Introdução

A Inosat fornece Soluções para a Mobilidade da Mão de Obra nas áreas de Gestão de Frotas e Gestão de Serviços. Os nossos produtos acompanham o desempenho da sua frota automóvel, que pode ter um grande impacto nos seus negócios. Coisas como a localização dos seus veículos, como os seus motoristas se comportam na estrada e quanto combustível consomem. Estas informações são colocadas em painéis compreensíveis para que possa agir rapidamente. A Reveal é uma ferramenta crítica para o ajudar a fazer mais em menos tempo, fornecer um melhor serviço ao cliente e, finalmente, melhorar os resultados nos seus negócios. Através dos nossos produtos de Serviço Externo, temos também a capacidade de gerir o ciclo de vida completo das solicitações de serviço dos nossos clientes desde o primeiro contacto, fornecendo um orçamento, agendamento, despacho, encaminhamento ideal de um motorista e recolha do pagamento.

Este *eBook* responde às questões mais frequentes ("FAQs") acerca dos Serviços de Rastreamento de Frotas Reveal ('os serviços' ou 'Reveal'), que lhe são vendidos pela Inosat na plataforma Reveal, e apresenta uma visão geral de algumas das principais considerações e requisitos de proteção de dados com os quais será necessário trabalhar antes, durante e após a implementação do serviço por si. Enquanto este *eBook* se foca predominantemente em questões de proteção de dados, deve considerar se quaisquer outros requisitos legais relevantes afetarão a implementação e uso dos serviços. Por exemplo, em alguns países, o uso de veículos conduzidos por funcionários é abrangido pelos requisitos da legislação laboral.

Quando relevante, foi feita referência às orientações regulatórias disponíveis no momento da publicação. Os reguladores revêm regularmente as suas orientações, portanto, deverá acompanhar atentamente os desenvolvimentos nesta área pois, em última análise, a responsabilidade é sua como Responsável pelo Tratamento de dados pessoais recolhidos e utilizados através do serviço, por forma a garantir a conformidade com as leis aplicáveis.

As informações fornecidas neste *eBook* não constituem aconselhamento jurídico ou profissional. Deve consultar sempre um advogado qualificado sobre qualquer problema ou assunto jurídico específico. A Inosat não assume qualquer responsabilidade pelas informações contidas neste *eBook* e isenta-se de toda a responsabilidade em relação às mesmas.

FAQs Reveal

1. De quem são recolhidas informações através dos serviços?
Primeiramente, serão recolhidas informações sobre os funcionários e contratados que dirigem os veículos nos quais implementa os serviços. Também podem ser recolhidas informações sobre outras pessoas (por exemplo, passageiros ou familiares do motorista com acesso ao veículo), dependendo de como e porquê o serviço é implementado por si.

2. Como são recolhidas as informações para o serviço?
O serviço recolhe informações de duas fontes:

- Através do dispositivo de bordo instalado nos seus veículos: que recolhe informações relativas aos locais e atividades dos mesmos. Se sabe (ou consegue determinar) o motorista ao qual cada veículo está atribuído, essas informações também serão dados pessoais.
- Temos várias aplicações móveis nas nossas plataformas que pode instalar para usar eficazmente o nosso serviço, tais como as nossas aplicações de Serviço Externo (Work, Workforce, Field) e de Gestão de Frota (Manager\Spotlight, Video, ELD). Para usar a aplicação, cada motorista deverá fornecer certas informações no registo.

Neste *eBook* referimo-nos coletivamente a quaisquer dados pessoais recolhidos através do serviço como 'Dados Pessoais Reveal'.

3. Que dados pessoais são recolhidos através do serviço?
A maioria dos dados pessoais que serão recolhidos através do serviço são determinados por si; o que deseja recolher varia dependendo de como e porquê a solução é implementada por si. O controle completo do tipo

de dados que recolhe é seu. Como tal, é da sua responsabilidade legal garantir que necessita de obter os dados recolhidos para usar o serviço.
Os dados pessoais recolhidos através dos dispositivos de bordo dos veículos podem incluir:

- Dados de localização (GPS) de veículos e indivíduos;
- Informações tacográficas (tempos de condução);
- Velocidade e comportamento do motorista do veículo;
- Dados de eventos do veículo (por exemplo, envolvimento num acidente, entrada ou saída numa área de delimitação geográfica);
- Outras informações do veículo (por exemplo, consumo de combustível, pressão dos pneus, dados operacionais).

Dados pessoais recolhidos através da aplicação podem incluir:

- Nome do motorista;
- Número de telefone, *e-mail* e morada do motorista;
- Credenciais de *log-in* do motorista;
- Registos do motorista (por exemplo, atribuição de veículo, número de motorista, localizações geográficas);
- Geolocalização GPS.

4. Serão recolhidas informações de 'categoria especial' ou infrações criminais através do Reveal?
De acordo com as leis de proteção de dados, as informações de categoria especial são dados pessoais relacionados com a raça, origem étnica, opiniões políticas, religião, associação a sindicatos, genética, biometria (quando usada para fins de identificação), saúde, vida e orientação sexuais. Juntamente com as informações sobre infrações criminais, o tratamento de informações de categoria especial é mais restrito.

Nenhuma informação de categoria especial ou infração criminal é solicitada pelo serviço (por exemplo, não é solicitado ao motorista que insira nenhuma informação dessa natureza na aplicação). Embora informações de categoria especial possam ser determinadas a partir de informações de localização (por exemplo, informações de geolocalização podem identificar que um motorista visita rotineiramente um centro religioso ou médico específicos), isso não aciona os requisitos do RGPD relacionados com o tratamento de informações de categoria especial, a menos que as informações de localização sejam, de facto, usadas para determinar esse tipo de dados de categoria especial. No entanto, dependendo de como e porquê o serviço é implementado por si, (supostas) informações de infração criminal podem ser processadas a partir das informações recolhidas (por exemplo, informações de atividade do veículo podem indicar que um motorista excedeu um limite de velocidade).

O que constitui uma infração criminal varia de país para país, assim como a categorização das informações como 'categoria especial' ou informações sobre infrações criminais. No caso de recolher dados que possam ser considerados informações de infração criminal, de acordo com a(s) lei(s) de proteção de dados, serão suas as obrigações adicionais com o RGPD e com a legislação nacional como Responsável pelo Tratamento desses dados pessoais.

5. Quem tem acesso aos Dados Pessoais Reveal?
O tratamento de Dados Pessoais Reveal durante o fornecimento do serviço estão disponíveis para os funcionários relevantes da Verizon com base na 'necessidade de conhecimento'. Os Dados Pessoais Reveal também são disponibilizados a empresas terceiras que prestam serviços à Verizon, para permitir que a Verizon administre o serviço (por exemplo, terceiros que fornecem serviços de alojamento). A Verizon também pode divulgar Dados Pessoais Reveal a terceiros, quando assim o é exigido por lei (por exemplo, organismos responsáveis pela aplicação da lei).

Além dos objetivos descritos acima, é uma opção sua divulgar Dados Pessoais Reveal para os seus próprios fins. Escolherá quem, na sua organização deve ter acesso aos Dados Pessoais Reveal (por exemplo, necessita de atribuir administradores que possam aceder ao portal *online* para visualizar as informações de localização e atividades em tempo real do veículo). Pode, também, optar por partilhar os Dados Pessoais Reveal com terceiros, como outras organizações dentro do seu grupo corporativo ou outros fornecedores de plataformas (por exemplo, quando outra plataforma faz interface com o Reveal).

6. A Verizon transfere Dados Pessoais Reveal para fora do Espaço Económico Europeu ('EEE')?
A Verizon hospeda os Dados Pessoais Reveal em *data centers* localizados dentro e fora do EEE. Uma lista desses países está disponível aqui: https://www.verizon.com/about/privacy/data-processing-activities. Quando a Verizon partilha Dados Pessoais Reveal para fora do EEE dentro do grupo Verizon, essas transferências são feitas de acordo com as Regras Vinculativas aplicáveis às empresas aprovadas pela UE para o Responsável pelo Tratamento e Subcontratante.

7. Durante quanto tempo é que a Verizon mantém os Dados Pessoais Reveal?
Os Dados Pessoais Reveal serão mantidos pelo tempo acordado nos termos do contrato e de acordo com as configurações de conservação selecionadas no produto por si. O tempo de conservação poderá variar dependendo da sua obrigação legal para conservar os dados ou de qualquer obrigação de reporte que possa ser solicitada por si. É sua responsabilidade como Responsável pelo Tratamento garantir o entendimento quanto ao tempo legalmente exigido para conservar os Dados Pessoais Reveal. Na rescisão dos serviços, a Inosat eliminará com segurança os Dados Pessoais Reveal.

