datos Personales de Reveal. Necesitará incluir información relativa a:

- Nombre y datos de contacto de su organización (y, en su caso, nombre y datos de contacto de su delegado de protección de datos, representante y/o Corresponsable del Tratamiento);
- La finalidad para la que se tratan los Datos Personales de Reveal;
- Descripción de las categorías de Datos Personales de Reveal y de las categorías de personas cuyos datos se tratan;
    - La Sección 3 anterior sobre "¿Qué datos personales se recogen a través del servicio?" le ayudará a completarlo.
- Las categorías de destinatarios a los que se comunicarán los Datos Personales de Reveal;
    - - La Sección 5 anterior sobre "Quién tiene acceso a los Datos Personales de Reveal" le ayudará a completarlo. También debe enumerar los destinatarios a los que da acceso a los Datos Personales de Reveal.
- Transferencias de Datos Personales de Reveal a países fuera del EEE;
    - La Sección 6 anterior sobre "¿Verizon transfiere Datos Personales de Reveal fuera del Espacio Económico Europeo (EEE)?" explica dónde se transfieren los datos y qué medidas de seguridad se utilizan para proteger los Datos Personales de Reveal.
- Plazos de conservación;
    - La Sección 7 anterior sobre "¿Cuánto tiempo Verizon conserva los Datos Personales de Reveal?" lo explica.
- Información sobre las medidas de seguridad, siempre que sea posible.
    - Consulte el Documento sobre Seguridad de la Información de los Sistemas Internos de Verizon para obtener una descripción de las medidas de seguridad técnicas y organizativas que Verizon implementa para cumplir con sus obligaciones al amparo del RGPD en la siguiente dirección url: https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit.

Verizon tiene a su disposición información para ayudarle con esta obligación en el siguiente enlace: https://www.verizon.com/about/privacy/data-processing-activities.

Usuarios del servicio en el Reino Unido
Si trata datos de infracciones penales y su base de legitimación para el tratamiento es una de las condiciones establecidas en el Anexo 1 de la Ley de Protección de Datos de 2018, deberá incorporar columnas adicionales en el RAT (relacionadas con la base de legitimación y las condiciones del tratamiento, y la retención/supresión de los correspondientes datos de acuerdo con su Documento de Política Apropiado, si fuera necesario).

D. Finalidades

Deberá identificar las finalidades para los que desea implementar el servicio y utilizar Datos Personales de Reveal, por ejemplo:

- Detección y prevención de la pérdida de bienes de su organización;
- Mejora de la productividad de los empleados;
- Optimización de rutas y recursos, y ahorro de combustible;
- Suministro a sus clientes de información de seguimiento en tiempo real;
- Garantía de la seguridad de sus empleados, por ejemplo, asegurando que se respeten las pausas para descansar y comer.

Es importante que tenga claras las finalidades para los que se implementa el servicio desde el principio.

- Usted necesita una "base de legitimación" para cada una de las finalidades para las que trata los Datos Personales de Reveal;
- Debe asegurarse de que no trata más Datos Personales de Reveal de lo que sea razonablemente necesario para este fin;
- Tiene que informar a los interesados cuáles son estas finalidades.

Una vez que haya recogido los Datos Personales de Reveal para estas finalidades, solamente podrá utilizarlos con estas finalidades o para otras que sean compatibles con las mismas. En ocasiones la ley aplicable permite excepciones a este principio.

Usuarios del servicio en Francia

Los dispositivos de geolocalización sólo pueden instalarse en vehículos utilizados por los empleados para las siguientes finalidades[4]:

- Seguimiento, justificación y facturación de los servicios de transporte de viajeros;
- Garantía de la seguridad de los empleados, mercancías y vehículos (en concreto, la localización de vehículos robados);
- Optimización de la asignación de recursos cuando los servicios se presten en amplias zonas geográficas, en particular en el contexto de servicios de emergencia;
- Seguimiento del tiempo de trabajo (pero únicamente cuando no se disponga de métodos alternativos de seguimiento del tiempo de trabajo);
- Cumplimiento de las obligaciones legales o reglamentarias;
- Aseguramiento de que se respetan las normas del empleador en relación con el uso de los vehículos de trabajo.

Por el contrario, se prohíbe el uso de un dispositivo de geolocalización instalado en los vehículos de empleados[5]:

- Para controlar el cumplimiento de los límites de velocidad;
- Para el seguimiento permanente de los empleados;
- Para el seguimiento del tiempo de trabajo, cuando se disponga de métodos alternativos;
- En el vehículo de un empleado con libertad para organizar sus funciones (por ejemplo, un representante de ventas);
- Para el seguimiento del uso privado del vehículo cuando se permita el uso privado (por ejemplo, durante las pausas o por parte de empleados con libertad de organización de sus viajes); o
- Para el seguimiento de los representantes sindicales o similares que actúen en el ámbito de sus funciones.

Usuarios del servicio en Alemania

Por lo general, no se permiten los sistemas de seguimiento a través de los cuales los empleados pueden ser supervisados permanentemente[6]

Usuarios del servicio en Polonia

En el caso y en la medida en que la implementación del servicio constituya un seguimiento de los empleados, las organizaciones sólo podrán tratar los Datos Personales de Reveal con la finalidad de "garantizar que los empleados hagan un uso eficaz de su tiempo de trabajo y un uso adecuado de sus equipos y herramientas". La autoridad de control polaca sugiere que esta finalidad es bastante amplia y puede permitirse para:

- Localización de un vehículo en caso de robo;
- Investigar la responsabilidad de un empleado por daños a un vehículo; o
- Optimización de rutas y recursos, y ahorro de combustible.

Usuarios del servicio en Portugal

[4] Directrices de la CNIL sobre la geolocalización de los vehículos de los empleados, 2018

[5] Directrices de la CNIL sobre la geolocalización de los vehículos de los empleados, 2018

[6] *Comisario de Protección de Datos y Libertad de Información de Renania-Palatinado, Sobre la legalidad del seguimiento por GPS de los empleados*; *Comisario de Protección de Datos y Libertad de Información de Baden-Württemberg, Protección de datos en el empleo 2018*, 2018, pp. 36- 37

Los servicios no pueden utilizarse para controlar el comportamiento de los empleados, y sólo pueden utilizarse en vehículos utilizados por los empleados para las siguientes finalidades permitidas[7]:

- **Gestión de flotas donde se prestan servicios externos:**
  - Servicios de asistencia técnica;
  - Distribución de mercancías;
  - Transporte de pasajeros;
  - Transporte de mercancías; y
  - Seguridad privada.

