Introduction

Verizon Connect provides Mobile Workforce Solutions in the Fleet Management and Field Service Management space. Our Products track the performance of your vehicle fleet that can have a big impact on your business. These are things like where your vehicles are, how your drivers are behaving on the road and how much fuel they use. This information is then put into digestible dashboards so you can act quickly. Reveal is a critical tool to help you get more done in less time, provide better customer service and ultimately improve results across your business. Through our Field Service products we also have the ability to manage the full lifecycle of our customers' service requests, from first customer contact, providing a quote for the work, scheduling the job, dispatch, optimal routing of a driver and taking payment.

This eBook answers FAQs about the Reveal Fleet Tracking Services ('the services' or 'Reveal') sold to you by Verizon Connect on the Reveal platform, and sets out an overview of some of the key data protection considerations and requirements that you will need to work through before, during, and after your deployment of the service. Whilst this eBook focuses predominantly on data protection issues, you should consider whether any other relevant legal requirements will impact your implementation and use of the services. For example, in some countries, employment law requirements will be triggered by use of the services in vehicles driven by employees.

Where relevant, reference has been made to regulatory guidance available at the time of publication. Regulators regularly review and revise their guidance, so you should keep a watching brief on developments in this area as it is ultimately your responsibility as the Controller of personal data collected and used through the service to ensure compliance with applicable law(s).

The information provided in this eBook does not constitute legal or professional advice. You should always consult a suitably qualified lawyer on any specific legal problem or matter. Verizon Connect assumes no responsibility for the information contained in this eBook and disclaims all liability in respect of such information.

Reveal FAQs

1. Whose information is collected through the services?
Primarily, information will be collected about the employees and contractors who drive the vehicles in which you deploy the services. Information may also be collected about other individuals (e.g. passengers or other individuals in a driver's household with access to the vehicle), depending on how and why you deploy the service.

2. How is information collected for the service?
The service collects information from two sources:

- The on-board device installed in your vehicles: This collects information about your vehicles' locations and activities. If you know (or could determine) the driver to which each vehicle is assigned, this information will also be personal data.
- We have several mobile apps across our platforms that you can install to effectively use our service, such as our Field Service related apps (Work, Workforce, Field) and our Fleet Management related Apps (Manager\Spotlight, Video, ELD). To use the app, each driver must provide certain information in the course of registering.

In this eBook, we refer collectively to any personal data collected through the service as 'Reveal Personal Data'.

3. What personal data is collected through the service?
You determine the majority of personal data that will be collected through the service; what you wish to collect will vary depending on how and why you deploy the solution. You are in complete control of the type of data that you collect. As such it is your legal responsibility to ensure that you need to obtain the data that you collect in order to use the service.

Personal data collected through the on-board device vehicle can include:

- Location data (GPS) of vehicles and individuals;
- Tachograph information (driving times);
- Speed and behaviour of the driver of the vehicle;
- Vehicle event data (e.g. involvement in an accident, entering or leaving a geofenced area);
- Other vehicle information (e.g. fuel consumption, tyre pressure, operational data).

Personal data collected through the app can include:

- Driver name;
- Driver telephone number, email address and home address;
- Driver log-in credentials;
- Driver records (e.g. vehicle assignment, driver number, geo-fence locations);
- GPS geolocation.

4. Is any 'special category' or criminal offences information collected through Reveal?

Under data protection laws, special category information is personal data relating to race, ethnic origin, political opinions, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation. Along with information about criminal offences, processing of special category information is more restricted.

Neither special category nor criminal offence information is requested via the service (e.g., drivers are not asked to input any information of this nature into the app). Whilst special category information may be inferred from location information (e.g. geolocation information might identify that a driver routinely visits a particular religious or medical center) this does not trigger GDPR requirements relating to processing of special category information unless the location information is, in fact, used to deduce this type of special category data. However, depending on how and why you deploy the service, (alleged) criminal offence information could be processed from the information collected (e.g. vehicle activity information might indicate that a driver has exceeded a speed limit).

What constitutes a criminal offence will vary country-by-country, as will categorisation of information as 'special category' or criminal offences information. In the event that you do collect data that could be considered criminal offences information, then, in accordance with data protection law(s), you will have additional GDPR and national law obligations as the Controller of that personal data.