8. A Verizon usa dos Dados Pessoais Reveal para as suas próprias finalidades?
Os Dados Pessoais Reveal são recolhidos pela Verizon para fornecer o serviço Reveal solicitado por si. A Verizon é um Subcontratante para esses fins.

Na medida do que é permitido por lei, a Verizon faz algum uso secundário de informações anónimas recolhidas através do Reveal para as suas próprias finalidades e para melhorar os produtos e serviços. Isto inclui análises para otimizar a solução Reveal e divulgações para as companhias de seguros. Nenhuma pessoa singular ou organização que utiliza o Reveal é identificável a partir das informações anónimas.

9. Como é que a Verizon garante que os Dados Pessoais Reveal são mantidos em segurança?
Consulte o Anexo de Segurança da Informação dos Sistemas Internos da Verizon para obter uma descrição das medidas técnicas e organizativas de segurança que a Verizon implementa para cumprir suas obrigações do RGPD em https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit.

Requisitos de Proteção de Dados

Esta seção explica como os requisitos de proteção de dados se aplicam uso do Reveal por si.

No final desta seção, incluímos uma *checklist* de artigos do Regulamento Geral de Proteção de Dados e onde são abordados neste *eBook*. Isso permitirá que possa verificar se uma determinada disposição do RGPD é relevante para o Reveal e onde é abordada neste *eBook*. Também incluímos uma lista de fontes de informação adicionais.

A. Avaliação de Impacto sobre a Proteção de Dados

Uma avaliação de impacto sobre a proteção de dados ('AIPD') é um processo para descrever e avaliar o tratamento de dados pessoais e identificar e gerir os riscos que o tratamento de dados representa para os indivíduos.

Coletivamente, as autoridades de controlo de proteção de dados consideram que as AIPDs devem ser realizadas quando uma organização processa dados pessoais para avaliar o desempenho, o local ou o movimento dos funcionários[1]. É provável que o uso do serviço exija que seja efetuada uma AIPD por si, mas cada autoridade de controlo publicou os seus próprios critérios. Deve consultar os critérios da sua autoridade de controlo competente para identificar se é necessária uma AIPD.

A sua AIPD deverá:

- Descrever que tratamentos de Dados Pessoais Reveal irão ocorrer;
    - A informação contida neste *eBook* acerca dos dados recolhidos, como são recolhidos e

[1] Grupo de Trabalho do Artigo 29, *Orientações sobre Avaliações de Impacto sobre a Proteção de Dados (AIPD) e determinar se o tratamento "pode resultar em alto risco" para os fins do Regulamento 2016/679* (WP248), p. 10

como são tratados irá ajudar.

- As finalidades do tratamento – se a base legal para o uso do serviço for que o tratamento é necessário para uma finalidade que seja do seu interesse legítimo, qual é esse interesse.
- Avalie se o tratamento é uma maneira necessária e proporcional de atender as finalidades;
    - Isso significa considerar se é razoavelmente possível cumprir o objetivo de outra maneira, que envolva menos tratamento de dados pessoais.
    - Por exemplo, se uma empresa deseja rastrear as horas trabalhadas por um funcionário, isso pode ser feito através de um processo alternativo, em vez de rastrear a sua localização durante todo o turno, pois isso seria, claramente, desproporcional.
- Avalie os riscos para as pessoas que o tratamento apresenta e como esses riscos podem ser tratados;
    - Por exemplo, se um funcionário tiver permissão para usar um veículo para uso pessoal, o rastreamento do veículo enquanto o funcionário não estiver a trabalhar seria intrusivo e desnecessário para a finalidade do empregador. Esse risco pode ser mitigado, permitindo que o funcionário desligue o serviço fora do horário de trabalho, ativando o "Privacy Switch" ("Botão de Privacidade") disponível e garantindo que os funcionários tenham conhecimento dessa opção.
- Descreva as medidas de segurança; e
- Descreva as outras medidas para garantir a proteção de dados pessoais e demonstrar conformidade.
    - A AIPD deve abordar os outros tópicos estabelecidos neste *eBook*.
    - Em particular, a AIPD deve definir como os direitos do titular dos dados são cumpridos.

Durante a conclusão da AIPD, deve consultar o seu Encarregado de Proteção de Dados (caso tenha um). Se apropriado, também deve consultar as pessoas singulares cujos dados serão tratados ou os seus representantes - por exemplo, através da Consulta de Funcionários, do Sindicato ou do Conselho de Trabalhadores - e refletir o resultado desta consulta na AIPD.

Se a sua AIPD concluir que o uso de Dados Pessoais Reveal para suas finalidades planeadas resulta em riscos elevados e sem mitigação para as pessoas singulares, deve consultar sua autoridade de controlo (em Portugal é a Comissão Nacional de Proteção de Dados).

Necessitará de manter qualquer AIPD sob revisão e avaliar periodicamente sua implementação do serviço e o uso de Dados Pessoais Reveal relativamente à mesma.

B. Política de Privacidade

Como em todo o tratamento de dados pessoais que realiza, é sua obrigação garantir que fornece informações claras e abrangentes sobre a recolha e uso dos Dados Pessoais Reveal às pessoas singulares.

Esta seção descreve as informações que deve incluir na sua política de privacidade para cumprir os requisitos de proteção de dados. No entanto, considere se outros requisitos legais relevantes terão impacto no conteúdo da sua política de privacidade e como o serviço é implementado por si. Por exemplo, em alguns países, as leis laborais exigem que inclua informações adicionais na sua política de privacidade ou noutros documentos internos.

O RGPD exige que inclua as seguintes informações na sua política de privacidade:

- A sua identidade e detalhes de contacto (assim como os do encarregado de proteção de dados, caso tenha nomeado um);
- As finalidades e bases legais do tratamento (e, quando trata os Dados Pessoais Reveal para uma finalidade que é do seu 'interesse legítimo', quais são esses interesses);
    - As secções com as finalidades e bases legais neste *eBook* irão ajudá-lo a examinar e na sua descrição.
- As categorias de Dados Pessoais Reveal tratados (e fontes), quando não são obtidas diretamente da pessoa singular;
    - A seção 3 acima em "Que dados pessoais são recolhidos através do serviço" irá ajudá-lo a na sua descrição
- Destinatários dos Dados Pessoais Reveal e quaisquer outros países fora do EEE para os quais os dados pessoais Reveal são transferidos (juntamente com os detalhes das salvaguardas implementadas);

- Período de Conservação dos Dados Pessoais Reveal;
- Se a transmissão de quaisquer Dados Pessoais Reveal é obrigatória e as possíveis consequências da falha na transmissão desses dados;
- A existência de qualquer tomada de decisão individual automatizada (incluindo a definição de perfil), juntamente com as informações significativas sobre a lógica adjacente, bem como o significado e as consequências previstas desse tratamento para o titular dos dados;
- Uma descrição dos direitos dos titulares de dados (incluindo o direito de retirar o consentimento, se o tratamento de Dados Pessoais Reveal for baseado no consentimento da pessoa singular) e a possibilidade de reclamação a uma autoridade de controlo.

A política de privacidade fornecida também deve cumprir requisitos adicionais nos termos do art. 12.º do RGPD (por exemplo, as informações que fornece às pessoas singulares são concisas, transparentes, inteligíveis, e facilmente acessíveis, e em linguagem clara e simples).

Utilizadores do serviço na França
Além dos requisitos do RGPD indicados acima, a Lei de Proteção de Dados da França exige que informe as pessoas singulares do seu direito de definir diretrizes sobre o uso dos seus dados pessoais após sua morte.

Aviso no Veículo

Dado que a recolha de Dados Pessoais Reveal é uma recolha de dados menos visível para as pessoas singulares mas pode ter consequências significativas, deve fazer esforços específicos para chamar à atenção dos motoristas para o uso do serviço. Além da política de privacidade abrangente descrita acima, as orientações regulatórias afirmam que também deve informar claramente os motoristas que um dispositivo de rastreamento foi instalado no veículo que conduzem e que os seus movimentos (e comportamento na condução, se a tecnologia relevante for implantada) estão a ser rastreados. Idealmente, essas informações devem ser exibidas com destaque em todos os veículos relevantes, à vista do motorista.[2]

Utilizadores do serviço na Polónia
Além do conteúdo acima indicado, em que a implementação do serviço equivale à monitorização de funcionários, o aviso no veículo também deve estabelecer:
- Que dados são recolhidos e gravados;
- Onde e por quanto tempo esses dados são armazenados; e
- Quem tem acesso aos dados[3].