- **Protección de bienes**:
  - Transporte de mercancías peligrosas; y
  - Transporte de materiales de alto valor.

Cuando los servicios se implementen de forma específica para geolocalizar vehículos operados por empleados en caso de robo, el empleador no podrá acceder a los datos de geolocalización recogidos hasta, y a menos, que el vehículo sea robado. Podrán recogerse otros datos del vehículo (como la velocidad media, la frenada o el consumo de combustible), pero no se vincularán a ningún dato personal que permita identificar al conductor.

E. Bases de Legitimación

Deberá identificar una base de legitimación en virtud del Art. 6 RGPD para cada una de las finalidades para las que se utilizan los Datos Personales de Reveal. Dependiendo de su situación, es posible que esté utilizando Datos Personales de Reveal porque es necesario para:

- **Cumplir con una obligación legal**: por ejemplo, si tiene la obligación legal de controlar el uso y las horas de conducción de los vehículos mediante la instalación de un tacógrafo en un vehículo;
- **Cumplir un contrato con el interesado**: por ejemplo, cuando una conducción correcta sea una condición de empleo;
- **Perseguir un fin que satisfaga sus intereses legítimos**: por ejemplo, mantener a sus conductores (y a otros usuarios de la carretera) seguros, hacer cumplir buenos hábitos de conducción, controlar la flota, mejorar la eficiencia del combustible y el mantenimiento, defenderse frente a accidentes y acusaciones falsas, garantizar la salud y la seguridad del personal y ayudar en relación con primas de seguros.

Es imprescindible que se asegure de que tiene una base de legitimación para tratar los datos y que puede justificarlo ante una Autoridad de Control de Protección de Datos según sea necesario.

Deberá demostrar que su tratamiento de los Datos Personales de Reveal es "necesario". "Necesario" significa que el tratamiento de los Datos Personales de Reveal debe ser una forma específica y proporcionada de alcanzar sus finalidades; el tratamiento debe ser "más que deseable, pero menos que indispensable o absolutamente necesario"[8]. Su valoración debe basarse en hechos, teniendo en cuenta el objetivo perseguido y cualquier otra opción menos intrusiva para lograr el mismo fin. Si existen alternativas realistas y menos intrusivas, entonces el tratamiento no es "necesario"[9].

Si se basa en intereses legítimos, tendrá que llevar a cabo y documentar una "evaluación de interés legítimo" para asegurarse de que sobre sus intereses legítimos no prevalezcan los intereses, derechos y libertades de los interesados. El tratamiento debe ser necesario a tal fin (es decir, proporcional a las necesidades de la empresa) y deben incluirse medidas de seguridad para proteger el derecho a la privacidad de los interesados. Si los intereses de los interesados prevalecen sobre los suyos, el tratamiento no debería seguir adelante.

Consentimiento: También puede tratar los Datos Personales de Reveal si el interesado ha dado su

[7] Directriz de la CNPD y código laboral

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

[9] *Directrices 2/2019 del Comité Europeo de Protección de Datos (CEPD) sobre el tratamiento de datos personales con arreglo al artículo 6(1)(b) RGPD en el contexto de la prestación de servicios online a interesados, aprobadas el 9 de abril de 2019*, p. 7

consentimiento para ello. No obstante, el consentimiento sólo es válido si se da libremente. Los interesados también deben ser libres de revocar su consentimiento, sin ningún tipo de perjuicio por ello. Esto dificulta la obtención de un consentimiento válido en el contexto laboral.[10]
Muchas autoridades de control de protección de datos han hecho observaciones sobre las bases de legitimación en el contexto telemático. Por ejemplo:

- En el Reino Unido y Polonia, donde se permite el uso privado de un vehículo, rara vez estará justificado el control de los movimientos cuando se utiliza de forma privada, sin el consentimiento libre del usuario.[11]
- En Portugal, el consentimiento no constituye una base de legitimación válida para el tratamiento de datos derivados de la geolocalización.[12]
- Los dispositivos de localización de vehículos no deben considerarse dispositivos para seguir o controlar el comportamiento o el paradero de los conductores u otro personal, por ejemplo, mediante el envío de alertas en relación con la velocidad del vehículo.[13]
- El tratamiento de datos de localización puede estar justificado cuando se realiza en el curso del control del transporte de personas o mercancías, de la mejora de la distribución de los recursos o para la seguridad del empleado, el vehículo o las mercancías transportadas, pero puede ser excesivo cuando los empleados sean libres de organizar sus viajes como deseen o cuando se realice únicamente para controlar el trabajo de un empleado, en los supuestos en los que éste pueda controlarse por otros medios.[14]

Es improbable que el envío de información excesiva a un cliente sobre la entrega de sus artículos por parte del conductor, por ejemplo, la fotografía del pasaporte (además del nombre y la ubicación del conductor) para que el cliente pueda verificar la identidad del conductor a su llegada, tenga una base de legitimación (habría un "interés legítimo" en proporcionar la fotografía a efectos de identificación, pero esto se considera desproporcionado para satisfacer la prueba de intereses en conflicto).[15]

Datos sobre infracciones penales

Si los Datos Personales de Reveal que trate incluyen datos sobre infracciones penales (según las leyes locales y la interpretación local de "infracciones penales"), el Art. 10 RGPD restringe el tratamiento de estos datos personales. Los datos sobre infracciones penales sólo pueden tratarse cuando se encuentren bajo el control de una "autoridad pública" o cuando lo autoricen las leyes nacionales o de la UE aplicables, por lo que deberá consultar la legislación local para identificar los requisitos pertinentes, por ejemplo:

Usuarios del servicio en Francia
En virtud de la Ley de Protección de Datos francesa, está prohibida la recogida de datos personales relativos al comportamiento de una persona que pueda, o probablemente vaya a, ser clasificada como una infracción o un delito. En consecuencia, está prohibido recoger el hecho de que la persona haya superado los límites de velocidad o información relativa al comportamiento de una persona que pueda revelar infracciones de las normas de tráfico.