5. Who has access to the Reveal Personal Data?

Reveal Personal Data processed in the course of providing the service is available to relevant Verizon employees on a 'need to know' basis. The Reveal Personal Data is also made available to third party companies who provide services to Verizon, to enable Verizon to administer the service (e.g., third parties which provide hosting services). Verizon may also disclose Reveal Personal Data to third parties where required to do so by law (e.g., law enforcement bodies).

In addition to the purposes described above you may choose to disclose Reveal Personal Data for your own purposes. You will choose who within your organisation should have access to Reveal Personal Data (e.g., you will need to assign administrators who can access the online portal in order to view real-time vehicle location and activity information). You may also choose to share Reveal Personal Data with third parties, such as other organisations within your corporate group, or other platform providers (e.g. where another platform interfaces with Reveal).

6. Does Verizon transfer Reveal Personal Data outside the European Economic Area ('EEA')?

Verizon hosts Reveal Personal Data in data centers located both inside and outside the EEA. A list of these countries is available here: https://www.verizon.com/about/privacy/data-processing-activities. Where Verizon shares Reveal Personal Data outside the EEA within the Verizon group, these transfers are made in accordance with EU approved Binding Corporate Rules for Controller & Processor.

7. How long does Verizon keep Reveal Personal Data?

Reveal Personal Data will be kept as long for as agreed in the contract terms and in accordance with the retention settings that you select within the product. This will vary depending on your legal requirement to

retain the data, or any reporting requirements you may request. It is your responsibility as the Controller to ensure that you understand how long you are legally required to retain the Reveal Personal Data. On termination of the services, Verizon Connect will securely delete the Reveal Personal Data.

8. Does Verizon use Reveal Personal Data for its own purposes?
The Reveal Personal Data is collected by Verizon to provide you with the Reveal service that you have requested. Verizon is a Processor for these purposes.

To the extent, permitted by law, Verizon makes some secondary use of anonymised information collected through Reveal for its own purposes and to improve the products and services. This includes analytics to optimise the Reveal solution and disclosures to insurance companies. No individuals, or organisations using Reveal, are identifiable from the anonymised information.

9. How does Verizon ensure that the Reveal Personal Data is kept secure?
Please refer to the Verizon Internal Systems Information Security Exhibit for a description of the technical and organisational security measures that Verizon implements to comply with its obligations under the GDPR at *https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit.*

Data Protection Requirements

This section explains how data protection requirements apply to your use of Reveal.

At the end of this section we have included a checklist of Articles in the General Data Protection Regulation and where they are addressed in this eBook. This will allow you to check if a particular provision in the GDPR is relevant to Reveal and where it is addressed in this eBook. We have also included a list of sources of additional information.

A. Data Protection Impact Assessment

A data protection impact assessment ('DPIA') is a process to describe and assess personal data processing and to identify and manage the risks which the data processing poses to individuals.

Collectively, data protection supervisory authorities consider that DPIAs must be conducted when an organisation processes personal data in order to evaluate the performance, location or movement of employees[1]. It is likely that your use of the service will require you to undertake a DPIA, but each supervisory authority has published its own DPIA criteria. You should consult the criteria of your competent supervisory authority to identify whether a DPIA is required.

Your DPIA should:

- Describe what processing of Reveal Personal Data will take place;
    - The information in this e-Book about what data is collected, how it is collected and how it is processed will help with this.
- The purposes of the processing – and, if the lawful basis for your use of the service is that the processing is necessary for a purpose which is in your legitimate interests, what this interest is.
- Assess if the processing is a necessary and proportionate way of meeting these purposes;
    - This means considering if it is reasonably possible to meet the purpose in another way which involves less processing of personal data.
    - For example, if a company wishes to track the hours worked by an individual, could this be done by an alternate process rather than tracking their whereabouts throughout the whole shift, as this would clearly be disproportionate.
- Assess the risks to individuals which the processing presents and how these risks can be addressed;

[1] WP29 *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248) p.10

- For example, if an employee is allowed to use a vehicle for private use, then tracking the vehicle while the employee is not working would be intrusive and not necessary for the employer's purpose. This risk could be mitigated by allowing the employee to turn the service off outside work hours by enabling the available 'privacy switch' and ensuring that employees are aware of this option.

- Describe the security measures; and
- Describe the other measures to ensure protection of personal data and to demonstrate compliance.
    - The DPIA should address the other topics set out in this eBook.
    - In particular, the DPIA should set out how data subject rights are met.