Cumprimento de Políticas

Se os Dados Pessoais Reveal forem usados para impor as suas regras e normas, deve garantir que isso seja lícito e que os funcionários saibam quais são as regras relevantes e que serão monitorizados por si para garantir que são cumpridas, por meio do serviço.

C. Registo de Atividades de Tratamento

Como Responsável pelo Tratamento, necessita de manter um Registo de Atividades de Tratamento ('RAT'), conforme estabelecido no Art. 30.º do RGPD. Necessita de garantir que o tratamento de Dados Pessoais Reveal seja coberto pelo seu RAT. As informações que terá de incluir são:
- Nome e detalhes de contacto da sua organização (e, quando aplicável, o nome e os detalhes de contacto do seu encarregado de proteção de dados, representante e / ou responsável conjunto);
- A finalidade da utilização dos Dados Pessoais Reveal;
- Uma descrição das categorias de Dados Pessoais Reveal e as categorias de titulares dos dados cujos dados são tratados;
    - A Seção 3 acima, em "Que dados pessoais são recolhidos através do serviço?" irá ajudá-lo a na sua descrição
- As categorias de destinatários a quem os Dados Pessoais Reveal serão divulgados;

[2] Grupo de Trabalho do Artigo 29, *Parecer 2/2017 sobre o tratamento de dados no local de trabalho* (WP249), p.20
[3] Gabinete de Proteção de Dados Polaco, *Proteção de dados no local de trabalho, orientações para empregadores,* p. 37

- A Seção 5 acima, em "Quem tem acesso aos Dados Pessoais Reveal?", irá ajudá-lo a na sua descrição. Deve também listar os destinatários a quem dá acesso aos Dados Pessoais Reveal.
- Transferências de Dados Pessoais Reveal para países fora do EEE;
  - A Seção 6 acima, em "*A Verizon transfere Dados Pessoais Reveal para fora do Espaço Económico Europeu ('EEE')?*" explica para onde os dados são transferidos e que salvaguardas são usadas para proteger os Dados Pessoais Reveal.
- Prazos:
  - A Seção 7 acima, sobre "*Durante quanto tempo é que a Verizon mantém os Dados Pessoais Reveal?*" tem a explicação.
- Informações acerca das medidas de segurança, sempre que possível.
  - Consulte o Anexo de segurança da informação de sistemas internos da Verizon para obter uma descrição das medidas de segurança técnicas e organizativas que a Verizon implementa para cumprir com suas obrigações no âmbito do RGPD no seguinte URL: https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit

A Verizon tem informações disponíveis para o ajudar nesta esta obrigação no seguinte link: https://www.verizon.com/about/privacy/data-processing-activities

Utilizadores do serviço no Reino Unido
Caso trate dados de infrações criminais e a sua base legal para o tratamento é uma das condições estabelecidas no Anexo 1 da Lei de Proteção de Dados de 2018, será necessário adicionar colunas ao RAT (relacionadas com base legal e as condições de tratamento e conservação / eliminação dos dados relevantes de acordo com o Documento de Política Apropriado, se necessário).

D. Finalidades

Necessita de identificar as finalidades desejadas ao implementar o serviço e usar os Dados Pessoais Reveal, por exemplo:

- Detetar e impedir a perda de propriedade da sua organização;
- Melhorar a produtividade dos funcionários;
- Otimizar rotas e recursos e economizar combustível;
- Fornecer aos seus clientes informações de rastreamento ao vivo;
- Garantir a segurança dos seus funcionários, como garantir que sejam respeitados intervalos para descanso e refeição.

É importante que tenha claras as finalidades para os quais o serviço é implementado desde o início.

- Necessita de uma "base legal" para cada finalidade separada para a qual trata os Dados Pessoais Reveal;
- Necessita garantir que não trata mais Dados Pessoais Reveal do que é razoavelmente necessário para essa finalidade;
- Necessita de dizer às pessoas individuais quais são essas finalidades.

Depois de recolher Dados Pessoais Reveal para essas finalidades, apenas poderá usar Dados Pessoais Reveal para essas finalidades ou para outras finalidades compatíveis com essas finalidades. Às vezes, a lei aplicável permite exceções a este princípio.

Utilizadores do serviço na França
Os dispositivos de geolocalização só podem ser instalados em veículos usados pelos funcionários para as seguintes finalidades [4]:

- Rastreamento, justificação e faturação de serviços de transporte de passageiros;
- Garantir a segurança dos funcionários, mercadorias e veículos (em particular, localizar veículos roubados);
- Otimizar a alocação de recursos onde os serviços são prestados em grandes áreas geográficas,

[4] Orientações da CNIL (autoridade de controlo Francesa) relativas à geolocalização em veículos de funcionários, 2018

particularmente no contexto de serviços de emergência;
- Acompanhamento do horário de trabalho (mas apenas quando não há métodos alternativos para acompanhar o horário de trabalho);
- Cumprimento de obrigações legais ou regulamentares;
- Garantir que as regras do empregador em relação ao uso de veículos de trabalho sejam respeitadas.

Por outro lado, é proibido o uso de um dispositivo de geolocalização instalado em veículos de funcionários [5]:
- Para monitorizar a adesão aos limites de velocidade;
- Para rastrear permanentemente os funcionários;
- Para rastrear o tempo de trabalho, quando estão disponíveis métodos alternativos;
- No veículo de um funcionário que tem liberdade na organização da sua função (por exemplo, um representante de vendas);
- Para rastrear o uso privado do veículo onde o uso privado é permitido (por exemplo, durante os intervalos ou por funcionários que podem organizar livremente as suas viagens); ou
- Para rastrear representantes de sindicatos ou similares atuando no âmbito das suas funções.

Utilizadores do serviço na Alemanha
Sistemas de rastreamento através dos quais os funcionários podem ser monitorizados permanentemente geralmente não são permitidos.[6]

Utilizadores do serviço na Polónia
Se, e na medida em que a implementação do serviço constituir monitorização de funcionários, as organizações só poderão tratar os Dados Pessoais Reveal com a finalidade legítima de "garantir que os funcionários façam uso efetivo do seu tempo de trabalho e uso adequado dos seus equipamentos e ferramentas". A autoridade de controlo Polaca sugere que esse objetivo legítimo é bastante amplo e pode permitir:
- Localizar um veículo em caso de roubo;
- Investigar a responsabilidade de um funcionário por danos a um veículo; ou
- Otimizar rotas e recursos e economizar combustível.

Utilizadores do serviço em Portugal
Os serviços não podem ser usados para monitorizar o comportamento dos funcionários e só podem ser implementados em veículos usados pelos funcionários para as seguintes finalidades permitidas[7]:

- **Gestão de frota onde são fornecidos serviços:**
  - Serviços de assistência técnica;
  - Distribuição de bens;
  - Transporte de passageiros;
  - Transporte de marcadorias; ou
  - Segurança privada.

- **Proteção de bens:**
  - Transporte de materiais perigosos; e
  - Transporte de materiais de alto valor.

Nos casos em que os serviços são implementados especificamente para localizar veículos operados por funcionários em caso de roubo, o empregador não pode aceder aos dados de geolocalização recolhidos até, e a menos, que o veículo seja roubado. Outros dados do veículo (como velocidade média, travagem, consumo de combustível) podem ser recolhidos, mas não vinculados a dados pessoais que identifiquem o motorista.

E. Legitimidade

[5] Orientações da CNIL (autoridade de controlo Francesa) relativas à geolocalização em veículos de funcionários, 2018
[6] Comissário para a Proteção de Dados e a Liberdade de Informação Rhineland-Palatinate, *Sobre a legalidade do rastreamento dos funcionários por GPS*; Comissário para a Proteção de Dados e a Liberdade de Informação Baden-Wuerttemberg, *Proteção de dados no contexto laboral*, 2018, pp. 36- 37
[7] Orientações da CNPD e do código do trabalho

Necessitará de identificar uma base legal nos termos do art. 6.º do RGPD para cada finalidade para a qual trata Dados Pessoais Reveal. Dependendo da sua situação, pode estar a usar Dados Pessoais Reveal porque é necessário para:

- **Cumprir uma obrigação legal:** por exemplo, quando tem uma obrigação legal de monitorizar o horário de uso / condução de veículos e coloca um tacógrafo num veículo;
- **Realizar um contrato com o titular dos dados:** por exemplo, quando uma boa condução é uma condição do emprego;
- **Obter um objetivo que seja do seu interesse legítimo:** por exemplo, manter os seus motoristas (e outros utilizadores da estrada) seguros, impor bons hábitos ao motorista, monitorizar a frota, melhorar a eficiência de combustível e manutenção, defender-se de acidentes e acusações falsas, garantir saúde e segurança do pessoal e auxiliar nos prémios de seguro.