Usuarios del servicio en Alemania
En la actualidad, el tratamiento normal de los Datos Personales de Reveal en Alemania no constituye un tratamiento de la información sobre infracciones penales. Sin embargo, el uso de los servicios específicamente para descubrir infracciones penales estaría restringido por el artículo 26(1) BDSG (por ejemplo, si los movimientos de los vehículos se controlan para descubrir robo, fraude o tráfico de drogas por parte de los

[10] Por ejemplo, el consentimiento de los empleados no se considera habitualmente válido en Alemania (Comisario de Protección de Datos y Libertad de Información (LDi) NRW, 24º *Informe sobre Protección de Datos y Libertad de Información 2017-2018*, p. 65, 66) y el consentimiento no es una base de legitimación válida para el tratamiento de datos personales en el contexto del empleo en Portugal (directriz de la CNPD sobre el uso de los peajes de geo-localización en el contexto del empleo y la interpretación estricta de las disposiciones del Código Laboral).
[11] Oficina del Comisionado de Información *El código de prácticas de empleo*, p. 76; (polaco) Oficina de Protección de Datos, *Protección de datos en el lugar de trabajo Directrices para los empleadores*, p. 38.
[12] Directriz de la CNPD sobre el uso de peajes de geo-localización en el contexto del empleo y la interpretación estricta de las disposiciones del Código de Trabajo
[13] *Dictamen 13/2011 del GT29 sobre los servicios de geolocalización en los dispositivos móviles inteligentes*
[14] *Dictamen 5/2005 del GT29 sobre el uso de los datos de localización con vistas a prestar servicios de valor añadido.*
[15] *Dictamen 2/2017 del GT29 sobre el tratamiento de datos en el trabajo.*

empleados - tenga en cuenta que las infracciones por exceso de velocidad no son actos delictivos en este sentido). Este no sería un caso de uso "normal" de Reveal y, por lo tanto, es probable que el tratamiento con este fin sólo se lleve a cabo de forma muy excepcional (por ejemplo, si un empleador investiga supuestos en los que sospecha que un empleado ha cometido un acto delictivo), pero si utiliza los servicios con este fin, deberá consultar el artículo 26(1) BDSG.

Usuarios del servicio en Italia
En general, el tratamiento de los Datos Personales de Reveal no constituye un tratamiento de información sobre infracciones penales según se entiende en Italia (sólo infracciones que serían objeto de una sanción administrativa). Sin embargo, deberá estar pendiente de si cualquier cambio en la legislación local introduce alguna infracción penal para la que los Datos Personales de Reveal puedan ser relevantes.

Usuarios del servicio en Polonia
Se aplican ciertos requisitos específicos al tratamiento de la información de infracciones penales relativa a los empleados en virtud del Código Laboral polaco de 1974, a saber, que no se puede confiar en el consentimiento de un empleado para el tratamiento de sus datos sobre infracciones penales. Se requiere una base jurídica alternativa, muy probablemente que la información sea tratada para cumplir con una obligación legal, o para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial.

Usuarios del servicio en Portugal
El tratamiento de datos sobre infracciones penales para la prevención o detección de un acto ilícito (como, por ejemplo, potencialmente, la comisión de infracciones penales de exceso de velocidad/tráfico) se permite en determinadas circunstancias, y cuando ello sea necesario a efectos de, o en relación con, cualquier procedimiento judicial, asesoramiento jurídico o, en su caso, para el reconocimiento, el ejercicio o la defensa de derechos. Sin embargo, los datos personales deben ser seudonimizados en un plazo de siete días a partir de su recogida.

Usuarios del servicio en España
En general, el tratamiento de los Datos Personales de Reveal no constituye un tratamiento de información sobre infracciones penales, tal y como se entiende en España (sólo la infracción de normas de tráfico). Sin embargo, deberá estar pendiente de si se produce cualquier cambio en las leyes locales que introduzca alguna infracción penal para la que sean relevantes los Datos Personales de Reveal, ya que el tratamiento de información sobre infracciones penales en España es restringido - las únicas circunstancias (potencialmente) relevantes en las que el tratamiento de información sobre infracciones penales podría tener lugar en este contexto son (i) cuando el propósito sea la prevención, investigación, detección o enjuiciamiento de infracciones penales o su ejecución, (ii) cuando el tratamiento se encuentre amparado por una norma con rango y efectos legales o por la legislación de la UE.

Usuarios del servicio en el Reino Unido
En el Reino Unido, deberá asegurarse de que, además de una base de legitimación, se cumpla una condición para el tratamiento, ya sea en virtud del artículo 9 del RGPD o del anexo 1 de la Ley de Protección de Datos de 2018. Por ejemplo, por lo que se refiere a los datos relativos a infracciones penales, la Ley de Protección de Datos de 2018 permite el tratamiento de datos personales para la prevención o detección de un acto ilícito (como, por ejemplo, potencialmente, la comisión de un delito de exceso de velocidad/tráfico) en determinadas circunstancias, y cuando sea necesario a efectos de, o en relación con, cualquier procedimiento judicial, asesoramiento jurídico o, en su caso, para el reconocimiento, el ejercicio o la defensa de derechos.

F. Minimización de Datos

Deberá asegurarse de que sólo utiliza los Datos Personales de Reveal que sean adecuados, relevantes y se limiten a lo necesario (en función de sus finalidades). Esto implica, en última instancia, que deberá identificar y utilizar la cantidad mínima de Datos Personales de Reveal que necesite para llevar a cabo sus finalidades.

Si permite que los empleados hagan uso personal de los vehículos, no hay necesidad, en general, de recoger información sobre el lugar donde se desplaza el vehículo fuera de las horas de trabajo. El servicio tiene la funcionalidad de asegurar que los empleados no sean supervisados fuera de las horas de trabajo. Esto se conoce como el "Privacy Switch" ("Interruptor de Privacidad") y es una forma sencilla y rentable de garantizar

el cumplimiento. En algunos países (como Francia, Alemania y Portugal), la autorización para que los empleados utilicen el "Privacy Switch" ("Interruptor de Privacidad") es obligatoria de acuerdo con las directrices normativas.[16]

G. Exactitud de los Datos

Deberá asegurarse de que los Datos Personales de Reveal que utilice no sean incorrectos o induzcan a error. En el contexto de Datos Personales de Reveal es especialmente importante que adopte medidas para garantizar la exactitud de los datos personales (por ejemplo, garantizar que los registros de los vehículos asignados a los empleados se realicen con precisión) y que valore detenidamente cualquier problema relacionado con la exactitud de los datos personales (por ejemplo, que un conductor cuestione su ubicación en un momento determinado).