In the course of completing your DPIA, you should consult your Data Protection Officer (if you have one). If appropriate, you should also consult individuals whose data will be processed, or their representatives – e.g., through Employee, Trade Union or Works Council Consultation – and reflect the output of this consultation in the DPIA.

If your DPIA concludes that the use of Reveal Personal Data for your planned purposes results in high and unmitigated risks to the individuals, you should consult with your competent supervisory authority (in the UK, this is the Information Commissioner's Office).

You will need to keep any DPIA under review and periodically assess your deployment of the service and use of Reveal Personal Data against it.

B. Privacy Notice

As with all personal data processing that you perform, it is your obligation to ensure that you provide individuals with clear and comprehensive information about your collection and use of their Reveal Personal Data.

This section describes the information that you are required to include in your privacy notice to comply with data protection requirements. However, you should consider whether any other relevant legal requirements will impact on the content of your privacy notice and how you implement the service. For example, in some countries, employment laws will require you to include additional information in your privacy notice or other internal documents.
The GDPR requires you to include the following information in your privacy notice:

- Your identity and contact details (and those of your data protection officer, if you've appointed one);
- The purposes and lawful bases of processing (and, where you process Reveal Personal Data for a purpose which is in your 'legitimate interests', what these interests are);
    - The sections on purposes and lawful basis in this eBook will help you consider and describe this.
- The categories of Reveal Personal Data processed (and sources), where not obtained directly from the individual;
    - Section 3 above on "What personal data is collected through the service" will help you describe this.
- Recipients of the Reveal Personal Data, and any non-EEA countries to which Reveal Personal Data is transferred (along with details of safeguards put in place);
- Retention period for the Reveal Personal Data;
- Whether provision of any Reveal Personal Data is mandatory, and the possible consequences of failure to provide such data;
- The existence of any automated individual decision-making (including profiling), along with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- A description of data subjects' rights (including the right to withdraw consent, if you process Reveal Personal Data where the individual has given consent) and the possibility to complain to a supervisory authority.

The privacy notice provided must also satisfy additional requirements under Art. 12 of the GDPR (e.g. the

information you provide to individuals is concise, transparent, intelligible and easily accessible, and in clear and plain language).

Users of the service in France
In addition to the GDPR requirements listed above, the French Data Protection Act requires you to inform individuals of their right to define guidelines regarding the use of their personal data after their death.

In-Vehicle Notice

Given that the collection of Reveal Personal Data is a less visible type of data collection to individuals, yet can have significant consequences, you should make particular efforts to bring the use of the service to the attention of drivers. In addition to the comprehensive privacy notice described above, regulatory guidance states that you must also clearly inform drivers that a tracking device has been installed in the vehicle that they are driving, and that their movements (and driving behaviour, if the relevant technology is deployed) are being tracked. Ideally, this information should be displayed prominently in every relevant vehicle, within the driver's eyesight.[2]

Users of the service in Poland
In addition to the content listed above, where deployment of the service amounts to employee monitoring, the in-vehicle notice should also set out:

- What data are collected and recorded;
- Where and how long these data are stored; and
- Who has access to the data[3].

Enforcing Policies

If Reveal Personal Data will be used to enforce your rules and standards, you must make sure that doing so is lawful, and that employees know what the relevant rules are and that you will monitor to see if they are met, via the service.

C. Record of Processing Activities

As a Data Controller, you need to maintain a Record of Processing Activities ('RPA') as set out in Art. 30 of the GDPR. You will need to ensure that the processing of Reveal Personal Data is covered in your RPA. You will need to include information about:

- Your organisation's name and contact details (and, where applicable, the name and contact details of your data protection officer, representative and/or joint Controller);
- The purpose for which you use Reveal Personal Data;
- A description of the categories of Reveal Personal Data and the categories of individuals whose data is processed;
    - Section 3 above on "What personal data is collected through the service?" will help you complete this.
- The categories of recipients to whom Reveal Personal Data will be disclosed;
    - Section 5 above on "Who has access to the Reveal Personal Data" will help you complete this. You should also list recipients to whom you give access to the Reveal Personal Data
- Transfers of Reveal Personal Data to countries outside the EEA;
    - Section 6 above on "Does Verizon transfer Reveal Personal Data outside the EEA" explains where data is transferred and what safeguards are used to protect the Reveal Personal Data
- Time limits;
    - Section 7 above on "How long does Verizon keep Reveal Personal Data" explains this.
- Information about security measures, where possible.
    - Please refer to the Verizon Internal Systems Information Security Exhibit for a description of the technical and organisational security measures that Verizon implements to comply with