É imperativo que garanta que possui uma base legal legítima para tratar os dados e que o possa justificar a uma Autoridade de Controlo, quando necessário.

Necessita de demonstrar que o tratamento de Dados Pessoais Reveal é "necessário". "Necessário" significa que o tratamento de Dados Pessoais Reveal será uma maneira direcionada e proporcional de atingir seu objetivo; o tratamento deve ser "mais do que desejável, mas menos do que indispensável ou absolutamente necessário"[8]. A sua avaliação deve ser baseada em factos, levando em consideração o objetivo a obter e quaisquer opções menos intrusivas para alcançar o mesmo objetivo. Se houver alternativas realistas e menos invasivas, o tratamento não será "necessário".[9]

Quando confiar em interesses legítimos, necessita de realizar e documentar um "teste de equilíbrio" para garantir que seus interesses legítimos não sejam ultrapassados pelos interesses, direitos e liberdades das pessoas singulares. O tratamento deve ser necessário para a finalidade (ou seja, proporcional à necessidade da empresa) e devem ser incluídas salvaguardas para proteger os direitos de privacidade das pessoas singulares. Se os interesses das pessoas singulares ultrapassam os seus interesses, o tratamento não deve prosseguir.

***Consentimento*:** também pode tratar Dados Pessoais Reveal se o titular dos dados o consentir. No entanto, o consentimento só é válido se for dado livremente. As pessoas singulares também devem ter a liberdade de revogar seu consentimento - sem prejuízo. Isso dificulta a obtenção de consentimento válido no contexto laboral.[10]
Muitas autoridades de controlo comentaram bases legais no contexto da telemática.
Por exemplo:

- No Reino Unido e na Polónia, onde o uso particular de um veículo é permitido, a monitorização de movimentos quando usado pessoalmente, sem o consentimento dado livremente do utilizador, raramente será justificado.[11]
- Em Portugal, o consentimento não é uma base legal válida para o processamento de dados derivados de geolocalização.[12]
- Os dispositivos de rastreamento de veículos não devem ser considerados dispositivos para rastrear ou monitorizar o comportamento ou a localização de motoristas ou outros funcionários, por exemplo, enviando alertas em relação à velocidade do veículo.[13]

[8] *South Lanarkshire Council v Scottish Information Commissioner* [2013] UKSC 55
[9] Comité Europeu para a Proteção de Dados, *Orientações 2/2019 sobre o tratamento de dados pessoais nos termos do Artigo 6, n.º 1 (b) do RGPD no contexto da prestação de serviços online a titulares de dados, adotado em 9 de abril de 2019*, pág. 7
[10] Por exemplo, o consentimento de funcionários geralmente não é considerado válido na Alemanha (Comissário de Proteção de Dados e Liberdade de Informação (LDi) NRW, 24.º *Relatório de proteção de dados e Liberdade de informação 2017-2018*, págs. 65, 66) e o consentimento não é uma base legal para o tratamento de dados pessoais no context laboral em Portugal (orientações da CNPD sobre o uso de ferramentas de geolocalização no contexto laboral e interpretação estrita das disposições do do Código do Trabalho)
[11] ICO ((autoridade de controlo Reino Unido), *Código de Práticas Laborais*, pág. 76; (Polónia) Gabinete de Proteção de Dados, *Proteção de dados no local de trabalho. Orientações para empregadores,* pág. 38
[12] Orientações da CNPD sobre o uso de ferramentas de geolocalização no contexto laboral e interpretação estrita das disposições do do Código do Trabalho

- O tratamento de dados de localização pode ser justificado quando é feito na monitorização do transporte de pessoas ou mercadorias, na melhoria da distribuição de recursos ou para a segurança do funcionário, veículo ou mercadorias transportadas, mas poderá ser excessivo quando os funcionários são livres de organizar as suas viagens como desejarem ou onde são realizados apenas para monitorizar o trabalho de um funcionário, quando pode ser monitorizado por outros meios.[14]
  Enviar informações excessivas a um cliente sobre o motorista que entrega a sua mercadoria, por exemplo fotografia de passaporte (além do nome e localização do motorista) para permitir que um cliente verifique a identidade do motorista de entrega na chegada é improvável que tenha uma base legal (haveria um 'interesse legítimo' em fornecer a fotografia para fins de identificação, mas isso é considerado desproporcional para um nível satisfatório no teste de equilíbrio).[15]

Dados de infrações criminais

Se os Dados Pessoais Reveal que trata incluirem dados de infrações criminais (à luz das leis locais e da interpretação local de 'infrações'), o Art. 10.º do RGPD restringe o tratamento desses dados pessoais. Os dados de infrações criminais só podem ser tratados quando estão sob o controle de uma 'autoridade oficial' ou quando autorizados pelas leis nacionais ou da UE aplicáveis; portanto, necessita de consultar as leis locais para identificar requisitos relevantes, por exemplo:

Utilizadores do serviço na França
De acordo com a Lei de Proteção de Dados da França, é proibida a recolha de dados pessoais relacionados ao comportamento de uma pessoa que possa ser ou venha a ser classificada como infração ou crime. Como resultado, é proibido recolher o facto de que a pessoa excedeu os limites de velocidade ou informações relacionadas ao comportamento de uma pessoa que possam revelar violações das regras de trânsito.

Utilizadores do serviço na Alemanha
A posição atual na Alemanha é que o tratamento normal de Dados Pessoais Reveal não constitui o tratamento de informações de infrações criminais. O uso dos serviços especificamente para descobrir infrações criminais seria, no entanto, restrito pela secção 26(1) BDSG (por exemplo, se os movimentos dos veículos são monitorizados para descobrir roubo, fraude ou tráfico de drogas pelos funcionários - note que as infrações por excesso de velocidade não são atos criminosos neste sentido). Este não seria um caso de uso "normal" do Reveal e, portanto, é provável que o tratamento para esse fim ocorra apenas de maneira excecional (por exemplo, se um empregador investigar casos em que suspeita que um funcionário cometeu um ato criminoso), mas se você usar os serviços para esse fim, deve consultar a secção 26(1) BDSG.

Utilizadores do serviço em Itália
Geralmente, o tratamento de Dados Pessoais Reveal não constitui o tratamento de informações de infrações criminais, como é entendido na Itália (apenas infrações que seriam puníveis com multa administrativa). No entanto, deve monitorizar se alguma alteração na lei local introduz qualquer infração criminal que possa ser relevante para os Dados Pessoais Reveal.

Utilizadores do serviço na Polónia
Certos requisitos específicos são aplicados ao tratamento de informações de infração criminal relacionadas com os funcionários nos termos do Código do Trabalho Polaco de 1974, ou seja, não pode confiar no consentimento de um funcionário para o tratamento dos seus dados de infração criminal. É necessária uma base legal alternativa, provavelmente a informação é tratada para cumprir uma obrigação legal ou para a declaração, exercício ou defesa em ações judiciais.

Utilizadores do serviço em Portugal
O tratamento de dados de infrações criminais para a prevenção ou deteção de um ato ilegal (como, potencialmente, a prática de infrações por excesso de velocidade / trânsito) é permitido em determinadas

[13] Grupo de Trabalho do Artigo 29, *Parecer 13/2011 sobre serviços de Geolocalização em dispositivos móveis inteligentes* (WP 185)
[14] Grupo de Trabalho do Artigo 29, *Parecer 5/2005 sobre o uso de dados de localização com o objetivo de fornecer serviços de valor acrescentado* (WP115)
[15] Grupo de Trabalho do Artigo 29, *Parecer 2/2017 sobre o tratamento de dados no local de trabalho* (WP249)

circunstâncias, e quando necessário para os fins ou em conexão com quaisquer procedimentos legais, consultoria jurídica ou conforme necessário para estabelecer, exercer ou defender direitos legais. Os dados pessoais devem, no entanto, ser pseudonimizados até sete dias após a recolha.