H. Conservación de los Datos Personales de Reveal

Los Datos Personales de Reveal únicamente podrán conservarse durante el tiempo que sea necesario para sus finalidades específicas. Deberá tener en cuenta la posible aplicación de algún requisito de retención legal (por ejemplo, para conservar los registros de horario de trabajo). Estos requisitos deberán ser reflejados en su política de conservación.

I. Seguridad de los Datos Personales de Reveal

Deberá aplicar las medidas "técnicas y organizativas adecuadas" para garantizar la confidencialidad, integridad y disponibilidad de los Datos Personales de Reveal, de conformidad con el Art. 32 del RGPD. Se puede utilizar una evaluación de riesgos para identificar los problemas particulares que presenta la implementación de Reveal y la utilización de los Datos Personales de Reveal, y para determinar el nivel de seguridad "adecuado" (teniendo en cuenta el estado actual de la técnica y los costes de implementación). Una vez implementadas, deberá probar periódicamente sus medidas técnicas y organizativas para asegurarse de que siguen siendo adecuadas. Cuando comparta Datos Personales de Reveal con otra organización que actúe como Encargado del Tratamiento de Datos en su nombre, deberá asegurarse de que el Encargado garantiza suficientemente (y acepta contractualmente) la implementación, asimismo, de medidas técnicas y organizativas apropiadas para proteger los datos.

En caso de que se produzca una violación de la seguridad de los datos personales, deberá cumplir con lo dispuesto en el Art. 33 y 34 del RGPD. Se lo notificaremos sin dilación indebida. Es posible que se le pida que lo notifique a la autoridad de control competente en un plazo de 72 horas a partir del momento en que tenga constancia del incidente (a menos que considere que es improbable que suponga un riesgo para los derechos y libertades de las personas físicas). Cuando la violación probablemente suponga un alto riesgo para los derechos y libertades de las personas físicas, también tendrá que notificar a las personas afectadas sin demora indebida. Deberá valorar la forma en la que identificaría si se ha producido una violación que implique a Datos Personales de Reveal, qué medidas tomaría para mitigar dicha violación, y cómo derivaría y evaluaría una violación para determinar si se requiere notificación.

<u>Usuarios del servicio en Francia</u>
De acuerdo con las directrices de la CNIL sobre la geolocalización de los vehículos de los empleados[17], deberá implementar, en particular, lo siguiente:

- Una política de autorización de acceso;
- Medidas para la transferencia segura de datos; y
- Un registro de las operaciones de acceso y tratamiento de datos.

<u>Usuarios del servicio en España</u>

[16] Comisario de Protección de Datos de Bavaria, 27º Informe de Actividad 2016, p. 241; directrices de la CNIL sobre la geolocalización de los vehículos de los empleados, 2018; Deliberación CNPD 7680/2014

[17] *Directrices de la* CNIL *sobre la geolocalización de los vehículos de los empleados,* 2018

Cuando se rectifican o borran datos personales, la Ley de Protección de Datos española exige a los Responsables del Tratamiento que "bloqueen" los datos como parte de las medidas técnicas y organizativas que implementen para cumplir con lo dispuesto en el Art. 32 - Esto significa que los correspondientes datos personales deben extraerse y almacenarse en una base de datos independiente, y que deben adoptarse medidas técnicas y organizativas para evitar el tratamiento de los datos (incluido cualquier acceso o visualización). Los datos personales pertinentes deben conservarse en una base de datos independiente y protegida para cumplir con las solicitudes que puedan recibirse de los organismos públicos competentes (tales como tribunales, fiscales, autoridades de control de protección de datos, etc.) o en el caso de que la transferencia de los datos a dichos organismos públicos sea necesaria para el ejercicio o la defensa de reclamaciones judiciales. Para calcular el período durante el cual es necesario mantener "bloqueados" los datos personales deben tenerse en cuenta los plazos de prescripción para las diferentes reclamaciones jurídicas que puedan surgir como consecuencia del tratamiento de los datos en cuestión. Los datos personales pueden suprimirse por completo una vez transcurridos los plazos de prescripción correspondientes.

Como Responsable del Tratamiento de los Datos Personales de Reveal deberá asegurarse de que puede cumplir esta obligación. Verizon le ayuda a cumplir con la misma, permitiéndole descargar copias de ciertos Datos Personales de Reveal a través del panel de control de autoservicio de Reveal y proporcionándole otros Datos Personales de Reveal si así lo solicita.

J. Derechos de los Interesados

Deberá identificar la forma en la que cumplirá con su obligación de responder a las solicitudes de los interesados. Según el RGPD, los interesados tienen los siguientes derechos con respecto a sus datos personales:

- Derecho de acceso;
- Derecho de rectificación;
- Derecho de supresión;
- Derecho de limitación del tratamiento;
- Derecho a la portabilidad de los datos;
- Derecho de oposición;
- Derechos en relación con la toma de decisiones automatizadas, incluida la elaboración de perfiles.

En su aviso de privacidad deberá informar a los interesados sobre la existencia de estos derechos.

La aplicabilidad de estos derechos puede ser limitada (por ejemplo, el derecho a la portabilidad de datos sólo existe cuando los datos personales sean tratados sobre la base de legitimación de una necesidad contractual o cuando haya existido consentimiento) y es posible que usted pueda aplicar exenciones (por ejemplo, cuando la divulgación de información afecte negativamente a los derechos de terceros, lo que podría incluir la protección de secretos comerciales).

Por lo general, deberá responder a estas solicitudes en el plazo de un mes y asegurarse de que su respuesta cumple con los requisitos adicionales establecidos en el Art. 12 RGPD (por ejemplo, que la información que usted proporcione a los interesados sea concisa, transparente, inteligible y de fácil acceso, y con un lenguaje claro y sencillo).

Cuando sea práctico hacerlo, Verizon puede ayudarle a cumplir con las solicitudes de personas relacionadas con el servicio.

<u>Usuarios del servicio en Francia</u>
En virtud de la Ley de Protección de Datos francesa, los particulares tienen derecho a definir las directrices relativas a la utilización de sus datos personales después de su fallecimiento. Usted deberá asegurarse de que es capaz de responder a este tipo de solicitud.

K. Intercambio de Datos Personales de Reveal

Además de las personas que solicitan acceso a sus propios datos, deberá determinar cómo responderá a las solicitudes de acceso a Datos Personales de Reveal por parte de terceros. Lo anterior podría incluir, por ejemplo, las solicitudes de los organismos encargados de hacer cumplir la ley y de las compañías de seguros,

cuando un vehículo se haya visto implicado en un accidente.