[2] WP29 *Opinion 2/2017 on data processing at work* (WP249), p.20

[3] (Polish) Data Protection Office, *Data protection in the workplace. Guidelines for employers,* p. 37

its obligations under the GDPR at the following url:.
https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit

Verizon has information available to assist you with this obligation at the following link:
https://www.verizon.com/about/privacy/data-processing-activities

Users of the service in the UK
If you process criminal offence data and your lawful basis for processing is one of the conditions set out in Schedule 1 of the Data Protection Act 2018, then you will be required to incorporate additional columns into the RPA (relating to lawful basis and condition of processing, and retention/deletion of the relevant data in line with your Appropriate Policy Document, if required).

D. Purposes

You will need to identify the purpose(s) for which you want to deploy the service and use Reveal Personal Data, e.g.:

- Detecting and preventing the loss of your organisation's property;
- Improving the productivity of employees;
- Optimising routes and resources and saving fuel;
- Providing your customers with live tracking information;
- Ensuring the safety and security of your employees, such as by ensuring that rest and meal breaks are observed.

It's important that you are clear about the purposes for which the service is deployed at the outset.

- You need a "lawful basis" for each separate purpose for which you process Reveal Personal Data;
- You need to make sure that you do not process more Reveal Personal Data than is reasonably necessary for this purpose;
- You need to tell individuals what these purposes are.

Once you have collected Reveal Personal Data for these purposes, you can then only use Reveal Personal Data for these purposes, or for other purposes which are compatible with those purposes. Sometimes applicable law allows exceptions to this principle.

Users of the service in France
Geolocation devices may only be installed in vehicles used by employees for the following purposes[4]:

- Tracking, justifying and invoicing for passenger transport services;
- Ensuring the safety and security of employees, goods and vehicles (in particular, locating stolen vehicles);
- Optimising the allocation of resources where services are provided in broad geographic areas, particularly in the context of emergency services;
- Tracking working time (but only where no alternative methods of tracking working time are available);
- Complying with legal or regulatory obligations;
- Ensuring that the employer's rules regarding the use of work vehicles are respected.

Conversely, use of a geolocation device installed in employee vehicles is forbidden[5]:

- For monitoring adherence to speed limits;
- For permanently tracking employees;
- For tracking working time, where alternative methods are available;
- In the vehicle of an employee who has freedom in the organization of their role (e.g., a sales representative);

[4] CNIL Guidelines on geolocation of employees' vehicles, 2018

[5] CNIL Guidelines on geolocation of employees' vehicles, 2018

- For tracking private use of the vehicle where private use is permitted (e.g. during breaks or by employees who may freely arrange their trips); or
- For tracking trade union representatives or similar acting within the scope of their functions.

Users of the service in Germany
Tracking systems through which employees can be permanently monitored are generally not permitted.[6]

Users of the service in Poland
If and to the extent that deployment of the service constitutes employee monitoring, organisations may only process Reveal Personal Data for the legitimate purpose of "ensuring that employees make effective use of their working time and proper use of their equipment and tools". The Polish supervisory authority suggests that this legitimate purpose is quite broad and may allow for:

- Locating a vehicle in case of theft;
- Investigating an employee's liability for a damage to a vehicle; or
- Optimising routes and resources and saving fuel.

Users of the service in Portugal
The services cannot be used for monitoring employee behaviour, and can only be deployed in vehicles used by employees for the following permitted purposes[7]:

- **Fleet management where external services are being provided:**
  - Technical assistance services;
  - Distribution of goods;
  - Passenger transport;
  - Transportation of goods; and
  - Private security.

- **Protection of goods:**
  - Transportation of hazardous materials; and
  - Transportation of high value materials.

Where the services are specifically deployed in order to geolocate employee-operated vehicles in the event of theft, the employer cannot access collected geolocation data until and unless the vehicle is stolen. Other vehicle data (such as average speed, breaking, fuel consumption) may be collected but not linked to any personal data that makes the driver identifiable.