Utilizadores do serviço na Espanha
Geralmente, o tratamento de Dados Pessoais Reveal não constitui o tratamento de informações de infrações criminais, como é entendido na Espanha (apenas a violação das regras de tráfego). No entanto, deve monitorizar se alguma alteração nas leis locais introduz qualquer infração criminal que possa ser relevante para os Dados Pessoais Reveal, pois o tratamento de informações de infrações criminais na Espanha é restrito - as únicas (potencialmente) circunstâncias relevantes nas quais o tratamento de informações de infrações criminais podem ocorrer neste contexto são quando: (i) a finalidade é a prevenção, investigação, deteção ou repressão de infrações ou execuções penais; (ii) o tratamento é coberto por uma regra com força e efeito estatutário ou pelo direito da UE.

Utilizadores do serviço no Reino Unido
No Reino Unido, precisa de garantir que, para além de uma base legal, seja também considerada uma condição para o tratamento nos termos do Artigo 9.º do RGPD ou do Anexo 1 da Lei de Proteção de Dados de 2018. Por exemplo, em relação aos dados de infrações criminais, a Lei de Proteção de Dados de 2018 permite o tratamento de dados pessoais para a prevenção ou deteção de um ato ilegal (como, potencialmente, a prática de uma infração por excesso de velocidade ou de tráfego) em determinadas circunstâncias, e onde isso é necessário para as finalidades ou em conexão com quaisquer procedimentos legais, consultoria jurídica ou conforme necessário para estabelecer, exercer ou defender direitos legais.

F. Minimização dos Dados

Deverá garantir que apenas usa Dados Pessoais Reveal que sejam adequados, relevantes e limitados ao necessário (à luz das suas finalidades). Fundamentalmente, significa que deve identificar e usar a quantidade mínima de Dados Pessoais Reveal necessária para cumprir as suas finalidades.

Se permitir que os funcionários façam uso pessoal dos veículos, geralmente não há necessidade de recolher informações sobre onde o veículo é levado fora do horário de trabalho. O serviço tem a funcionalidade de garantir que os funcionários não sejam monitorizados quando estiverem fora do horário de trabalho. Isso é conhecido como "Privacy Switch" ("Botão de Privacidade") e é uma maneira simples e económica de garantir a conformidade. Em alguns países (como França, Alemanha e Portugal), é necessário permitir que os funcionários usem o "Privacy Switch" ("Botão de Privacidade") sob orientação regulamentar.[16]

G. Exatidão dos Dados

Necessitará de garantir que os Dados Pessoais Reveal que usa não sejam incorretos ou factualmente falsos. No contexto dos Dados Pessoais Reveal, é particularmente importante que tome medidas para garantir a precisão dos dados pessoais (por exemplo, garantir que os registos dos veículos atribuídos aos funcionários sejam feitos com precisão) e considere cuidadosamente quaisquer desafios à precisão dos dados pessoais (por exemplo, um motorista que contesta sua localização em um determinado momento).

H. Conservação de Dados Pessoais Reveal

Os Dados Pessoais Reveal devem ser apenas mantidos pelo tempo necessário para a sua finalidade específica. Necessita de considerar se existem requisitos de conservação legal aplicáveis (por exemplo, para manter registos de horário de trabalho). Isto necessita de ser abordado na sua política de conservação.

I. Segurança dos Dados Pessoais Reveal

[16] Comissário da Baviera para a Proteção de Dados, *27.º Relatório de Atividades de 2016*, pág. 241; Orientações da CNIL (autoridade de controlo Francesa) relativas à geolocalização em veículos de funcionários, 2018; Deliberação 7680/2014 da CNPD

Necessitará de implementar medidas "técnicas e organizativas apropriadas" para garantir a confidencialidade, integridade e disponibilidade dos Dados Pessoais Reveal, de acordo com o art. 32.º do RGPD. Uma avaliação de risco pode ser usada para identificar problemas específicos apresentados na sua implementação do Reveal e uso dos Dados Pessoais Reveal, para determinar o nível de segurança "apropriado" (levando em consideração situação existente e os custos de implementação). Uma vez implementado, deve testar regularmente as suas medidas técnicas e organizativas para garantir que continuem apropriadas. Quando partilha Dados Pessoais Reveal com outra organização que atua como Subcontratante em seu nome, será necessário garantir que o Subcontratante forneça garantias suficientes (e concorde contratualmente) para também implementar as medidas técnicas e organizativas apropriadas para proteger os dados.

No caso de uma violação de segurança envolvendo dados pessoais, necessitará de cumprir o art. 33.º e 34.º do RGPD. Nós o notificaremos sem demora injustificada. A autoridade controlo poderá ter de ser notificada por si no prazo de 72 horas após tomar conhecimento do incidente (a menos que considere improvável que seja um risco para os direitos e liberdades das pessoas singulares. Nos casos em que a violação possa resultar num alto risco para os direitos e liberdades das pessoas singulares também precisará de notificar as pessoas afetadas sem demora injustificada. Deve considerar como identificaria a ocorrência de uma violação envolvendo os Dados Pessoais Reveal, quais as medidas que tomaria para atenuar a violação e como escalaria e avaliaria uma violação para determinar se a notificação é necessária.

Utilizadores do serviço na França

De acordo com as orientações da CNIL sobre geolocalização nos veículos dos funcionários[17], deve implementar, em particular, o seguinte

- Uma política de controle de acessos;
- Medidas de segurança para transferência de dados; e
- Um registo de acesso aos dados e operações de tratamento.

Utilizadores do serviço na Espanha

Quando os dados pessoais estão a ser retificados ou apagados, a Lei Espanhola de Proteção de Dados exige que os Responsáveis pelo Tratamento 'bloqueiem' os dados como parte das medidas técnicas e organizativas que implementam para cumprir o art. 32.º - isto significa que os dados pessoais relevantes devem ser extraídos e armazenados numa base de dados separada, e medidas técnicas e organizativas precisam de ser adotadas para impedir o tratamento dos dados (incluindo qualquer acesso ou visualização). Os dados pessoais relevantes precisam de ser mantidos numa base de dados separada e protegida, a fim de atender a quaisquer solicitações que possam ser recebidas de órgãos públicos competentes (como tribunais, procuradores, autoridades de controlo etc.) ou no caso de a transferência dos dados para esses órgãos públicos seja necessária para o exercício ou defesa de direitos judiciais. Para calcular o período durante o qual os dados pessoais precisam de ser mantidos 'bloqueados', os períodos de conservação para diferentes ações judiciais que possam surgir como consequência do tratamento dos dados relevantes precisam de ser considerados. Os dados pessoais podem ser totalmente eliminados após o término dos períodos de conservação relevantes.

Como Responsável pelo Tratamento dos Dados Pessoais Reveal, precisa de garantir que consegue cumprir essa obrigação. A Verizon ajuda-o a cumprir essa obrigação, permitindo que obtenha cópias de determinados Dados Pessoais Reveal por meio do painel de *self service* Reveal e fornecendo-lhe outros Dados Pessoais Reveal mediante solicitação.

J. Direitos dos Titulares dos Dados

Necessitará de identificar como cumprirá a sua obrigação de responder às solicitações de pessoas singulares. Sob o RGPD, as pessoas singulares têm os seguintes direitos em relação aos seus dados pessoais:

- O direito de acesso;
- O direito de retificação;
- O direito ao apagamento;
- O direito à limitação do tratamento;

[17] Orientações da CNIL (autoridade de controlo Francesa) relativas à geolocalização em veículos de funcionários, 2018

- O direito de portabilidade;
- O direito de oposição;
- Direitos em relação à tomada de decisões automatizadas e definição de perfis.

Na sua política de privacidade deve informar as pessoas singulares que esses direitos existem.

A aplicabilidade desses direitos pode ser limitada (por exemplo, o direito à portabilidade de dados existe apenas quando os dados pessoais são processados com base na necessidade legal ou consentimento contratual) e pode aplicar isenções (por exemplo, se a divulgação de informações afetasse adversamente os direitos de terceiros, que podem incluir a proteção de segredos comerciais).

Geralmente, necessita de responder a estas solicitações no prazo de um mês e garantir que a sua resposta atenda as obrigações adicionais nos termos do art. 12.º do RGPD (por exemplo, as informações fornecidas às pessoas singulares são concisas, transparentes, inteligíveis e facilmente acessíveis e em linguagem clara e simples).

Sempre que possível, a Verizon pode ajudá-lo a cumprir com as solicitações de pessoas singulares relacionados ao serviço.