Cualquier intercambio de Datos Personales de Reveal (inclusive, por ejemplo, con otras empresas dentro de su grupo societario o con otro proveedor de servicios) deberá cumplir con todos los requisitos de protección de datos establecidos en este eBook (por ejemplo, el intercambio debe ser legal, proporcionado, transparente, etc.). Deberá considerar si es necesario suscribir contratos u otros acuerdos con la empresa (por ejemplo, cuando la otra empresa actúe como Encargado del Tratamiento de Datos en su nombre, o como Corresponsable del Tratamiento de Datos junto con usted). Cuando este intercambio implique una transferencia de Datos Personales de Reveal fuera del Espacio Económico Europeo ("**EEE**"), deberá asegurarse de que la transferencia está permitida de acuerdo con el RGPD.

Usuarios del servicio en Francia
De acuerdo con las directrices de la CNIL, deberá limitar el acceso a la información relacionada con (o resultante de) los dispositivos de geolocalización a (según corresponda): (i) su propio personal autorizado, (ii) el empleador de la persona a la que se refiera la información de geolocalización; y (ii) el personal autorizado de un cliente al que preste los correspondientes servicios. Como cuestión de principio, el nombre del conductor no debe ser compartido, a menos que esta información sea especialmente relevante y necesaria.

L. Toma de Decisiones Automatizada

La ley de protección de datos prohíbe que las entidades tomen decisiones basadas únicamente en el tratamiento automatizado de datos personales cuando la decisión produzca efectos jurídicos o similares significativos. Usted deberá identificar cualquiera de dichos usos del servicio. Esto podría tener relevancia cuando:

- El salario de un conductor se calcule automáticamente en función de la hora de inicio o finalización de la conducción de un vehículo;
- Se emita automáticamente un aviso a un conductor por acceder a un área geo-cercada;
- La elegibilidad de un conductor para recibir un bono se calcule automáticamente en función del número de trabajos asignados y completados por él, conforme a lo registrado por el servicio.

Estas restricciones no serán de aplicación cuando, previamente a la adopción de una decisión, se haya llevado a cabo una revisión sustancial por una persona física.

Las entidades están autorizadas a tomar este tipo de decisiones individuales automatizadas en los supuestos en los que se trate de una decisión:

- Necesaria para la ejecución o la celebración de un contrato;
- Autorizada por la legislación de la Unión o de un Estado miembro a la que se encuentre sujeto el Responsable del Tratamiento y que también establezca medidas adecuadas de protección de los derechos, libertades e intereses legítimos del interesado; o bien
- Basada en el consentimiento expreso del interesado.

Cuando se toma una decisión individual automatizada, es necesario proporcionar información clara a los interesados sobre este tema (véase "Aviso de Privacidad", más arriba) y, al menos, dar a los interesados derecho a obtener su participación en el proceso de toma de decisiones, a expresar su punto de vista y a oponerse a la decisión.

Usuarios del servicio en Portugal
No se permite el uso de datos de geolocalización y telemetría de vehículos para la toma de decisiones exclusivamente automatizada.[18]

M. Consulta a Empleados/Comité de Empresa/Sindicatos

En virtud de la legislación laboral, es posible que se le pida que consulte a sus empleados, al comité de

[18] Directriz de la CNPD sobre el uso de los peajes de geo-localización en el contexto del empleo y la interpretación estricta de las disposiciones del Código Laboral.

empresa o a los sindicatos sobre la implementación del servicio, o sobre otros usos que usted decida hacer de Datos Personales de Reveal. Alternativamente, es posible que se le pida que consulte con los sindicatos o los representantes de los trabajadores al amparo de los términos de los acuerdos voluntarios que existan. Incluso aunque no sea necesario, usted podría considerar apropiado consultar con el personal sobre la implementación del servicio y el uso de Datos Personales de Reveal como parte del proceso de EIPD.

Si usted suscribe con su comité de empresa un acuerdo vinculante, el presente acuerdo constituirá una "norma más específica" para garantizar los derechos de protección de datos de los empleados de acuerdo con el artículo 88(1) RGPD. Esto significa que un acuerdo de este tipo puede, en algunas circunstancias, proporcionar seguridad jurídica sobre cómo puede utilizarse Reveal en su organización. Para cumplir con el requisito de una "norma más específica" conforme al artículo 88(1) RGPD, el acuerdo con el comité de empresa deberá ser vinculante de conformidad con su legislación laboral local, y deberá abordar adecuadamente los intereses de protección de datos de los empleados (véase el artículo 88(2) RGPD). En caso de duda, por favor, solicite asesoramiento jurídico.

Usuarios del servicio en Francia
Según el Art. L2312-38 del Código de Trabajo francés, deberá informar y consultar a los Comités de Empresa (*Conseil Economique et Social*) antes de implantar cualquier sistema o medio que permita controlar la actividad de los empleados, como, por ejemplo, el seguimiento de la geolocalización.

Usuarios del servicio en Alemania
En virtud del Artículo 87(6) de la Ley de Comités de Empresa (Betriebsverfassungsgesetz -BetriebsVG), cuando su empresa cuente con un comité de empresa, éste tendrá derecho a co-determinar la introducción y el uso de equipos técnicos diseñados para supervisar el comportamiento o el rendimiento de los empleados. No está permitido el "control" permanente del comportamiento y del rendimiento de los empleados a través de la supervisión - si usted es el empleador, deberá excluir dicho "control" permanente de empleados por medio de acuerdos con el comité de empresa o de normas unilaterales vinculantes.[19]

El artículo 26, apartado 4, de la Ley Federal de Protección de Datos establece explícitamente que puede permitirse el tratamiento de datos sobre la base de acuerdos de empresa, si estos acuerdos de empresa cumplen los requisitos del artículo 88(2) RGPD.

Usuarios del servicio en Italia
Es posible que tenga que consultar al sindicato o sindicatos de su organización, si existieran, u obtener autorización de la Autoridad Laboral competente sobre la implementación del servicio y el uso que haga de los Datos Personales de Reveal para cumplir con lo dispuesto en el Art. 4 (2) de la Ley 300/1970 (Estatuto del Trabajador Italiano), a menos que los Datos Personales de Reveal que usted trate se limiten a los datos estrictamente necesarios para cumplir con sus obligaciones legales.

Usuarios del servicio en Polonia
Deberá determinar el fin, el alcance y los métodos de seguimiento en su Reglamento de Trabajo (una política interna obligatoria para los empleadores con más de 50 trabajadores en Polonia) o en el Convenio Colectivo de Empresa. Si hay sindicatos en su organización, los cambios en el Reglamento de Trabajo o en el Convenio Colectivo de Empresa requerirán la cooperación con los sindicatos.

En lo que respecta a los empleados existentes, deberá informarles de que tiene la intención de poner en marcha un sistema de supervisión. Tendrá que suministrar esta información no más tarde de dos semanas antes de la puesta en marcha del sistema de seguimiento.

Usuarios del servicio en Portugal
En virtud del Art. 21 del Código de Trabajo portugués, deberá informar y consultar a los Comités de Empresa (Comissão de Trabalhadores) antes de implantar cualquier sistema o medio que permita el seguimiento de la actividad de los empleados como, por ejemplo, el seguimiento de la geolocalización.

[19] Comisario de Protección de Datos y Libertad de Información de Baden-Württemberg, *Protección de datos de empleo*, 2018; Centro Independiente de Protección de Datos de Schleswig-Holstein, Informe de actividad 2017-2018, 103

Usuarios del servicio en España

Conforme al Art. 64(1) del Estatuto de los Trabajadores, deberá informar a los representantes de los trabajadores antes de la aplicación de cualquier medida que pueda afectar a los trabajadores, entendiéndose que entre dichas medidas se incluye la aplicación de dispositivos de geolocalización o cualquier otra solución de supervisión.

Como apoyo a lo anterior, el Art. 90(2) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece que, con carácter previo a la implantación de los dispositivos de geolocalización, los empleados y los representantes de los trabajadores deben ser informados de la existencia y de las características de los mismos.

N. Mitigación de Riesgos y Protección de Datos desde el Diseño y por Defecto

Deberá asegurarse de que se han tomado todas las medidas necesarias para mitigar los riesgos para las personas físicas (conforme se identificaron durante el proceso de EIPD) y para cumplir con los requisitos de "protección de datos desde el diseño y por defecto". La protección de datos desde el diseño significa que las cuestiones de privacidad deben considerarse y abordarse desde el principio de una actividad de tratamiento de datos (es decir, durante la fase de diseño) y durante el ciclo de vida de dicha actividad de tratamiento. La protección de datos por defecto requiere que usted se asegure de que se traten los datos mínimos necesarios para lograr su(s) finalidad(es) (por ejemplo, en lugar de permitir un acceso amplio a Datos Personales de Reveal, el acceso debe estar restringido a personas específicas en función de la "necesidad de conocer").

Las directrices de las autoridades de control de protección de datos ofrecen ejemplos de reducción de riesgos en el contexto de la telemática y del control de los empleados:

- Se debe permitir a los conductores desactivar temporalmente el seguimiento de la ubicación en determinadas circunstancias (por ejemplo, al visitar una clínica médica), en las que se permite a los empleados hacer un uso personal de los vehículos de la empresa.[20]
- Cuando exista la necesidad de controlar la ubicación de un vehículo fuera del horario laboral de un empleado (por ejemplo, para evitar el robo de vehículos), la implementación debe ser proporcional a los riesgos, por ejemplo, la ubicación del vehículo no quedará registrada (o no será visible para usted) fuera del horario laboral, a menos que abandone un perímetro ampliamente definido (por ejemplo, una región).[21]
- La cifra de personal con acceso a Datos Personales de Reveal debe ser mínima. El personal debe tener la formación adecuada y estar sujeto a obligaciones de confidencialidad y seguridad.[22]
  Valore qué personal es el más apropiado para acceder a Datos Personales de Reveal (puede que, por ejemplo, no se deban encontrar incluidos superiores jerárquicos).[23]

O. Designación de un Delegado de Protección de Datos (DPD)

En el Art. 37 RGPD se establecen varios requisitos para el nombramiento de un Delegado de Protección de Datos (DPD). Es posible que sus actuales actividades de tratamiento no requieran que designe a un DPD. Sin embargo, el uso que usted haga de los servicios puede hacer necesario que cuente con un DPD conforme al Art 37(1)(b), que exige la designación de un DPD cuando las actividades principales de una organización consistan en un seguimiento regular y sistemático de interesados a gran escala. La utilización de los servicios para controlar a los conductores y a su comportamiento al volante probablemente se encuentre dentro del ámbito de aplicación del Art. 37(1)(b), en cuyo caso se le pedirá que nombre a un DPD. Otras disposiciones del RGPD (arts. 38 y 39) establecen los requisitos relativos a la posición y a las funciones del DPD - usted también deberá cumplir con estos requisitos si se requiere el nombramiento de un DPD.

Usuarios del servicio en Alemania

Conforme al artículo 38 de la Ley Federal de Protección de Datos (BDSG), usted deberá designar a un DPD si

[20] *Dictamen 2/2017* del Grupo de Trabajo del artículo 29 *sobre el tratamiento de datos en el trabajo* (GT 249), p. 20.

[21] *Dictamen 2/2017* del Grupo de Trabajo del artículo 29 *sobre el tratamiento de datos en el trabajo* (GT 249), p. 20.

[22] Oficina del Comisionado de Información *Código de prácticas de empleo*, p. 67

[23] Oficina del Comisionado de Información *Código de prácticas de empleo*, p. 67

emplea de forma permanente, al menos, a 20 personas para el tratamiento automatizado de datos personales o si el tratamiento de datos personales que realiza requiere que usted lleve a cabo una EIPD. Es probable que tenga que nombrar a un DPD si utiliza los servicios en Alemania.