Utilizadores do serviço na França
Sob a Lei de Proteção de Dados da França, as pessoas singulares têm o direito de definir orientações sobre o uso dos seus dados pessoais após a morte. É necessário que garanta que consiga responder a este tipo de solicitações.

K. Partilha de Dados Pessoais Reveal

Além de as pessoas solicitarem acesso a seus próprios dados, necessitará de determinar como responderá às solicitações de acesso aos Dados Pessoais Reveal de terceiros. Isso pode incluir, por exemplo, solicitações de organismos responsáveis pela aplicação da lei e seguradoras, quando, por exemplo, um veículo esteve envolvido num acidente.

Qualquer partilha de Dados Pessoais Reveal (incluindo, por exemplo, com outras organizações do seu grupo corporativo ou com outro provedor de serviços) precisará de atender a todos os requisitos de proteção de dados estabelecidos neste *eBook* (por exemplo, a partilha deve ser legal, proporcional, transparente, etc.) Necessitará de considerar se precisam ser estabelecidos com a organização contratos ou outros acordos (por exemplo, quando a outra organização atua como Subcontratante em seu nome ou como Responsável Conjunta pelo Tratamento). Nos casos em que essa partilha envolva uma transferência de Dados Pessoais Reveal para fora do Espaço Económico Europeu ('**EEE**'), necessitará de garantir que a transferência é permitida pelo RGPD

Utilizadores do serviço na França
Nos termos das orientações da CNIL, deve limitar o acesso a informações relacionadas a (ou resultantes de) dispositivos de geolocalização a (conforme relevante): (i) os seus próprios funcionários autorizados, (ii) o empregador da pessoa singular relacionada com as informações de geolocalização; e (ii) funcionários autorizados de um cliente ao qual são fornecidos serviços relevantes. Por uma questão de princípio, o nome do motorista não deve ser partilhado, a menos que essas informações sejam particularmente relevantes e necessárias.

L. Decisões Automatizadas

A lei de proteção de dados proíbe que as organizações tomem decisões com base apenas no tratamento automatizado de dados pessoais, onde a decisão teria efeitos legais ou efeitos significativos da mesma forma. Necessitará de identificar essa utilização do serviço. Isso pode ser relevante quando:

- O salário de um motorista é calculado automaticamente com base no horário em que ele inicia / termina a condução de um veículo;
- Um motorista automaticamente avisado ao entrar numa área protegida por área geográfica;

- A elegibilidade de um motorista para um bónus é calculada automaticamente com base no número de trabalhos atribuídos e concluídos por este, conforme registado pelo serviço.

Se houver uma revisão humana significativa de uma decisão antes de ser tomada, essas restrições não se aplicarão.

As organizações têm permissão para tomar esse tipo de decisão exclusivamente automatizada quando a decisão é:

- Necessária para a execução ou celebração de um contrato;
- Autorizada pela legislação da União ou do Estado-Membro a que o Responsável pelo Tratamento está sujeito e que também estabelece medidas adequadas para salvaguardar os direitos, liberdades e interesses legítimos do titular dos dados; ou
- Baseada no consentimento explícito do titular dos dados.

Quando a tomada de decisão individual automatizada ocorre, necessita de fornecer informações claras para as pessoas singulares acerca disso (consulte 'Política de Privacidade', acima) e, pelo menos, permitir que as pessoas singulares tenham o direito de obter intervenção humana no processo de tomada de decisão, para manifestar o seu ponto de vista e contestar a decisão.

Utilizadores do serviço em Portugal
Não é permitido o uso de dados de geolocalização e telemetria de veículos para a tomada de decisões automatizadas.[18]

M. Funcionários/Comissão de Trabalhadores/Consulta Sindical

De acordo com a legislação laboral, pode ser exigido que consulte os seus funcionários, comissão de trabalhadores ou sindicato sobre a implementação do serviço ou caso opte por utilizações adicionais dos Dados Pessoais Reveal. Como alternativa, pode ser exigido que consulte sindicatos ou representantes de funcionários sob os termos de quaisquer acordos voluntários em vigor. Mesmo que não seja necessário, pode considerar apropriado consultar os funcionários sobre a implementação do serviço e o uso de Dados Pessoais Reveal como parte do processo de AIPD.

Se acordar um contrato vinculativo com a comissão de trabalhadores, esse contrato constituiria uma "regra mais específica" para garantir os direitos de proteção de dados dos funcionários, de acordo com o Artigo 88.º, n.º 1 do RGPD. Isto significa que esse contrato pode, em algumas circunstâncias, fornecer segurança jurídica sobre como o Reveal pode ser usado na sua organização. Para atender ao requisito de uma "regra mais específica" de acordo com o Artigo 88.º, nº 1 do RGPD, o contrato de trabalho deve ser vinculativo de acordo com as leis laborais locais e deve atender adequadamente aos interesses de proteção de dados dos funcionários (consulte o Artigo 88.º, n.º 2 do RGPD). Em caso de dúvida, deve procurar aconselhamento jurídico.

Utilizadores do serviço na França
De acordo com o Art. L2312-38 do Código do Trabalho Francês, deve consultar e informar a Comissão de Trabalhadores (*Conseil Economique et Social*) antes de implementar qualquer sistema ou meio que permita monitorizar a atividade dos funcionários, como o rastreamento de localização geográfica.

Utilizadores do serviço na Alemanha
Nos termos da Secção 87, n.º 6 Lei Constitucional Laboral (Betriebsverfassungsgesetz -BetriebsVG), a comissão de trabalhadores, se existir na sua organização, tem o direito de co-determinar a introdução e o uso de equipamentos técnicos destinados a monitorizar o comportamento ou desempenho dos funcionários. Não é permitido o 'controle' permanente do comportamento e desempenho dos funcionários por meio de

[18] Orientação da CNPD sobre o uso de ferramentas de geolocalização no contexto laboral e interpretação estrita das disposições do Código do Trabalho

monitorização - se é o empregador, é necessário excluir esse 'controle' permanente dos funcionários por meio de acordos com a comissão de trabalhadores ou regulamentos unilateralmente vinculativos.[19]

A Secção 26, n.º 4 da Lei Federal de Proteção de Dados declara explicitamente que o tratamento de dados pode ser permitido com base em contratos laborais, se estes cumprirem os requisitos do Artigo 88.º, n.º 2 do RGPD.

Utilizadores do serviço em Itália
Pode precisar de consultar os sindicatos da sua organização, se os houver, ou obter autorização da Organização do Trabalho competente sobre a implementação do serviço e seu uso dos Dados Pessoais Reveal para cumprir o Art. 4.º, n.º 2 da Lei n.º 300/1970 (Estatuto do Trabalhador Italiano), a menos que os Dados Pessoais Reveal que trata sejam limitados aos dados estritamente necessários para cumprir as obrigações legais.

Utilizadores do serviço na Polónia
Deve definir a finalidade, o âmbito e os métodos de monitorização no seu Regulamento do Trabalho (uma política interna obrigatória para empregadores com mais de 50 funcionários na Polónia) ou no Acordo Coletivo de Trabalho Corporativo. Se houver sindicatos na sua organização, as alterações no Regulamento do Trabalho ou no Acordo Coletivo de Trabalho Corporativo exigirão cooperação com os sindicatos.

No que diz respeito aos funcionários existentes, deve informá-los que pretende iniciar um sistema de monitorização. Isso deve ser feito o mais tardar duas semanas antes do lançamento do sistema de monitorização.

Utilizadores do serviço em Portugal
Nos termos do Art. 21.º do Código do Trabalho Português, deve informar e consultar a Comissão de Trabalhadores antes da implementação de quaisquer sistemas ou meios que permitam a monitorização de funcionários, tal como a monitorização por geolocalização.

Utilizadores do serviço em Espanha
Nos termos do Art. 64.º, n.º 1 do Estatuto do Trabalhador Espanhol, necessitará de informar os representantes dos funcionários antes da implementação de qualquer medida que possa afetar os funcionários, que inclui a implementação de dispositivos de geolocalização ou qualquer outra solução de monitorização.

Em apoio ao exposto, o Art. 90.º, n.º 2 da Lei Orgânica 3/2018, de 5 de dezembro, relativa à Proteção de Dados Pessoais e à concessão de direitos digitais afirma que, antes da implementação dos dispositivos de geolocalização, os representantes dos funcionários e dos trabalhadores precisam de ser informados sobre a existência e características desses dispositivos.