Información Adicional

Legislación

- Reglamento General de Protección de Datos (UE) 2016/679 ('RGPD')
- Ley de Protección de Datos de 2018 (Reino Unido)
- Ley 58/2019, de 8 de agosto de 2019 (Portugal) Código de Trabajo (Portugal)
- Ley Orgánica 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y Garantía de Derechos Digitales (España)
- Ley Federal de Protección de Datos (Bundesdatenschutzgesetz - BDSG) 2018 (Alemania)
- Ley de Comités de Empresa (Betriebsverfassungsgesetz -BetriebsVG) (Alemania)
- Decreto Legislativo n.º 196/2003 (Código de Protección de Datos italiano) (Italia)
- Ley nº 300/1970 (Estatuto de los Trabajadores italiano) (Italia)
- Decreto Legislativo 101/2018 (Italia)
- Ley de Protección de Datos francesa n°78-17(Francia)
- Código de Trabajo francés (Francia)

Jurisprudencia

South Lanarkshire Council v Scottish Information Commissioner [2013] UKSC 55 (REINO UNIDO)

Guía Regulatoria

UE

- *Dictamen 5/2005* del Grupo de Trabajo del Artículo 29 *sobre el uso de los datos de localización con vistas a prestar servicios de valor añadido* (GT115)
- *Dictamen 13/2011* del Grupo de Trabajo del Artículo 29 *sobre los servicios de Geolocalización en los dispositivos móviles inteligentes* (GT 185)
- *Directrices* del Grupo de Trabajo del Artículo 29 *sobre la Evaluación de Impacto relativa a la Protección de Datos (EIPD) y para determinar si es "el tratamiento entraña probablemente un alto riesgo" a efectos del Reglamento 2016/679* (GT248).
- *Dictamen 2/2017* del Grupo de Trabajo del Artículo 29 *sobre el tratamiento de datos en el trabajo* (GT249)
- *Directrices* del Grupo de Trabajo del artículo 29 *sobre decisiones individuales Automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* (GT251)
- *Directrices 2/2019 del Comité Europeo de Protección de Datos sobre el tratamiento de datos personales con arreglo al artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios online a los interesados (versión para consulta pública).*

Francia

- Directrices de la CNIL sobre la geolocalización de los vehículos de los empleados, 2018

Alemania

- Comisario de Protección de Datos y Libertad de Información de Renania-Palatinado, *sobre la legalidad del seguimiento por GPS de los empleados*
- Comisario de Protección de Datos y Libertad de Información de Baden-Württemberg, *Protección de datos en el empleo 2018*
- Conferencia sobre Protección de Datos de las autoridades independientes de protección de datos federales y estatales (Länder) (Datenschutzkonferenz - DSK), documento breve nº 14: *Protección de datos en el empleo* (17 de diciembre de 2018).
- Comisario de Protección de Datos de Baviera, 27º *Informe de Actividades 2016*
- Conferencia sobre Protección de Datos de las autoridades independientes de protección de datos federales y estatales (Länder) (Datenschutzkonferenz - DSK), Documento breve nº 17: *Categorías especiales de datos personales* (27 de marzo de 2018).
- Conferencia sobre Protección de Datos de las autoridades independientes de protección de datos

federales y estatales (Länder) (Datenschutzkonferenz - DSK), documento breve núm. 19: *Información y compromiso de los empleados en el cumplimiento de los requisitos de protección de datos según el RGPD* (29 de mayo de 2018).

- Comisario de Protección de Datos y Libertad de Información de Renania del Norte-Westfalia (LDi NRW), 24º Informe sobre protección de Datos y libertad de información 2017-2018, *Posicionamiento por satélite para la determinación de la posición de los vehículos de empresa - no se permiten medios de control de los empleados*.
- Comisario de Protección de Datos y Privacidad de Berlín libertad de información, *Informe anual 2018*
- Centro Independiente de Protección de Datos de Schleswig-Holstein, Informe de Actividades 2017-2018
- Comisario de Protección de Datos de Baja Sajonia, 24º Informe de Actividades 2017-2018, *seguimiento GPS de los vehículos de empresa*

Polonia

- Oficina de Protección de Datos*, Protección de datos en el lugar de trabajo. Directrices para los empleadores*

Portugal

- Deliberación CNPD 7680/2014 (Directriz sobre el uso de la geolocalización en el contexto del empleo).

REINO UNIDO

- *Código de Prácticas de Empleo y Orientación Suplementaria* de la Oficina del Comisionado de Información

Listado del RGPD

Artículo del RGPD	**Asunto**	**Relevancia para Reveal**	**Referencia en el eBook**
Art. 1, 2 o 3	Objeto, ámbito de aplicación material y ámbito territorial	Sin relevancia específica	N/A
Art. 4	Definiciones	Define los conceptos de "datos personales" y "datos personales de categoría especial".	"*Preguntas Frecuentes sobre Reveal*", secciones 3 y 4
Art. 5	Principios y responsabilidad proactiva	El tratamiento de los Datos Personales de Reveal debe cumplir con los principios de protección de datos, y el Responsable del Tratamiento debe ser capaz de demostrar su cumplimiento.	"*Cumplimiento de los Requisitos de Protección de Datos*", en general
Art. 6 y 7	Licitud del tratamiento y condiciones para el consentimiento	Debe existir una base de legitimacióna para cada una de las finalidades del tratamiento de los Datos Personales de Reveal	"*Cumplimiento de los Requisitos de Protección de Datos*", sección E
Art. 8	Condiciones aplicables al Consentimiento del Niño en relación con SSI	Sin relevancia específica	N/A
Art. 9 y 10	Tratamiento de categorías especiales de datos personales y de información sobre condenas e infracciones penales	Debe darse alguna circunstancia para cada uno de las finalidades del tratamiento de los Datos Personales de	"*Preguntas Frecuentes sobre Reveal*", sección 4, y "*Cumplimiento de los Requisitos de Protección de Datos*", sección E

		Reveal, cuando se traten categorías especiales de o de información sobre infracciones penales.	
Art. 11	Tratamiento que no requiere identificación	Sin relevancia específica	N/A
Art. 12	Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado	Toda la información que se facilite a las personas sobre las que se traten los Datos Personales de Reveal deberá ser concisa, transparente, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo.	"*Cumplimiento de los Requisitos de Protección de Datos*", secciones B y J
Art. 13 y 14	Información que deberá facilitarse al interesado	Se debe proporcionar un aviso de protección de datos a las personas sobre las que se tratan los Datos Personales de Reveal	*"Cumplimiento de los Requisitos de Protección de Datos*", sección B
Art. 15	Derecho de acceso	Deberá proporcionarse acceso a los Datos Personales de Reveal a los interesados que lo soliciten (sujeto a exenciones).	*"Cumplimiento de los Requisitos de Protección de Datos*", sección J
Art. 16	Derecho de rectificación	Los Datos Personales de Reveal deberán ser rectificados a petición del interesado	*"Cumplimiento de los Requisitos de Protección de Datos*", sección J
Art. 17	Derecho de supresión	Los Datos Personales de Reveal deberán ser suprimidos a petición del interesado, si dicho derecho fuera de aplicación	*"Cumplimiento de los Requisitos de Protección de Datos*", sección J
Art. 18	Derecho a la limitación del tratamiento	El tratamiento de los Datos Personales de Reveal deberá ser limitado a petición del interesado, si dicho derecho fuera de aplicación	*"Cumplimiento de los Requisitos de Protección de Datos*", sección J
Art. 19	Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento	Cuando se reciba una solicitud de rectificación, supresión o limitación de tratamiento relativa a Datos Personales de Reveal, deberá notificarse a los terceros a los que se hayan comunicado los datos.	*"Cumplimiento de los Requisitos de Protección de Datos*", sección J
Art. 20	Derecho a la portabilidad de	Los Datos Personales de	*"Cumplimiento de los*

	los datos	Reveal deberán ser transmitidos al interesado (o a los terceros que designe) a petición del interesado, si dicho derecho fuera de aplicación.	*Requisitos de Protección de Datos*", sección J
Art. 21	Derecho de oposición	Deberá cesar el tratamiento de los Datos Personales de Reveal a petición del interesado, si dicho derecho fuera de aplicación.	*"Cumplimiento de los Requisitos de Protección de Datos*", sección J
Art. 22	Decisiones individuales automatizadas, incluida la elaboración de perfiles	Las decisiones individuales automatizadas sobre personas físicas cuando la decisión produzca efectos jurídicos o similares significativos para los interesados, sólo podrán adoptarse de conformidad con el artículo 22	*"Cumplimiento de los Requisitos de Protección de Datos*", sección L
Art. 23	Limitaciones	Sin relevancia específica	N/A
Art. 24	Responsabilidad del Responsable del Tratamiento	Deberán implementarse medidas técnicas y organizativas apropiadas a fin de garantizar (y demostrar) que el tratamiento es conforme con el RGPD	"*Cumplimiento de los Requisitos de Protección de Datos*", de forma general
Art. 25	Protección de datos desde el diseño y por defecto	Las cuestiones de protección de datos deben abordarse desde el principio y durante el ciclo de vida del tratamiento de los Datos Personales de Reveal, y deben tratarse los datos personales mínimos necesarios para lograr su fin.	*"Cumplimiento de los Requisitos de Protección de Datos*", secciones F y N
Art. 26	Corresponsables del Tratamientos	Sin relevancia específica	N/A
Art. 27	Representantes de Responsables o Encargados del Tratamiento no establecidos en la Unión	Sin relevancia específica	N/A
Art. 28	Encargado del Tratamiento	Sólo deberá contratarse para tratar Datos Personales de Reveal a Encargados del Tratamiento que ofrezcan garantías	*"Cumplimiento de los Requisitos de Protección de Datos*", sección I

		suficientes, y se impondrán obligaciones contractuales a estos Encargados del Tratamiento	
Art. 29	Tratamiento bajo la autoridad del Responsable o del Encargado del Tratamiento	Sin relevancia específica	N/A
Art. 30	Registro de las actividades de tratamiento	El tratamiento de los Datos Personales de Reveal deberá quedar reflejado en el registro de las actividades de tratamiento.	*"Cumplimiento de los Requisitos de Protección de Datos*", sección C
Art. 31	Cooperación con la autoridad de control	Sin relevancia específica	N/A
Art. 32	Seguridad del tratamiento	Deberán aplicarse medidas técnicas y organizativas apropiadas para proteger la seguridad de los Datos Personales de Reveal.	*"Cumplimiento de los Requisitos de Protección de Datos*", sección I
Art. 33 y 34	Notificación de una violación de la seguridad de los datos (a la autoridad de control y al interesado)	En caso de violación de la seguridad de los datos personales que implique a Datos Personales de Reveal, dicha violación deberá notificarse a las autoridades de control y a las personas afectadas cuando se cumplan las condiciones.	*"Cumplimiento de los Requisitos de Protección de Datos*", sección I
Art. 35 y 36	Evaluación de impacto relativa a la protección de datos y consulta previa	Cuando el tratamiento entrañe un alto riesgo no mitigado para las personas físicas, deberá realizarse una evaluación de impacto de la protección de datos para el tratamiento de los Datos Personales de Reveal y puede ser necesaria la consulta con las autoridades de control	*"Cumplimiento de los Requisitos de Protección de Datos*", sección A
Art. 37, 38 y 39	Delegado de Protección de Datos	Deberá nombrarse un correspondiente Delegado de Protección de Datos si las actividades principales del Responsable del Tratamiento consisten en una observación	"*Cumplimiento de los Requisitos de Protección de Datos",* sección Q

		"habitual y sistemática" de interesados a gran escala o en el tratamiento a gran escala de datos de categoría especial/ relativos a infracciones penales.	
Art. 40, 41, 42 y 43	Códigos de conducta, certificación y acreditación	Sin relevancia específica	N/A
Art. 44 - 50	Transferencias	Solamente deberán realizarse transferencias de Datos Personales de Reveal fuera del EEE a países que no sean "adecuados" (por ejemplo, a otros proveedores de plataformas o empresas del grupo) cuando exista un mecanismo de transferencia o una excepción.	"*Preguntas Frecuentes sobre Reveal*", sección 6, y *"Cumplimiento de los Requisitos de Protección de Datos*", sección K
Art. 51 - 59	Autoridad de control y competencia, funciones, poderes e informes de actividad	Sin relevancia específica	N/A
Art. 60 - 67	Cooperación y coherencia	Sin relevancia específica	N/A
Art. 68 - 76	Comité Europeo de Protección de Datos	Sin relevancia específica	N/A
Art. 77	Derecho a presentar una reclamación ante una autoridad de control	Sin relevancia específica	N/A
Art. 78	Derecho a la tutela judicial efectiva contra una autoridad de control	Sin relevancia específica	N/A
Art. 79 - 82	Derecho a la tutela judicial efectiva contra un Responsable o Encargado del Tratamiento, e indemnización	Sin relevancia específica	N/A
Art. 83 - 84	Multas administrativas y sanciones	Sin relevancia específica	N/A
Art. 85 - 91	Disposiciones relativas a situaciones específicas de tratamiento	Sin relevancia específica	N/A
Art. 92 - 93	Actos delegados y actos de ejecución	Sin relevancia específica	N/A
Art. 94 - 99	Disposiciones finales	Sin relevancia específica	N/A