N. Mitigação do Risco e Proteção de Dados Desde a Conceção e Por Defeito

Deve garantir que todas as etapas necessárias para mitigar os riscos para as pessoas singulares (identificadas durante o processo de AIPD) e para cumprir com os requisitos de 'proteção de dados desde a conceção e por defeito' foram tomadas. Proteção de dados desde a conceção significa que as questões de privacidade devem ser consideradas e abordadas no início de uma atividade de tratamento de dados (ou seja, a fase de design) e durante todo o ciclo de vida dessa atividade de tratamento. A proteção de dados por defeito exige que garanta que apenas os dados mínimos necessários para atingir as suas finalidades sejam processados (por exemplo, em vez de permitir amplo acesso aos Dados Pessoais Reveal, o acesso deve ser restrito a indivíduos específicos, com base em 'necessidade de conhecimento')

As orientações das autoridades de controlos estabelecem exemplos de mitigação de riscos no contexto da telemática e monitorização de funcionários:

- Os motoristas devem ter permissão para desativar temporariamente o rastreamento de local em

[19] Comissário para a Proteção de Dados e a Liberdade de Informação Baden-Wuerttemberg, *Proteção de dados no contexto laboral*, 2018; Centro Independente para a Proteção de Dados Schleswig-Holstein, Relatório de Atividades 2017-2018, 103

determinadas circunstâncias (por exemplo, ao visitar uma clínica médica), quando os funcionários têm permissão para fazer uso pessoal dos veículos da organização.[20]

- Quando existe a necessidade de monitorizar a localização de um veículo fora do horário de trabalho de um funcionário (por exemplo, para prevenir o roubo do veículo), a implementação deverá ser proporcional aos riscos, por exemplo, a localização do veículo não fica registada (ou visível para si) fora do horário de trabalho, a menos que deixe um círculo amplamente definido (por exemplo, região).[21]
- O número de pessoas com acesso aos Dados Pessoais Reveal deve ser minimizado. Os funcionários devem ser treinados adequadamente e sujeitos a obrigações de confidencialidade e segurança.[22] Considere quais os funcionários mais apropriados para aceder aos Dados Pessoais Reveal (não deverão ser, por exemplo, gestores de linha).[23]

O. Designação de um Encarregado de Proteção de Dados (EPD ou 'DPO')

No Art. 37º do RGPD estão estabelecidas várias razões para nomear um encarregado de proteção de dados ('DPO'). As suas atividades de tratamento existentes talvez ainda não exijam a indicação de um DPO. No entanto, o seu uso dos serviços pode desencadear a necessidade de nomear um DPO à luz do Art. 37.º, n.º 1 (b), que exige a nomeação de um DPO sempre que as atividades principais de uma organização consistam em monitorização regular e sistemática dos titulares de dados em uma grande escala. O uso dos serviços para monitorizar motoristas e o seu comportamento ao conduzir enquadra-se, provavelmente, no âmbito do Art. 37.º, n.º 1 (b), caso em que deverá nomear um DPO. Outras disposições do RGPD (Arts. 38.º e 39.º) estabelecem requisitos relacionados à posição e tarefas do DPO - também precisará de os cumprir se for necessária a nomeação de um DPO.

Utilizadores do serviço na Alemanha

Nos termos da Secção 38 da Lei Federal de Proteção de Dados (BDSG) é obrigado a designar um DPO se empregar permanentemente pelo menos 20 pessoas para o tratamento automatizado de dados pessoais ou se o tratamento de dados pessoais que executa exija que realize uma AIPD. É provável que precise de nomear um DPO se usar os serviços na Alemanha.

Outras Informações

Legislação

- Regulamento Geral de Proteção de Dados (EU) 2016/679 ('RGPD')
- Lei de Proteção de Dados 2018 (UK)
- Lei 58/2019, de 8 de agosto de 2019 (Portugal)
- Código do Trabalho (Portugal)
- Lei Constitucional n.º 3/2018, de 5 de dezembro de 2018, na Proteção de Dados Pessoais e Garantia de Direitos Digitais (Espanha)
- Lei Federal de Proteção de Dados (Bundesdatenschutzgesetz – BDSG) 2018 (Alemanha)
- Lei Constitucional Laboral (Betriebsverfassungsgesetz -BetriebsVG) (Alemanha)
- Decreto Legislativo n.º 196/2003 (Código de Proteção de Dados italiano) (itália)
- Lei n.º 300/1970 (Estatuto dos Trabalhadores Italianos) (Itália)
- Decreto Legislativo n.º 101/2018 (Itália)
- Lei de Proteção de Dados Francesa n.º 78-17 (França)
- Código do Trabalho Francês (França)

Jurisprudência

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

[20] Grupo de Trabalho do Artigo 29 *Parecer 2/2017 sobre o tratamento de dados no local de trabalho* (WP249), p.20
[21] Grupo de Trabalho do Artigo 29 *Parecer 2/2017 sobre o tratamento de dados no local de trabalho* (WP249), p.20
[22] ICO (autoridade de controlo do Reino Unido)*, Código de Práticas Laborais*, pág. 67
[23] ICO (autoridade de controlo do Reino Unido)*, Código de Práticas Laborais*, pág. 67

Orientação Regulamentar

UE

- Grupo de Trabalho do Artigo 29, *Parecer 5/2005 sobre o uso de dados de localização com o objetivo de fornecer serviços de valor acrescentado* (WP115)
- Grupo de Trabalho do Artigo 29, *Parecer 13/2011 sobre serviços de Geolocalização em dispositivos móveis inteligentes* (WP 185)
- Grupo de Trabalho do Artigo 29, *Orientações sobre Avaliações de Impacto sobre a Proteção de Dados (AIPD) e determinar se o tratamento "pode resultar em alto risco" para os fins do Regulamento 2016/679* (WP248)
- Grupo de Trabalho do Artigo 29, *Parecer 2/2017 sobre o tratamento de dados no local de trabalho* (WP249)
- Grupo de Trabalho do Artigo 29, *Orientações sobre tomada de decisão individual automatizada e criação de perfil para os fins do Regulamento* (WP251)
- Comité Europeu para a Proteção de Dados, *Orientações 2/2019 sobre o tratamento de dados pessoais nos termos do Artigo 6, n.º 1 (b) do RGPD no contexto da prestação de serviços online a titulares de dados (versão para consulta pública)*

França

- Orientações da CNIL relativas à geolocalização em veículos de funcionários, 2018

Alemanha

- Comissário de Proteção de Dados e Liberdade de Informação Rhineland-Palatinate *Sobre a legalidade do rastreamento dos funcionários por GPS,*
- Comissário para a Proteção de Dados e a Liberdade de Informação Baden-Wuerttemberg, *Proteção de Dados no contexto laboral*, 2018
- Conferência de Proteção de Dados das Autoridades de Controlo Federais e Estaduais (Länder) Independentes (Datenschutzkonferenz - DSK), *Breve artigo n.º 14: Proteção de Dados no contexto laboral*, de 17 de dezembro de 2018
- Comissário da Baviera para a Proteção de Dados, *27.º Relatório de Atividades de 2016*
- Conferência de Proteção de Dados das Autoridades de Controlo Federais e Estaduais (Länder) Independentes (Datenschutzkonferenz - DSK), *Breve artigo n.º* 17: *Categorias especiais de dados pessoais, de* 27 de março de 2018
- Conferência de Proteção de Dados das Autoridades de Controlo Federais e Estaduais (Länder) Independentes (Datenschutzkonferenz - DSK), *Breve artigo n.º* 19: *Informação e compromisso dos funcionários em cumprir os requisitos de proteção de dados sob o RGPD,* de 29 de maio de 2018
- 24º Relatório de Proteção de Dados e Liberdade de Informação, do Comissário de Proteção de Dados e Liberdade de Informação North Rhine-Westphalia (LDi NRW), *Posicionamento via satélite para determinar a posição dos veículos da empresa - nenhum meio permitido de monitorizar os funcionários,*
- Comissário de Proteção de Dados e Liberdade de Informação de Berlim, *Relatório anual 2018*
- Centro Independente para a Proteção de Dados Schleswig-Holstein, *Relatório de Atividades 2017 – 2018*
- Comissário de Proteção de Dados Lower Saxony, *Monitorização GPS de veículos da empresa,* 24º Relatório de Atividades 2017-2018

Polónia

- Gabinete de Proteção de Dados, *Proteção de dados no local de trabalho. Orientações para empregadores*

Portugal

- *Deliberação 7680/2014 sobre o uso de geolocalização no contexto laboral*, da CNPD

Reino Unido

- ICO*, Código de Práticas Laborais e Orientação Suplementar*

GDPR Checklist

Artigo RGPD	Tema	Relevância para o Reveal	Referência *eBook*

Art. 1, 2 ou 3	Assunto e objetivos; material; âmbito territorial	Sem relevância específica	N/A
Art. 4	Definições	Define conceitos de 'dados pessoais' e 'categorias especiais' de dados pessoais	" *FAQs Reveal* ", secção 3 e 4
Art. 5	Princípios e responsabilidade	O tratamento de Dados Pessoais Reveal deve obedecer aos princípios de proteção de dados e o Responsável pelo Tratamento deve ser capaz de demonstrar conformidade	"*Abordagem aos requisitos de proteção de dados", geral*
Art. 6 e 7	Licitude do tratamento e condições para o consentimento	Deve existir uma base legal para cada finalidade de tratamento de Dados Pessoais Reveal	" *Abordagem aos requisitos de proteção de dados* ", secção E
Art. 8	Condições para o consentimento de crianças em SSI	Sem relevância específica	N/A
Art. 9 e 10	Tratamento de categorias especiais de dados pessoais e informações relativas a infrações penais	Deve existir uma condição para cada finalidade de tratamento de Dados Pessoais Reveal, em que os dados pessoais são dados de categoria especial ou informações de infrações criminais	"*Reveal FAQs*", section 4, and " *Abordagem aos requisitos de proteção de dados* ", secção E
Art. 11	Tratamento que não exige identificação	Sem relevância específica	N/A
Art. 12	Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados	Qualquer informação fornecida a pessoas singulares sobre os quais os Dados Pessoais Reveal são tratados deve ser concisa, transparente, inteligível e facilmente acessível, usando linguagem clara e simples.	" *Abordagem aos requisitos de proteção de dados* ", secções B e J
Art. 13 e 14	Informações a facultar aos titulares dos dados	Deve ser fornecida uma política de proteção de dados às pessoas singulares relativamente aos Dados Pessoais Reveal.	*" Abordagem aos requisitos de proteção de dados* ", secção B
Art. 15	Direito de acesso	O acesso aos Dados Pessoais Reveal deve ser fornecido às pessoas singulares mediante solicitação (sujeito a exceções)	*" Abordagem aos requisitos de proteção de dados* ", secção J
Art. 16	Direito de retificação	Os Dados Pessoais Reveal devem ser	*" Abordagem aos requisitos de proteção de dados* ",

		retificados mediante solicitação das pessoas singulares	secção J
Art. 17	Direito ao apagamento	Os Dados Pessoais Reveal devem ser apagados mediante solicitação das pessoas singulares, se o direito se aplicar	*" Abordagem aos requisitos de proteção de dados* ", secção J
Art. 18	Direito à limitação	Os Dados Pessoais Reveal devem ser limitados mediante solicitação das pessoas singulares, se o direito se aplicar	*" Abordagem aos requisitos de proteção de dados* ", secção J
Art. 19	Obrigação de notificação da retificação, apagamento ou limitação	Quando uma solicitação de retificação, apagamento ou restrição relacionada com os Dados Pessoais Reveal é recebida, terceiros para os quais os dados foram divulgados devem ser notificados da solicitação	*" Abordagem aos requisitos de proteção de dados* ", secção J
Art. 20	Direito à portabilidade dos dados	Os Dados Pessoais Reveal devem ser transferidos para as pessoas singulares (ou terceiros nomeados) mediante solicitação das mesmas, se o direito se aplicar	*" Abordagem aos requisitos de proteção de dados* ", secção J
Art. 21	Direito de oposição	Os Dados Pessoais Reveal não devem mais ser tratados mediante solicitação de pessoas singulares, se o direito se aplicar	*" Abordagem aos requisitos de proteção de dados* ", secção J
Art. 22	Decisões individuais automatizadas, incluindo definição de perfis	Decisões unicamente automatizadas sobre pessoas singulares que criam efeitos legais ou similares significativos para as mesmas só podem ser tomadas de acordo com o Art. 22.º	*" Abordagem aos requisitos de proteção de dados* ", secção L
Art. 23	Restrições	Sem relevância específica	N/A
Art. 24	Responsabilidade do Responsável pelo Tratamento	Medidas técnicas e organizativas apropriadas devem ser implementadas para garantir (e demonstrar) que o tratamento é realizado em conformidade com o RGPD	" *Abordagem aos requisitos de proteção de dados* ", geral

Art. 25	Proteção de dados desde a conceção e por defeito	As questões de proteção de dados devem ser abordadas desde o início e durante o ciclo de vida do tratamento de Dados Pessoais Reveal, e apenas devem ser tratados os dados pessoais mínimos necessários para atingir a sua finalidade.	*" Abordagem aos requisitos de proteção de dados* ", secções F e N
Art. 26	Responsáveis conjuntos	Sem relevância específica	N/A
Art. 27	Representantes dos Responsáveis pelo Tratamento ou Subcontratantes não estabelecidos na União	Sem relevância específica	N/A
Art. 28	Subcontratantes	Somente os Subcontratantes que fornecem garantias suficientes devem ser contratados para tratar Dados Pessoais Reveal e devem ser impostas, sob contrato, as obrigações dos mesmos	*" Abordagem aos requisitos de proteção de dados* ", secção I
Art. 29	Tratamento sob a autoridade do Responsável pelo Tratamento ou do Subcontratante	Sem relevância específica	N/A
Art. 30	Registos de atividades de tratamento	O tratamento de Dados Pessoais Reveal deve ser refletido no registo das atividades de tratamento	*" Abordagem aos requisitos de proteção de dados* ", secção C
Art. 31	Cooperação com a autoridade de controlo	Sem relevância específica	N/A
Art. 32	Segurança do tratamento	Devem ser implementadas medidas técnicas e organizativas apropriadas para proteger a segurança dos Dados Pessoais Reveal	*" Abordagem aos requisitos de proteção de dados* ", secção I
Art. 33 e 34	Notificação de violação de dados pessoais (à autoridade de controlo e pessoas singulares)	No caso de uma violação de dados pessoais que envolva Dados Pessoais Reveal, a notificação deve ser feita às autoridades de controlo e às pessoas afetadas se os limites forem atingidos	*" Abordagem aos requisitos de proteção de dados* ", secção I
Art. 35 e 36	Avaliação de impacto sobre a proteção de dados e consulta prévia	Uma avaliação de impacto sobre a proteção de dados deve ser executada para o tratamento de Dados	*" Abordagem aos requisitos de proteção de dados* ", secção A

		Pessoais Reveal e pode ser necessária a consulta às autoridades de controlo se o tratamento apresentar elevados riscos, e sem mitigação, para as pessoas singulares	
Art. 37, 38 and 39	Encarregado de proteção de dados	Deve ser designado um encarregado de proteção de dados relevante se as atividades principais do Responsável pelo Tratamento equivalerem à monitorização 'regular e sistemática' dos titulares de dados em larga escala ou ao tratamento de dados de categoria especial / infrações criminais em larga escala.	" *Abordagem aos requisitos de proteção de dados ",* secção Q
Art. 40, 41, 42 e 43	Códigos de conduta, certificações e acreditações	Sem relevância específica	N/A
Art. 44 - 50	Transferências	Quaisquer transferências de Dados Pessoais Reveal para fora do EEE para países que não são 'adequados' (por exemplo, para outros fornecedores de plataformas ou empresas do grupo) devem ser realizadas apenas quando houver um mecanismo de transferência ou se houver uma derrogação	" *FAQs Reveal* ", secção 6, e *" Abordagem aos requisitos de proteção de dados* ", secção K
Art. 51 - 59	Autoridade de controlo e competência, atribuições, poderes e relatórios	Sem relevância específica	N/A
Art. 60 - 67	Cooperação e coerência	Sem relevância específica	N/A
Art. 68 - 76	Comité Europeu para a Proteção de Dados	Sem relevância específica	N/A
Art. 77	Direito de apresentar reclamação a uma autoridade de controlo	Sem relevância específica	N/A
Art. 78	Direito à ação judicial contra uma autoridade de controlo	Sem relevância específica	N/A
Art. 79 - 82	Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante, e indemnização	Sem relevância específica	N/A
Art. 83 - 84	Coimas e sanções	Sem relevância específica	N/A
Art. 85 - 91	Disposições relativas a	Sem relevância específica	N/A

	situações específicas de tratamento		
Art. 92 - 93	Atos delegados e atos de execução	Sem relevância específica	N/A
Art. 94 - 99	Disposições finais	Sem relevância específica	N/A