E. Lawful Bases

You will need to identify a lawful basis under Art. 6 GDPR for each purpose for which you use Reveal Personal Data. Depending on your situation, you may be using Reveal Personal Data because this is necessary to:

- **Comply with a legal obligation:** for example, where you are under a legal obligation to monitor the use/driving hours of vehicles by fitting a tachograph to a vehicle;
- **Perform a contract with the data subject**: for example, where good driving is a condition of employment;
- **Pursue a purpose which is in your legitimate interests:** for example, keeping your drivers (and other road users) safe, enforcing good driver habits, fleet monitoring, improving fuel & maintenance efficiency, defending against accidents and false accusations, ensuring health & safety of staff, and assisting with insurance premiums.

It is imperative that you ensure that you have a legitimate legal basis to process the data and are able to justify this to a Data Protection Supervisory Authority as required.

[6] Commissioner for Data Protection and Freedom-of-Information Rhineland-Palatinate, *On the lawfulness of GPS-tracking of employees*; Commissioner for Data Protection and Freedom-of-Information Baden-Wuerttemberg, *Employment data protection*, 2018, pp. 36- 37

[7] Guideline from CNPD and labor code

You will need to demonstrate that your processing of Reveal Personal Data is "necessary". "Necessary" means that the processing of Reveal Personal Data must be a targeted and proportionate way of achieving your purpose; the processing must be "more than desirable, but less than indispensable or absolutely necessary"[8]. Your assessment should be fact-based, taking into account the objective pursued and any less intrusive options for achieving the same goal. If there are realistic, less intrusive alternatives, then the processing is not "necessary".[9]

Where relying on legitimate interests, you will need to conduct and document a "balancing test" to ensure that your legitimate interests are not overridden by the interests, rights and freedoms of individuals. The processing should be necessary for the purpose (i.e. proportionate to the business need) and safeguards should be included to protect the privacy rights of individuals. If individuals' interests outweigh your interests then the processing should not go ahead.

***Consent*:** You may also process Reveal Personal Data if the data subject has given consent to this. However, consent is only valid if it is freely given. Individuals must also be free to revoke their consent – without detriment. This makes it difficult to obtain valid consent in the employment context.[10]
Many data protection supervisory authorities have commented on lawful bases in the context of telematics. For example:

- In the UK and Poland, where private use of a vehicle is allowed, monitoring movements when it is used privately, without the freely given consent of the user, will rarely be justified.[11]
- In Portugal, consent is not a valid lawful basis for processing geolocation-derived data.[12]
- Vehicle tracking devices should not be regarded as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example by sending alerts in relation to speed of vehicle.[13]
- Processing location data can be justified where this is done in the course of monitoring the transport of people or goods, improving the distribution of resources, or for the security of the employee, vehicle, or goods being transported, but is likely to be excessive where employees are free to organise their travel arrangements as they wish or where done solely to monitor an employee's work where this can be monitored by other means.[14]
  Sending excessive information to a customer about the driver delivering their items e.g. passport photograph (in addition to name and location of driver) to enable a customer to verify the identity of the delivery driver upon arrival is unlikely to have a lawful basis (there would be a 'legitimate interest' in providing the photograph for identification purposes, but this is considered disproportionate to satisfy the balancing test).[15]

Criminal offence data

If the Reveal Personal Data you process includes any criminal offence data (in light of local laws and local interpretation of 'offences') then Art. 10 GDPR restricts the processing of this personal data. Criminal offences data can only be processed when under the control of an 'official authority' or where authorized by applicable

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

[9] European Data Protection Board (EDPB), *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, adopted on 9 April 2019*, p. 7

[10] For example, consents of employees are regularly not considered to be valid in Germany (Commissioner for Data Protection and Freedom-of-Information (LDi) NRW, 24th *Report on Data protection and information freedom 2017-2018*, p. 65, 66) and consent is not a valid lawful basis for processing personal data in the employment context in Portugal (CNPD guideline on use of geo-localization tolls in the context of employment and strict interpretation of Labour Code dispositions)

[11] Information Commissioner's Office *The employment practices code*, p. 76; (Polish) Data Protection Office, *Data protection in the workplace Guidelines for employers,* p. 38

[12] CNPD guideline on use of geo-localization tolls in the context of employment and strict interpretation of Labour Code dispositions

[13] WP29 *Opinion 13/2011 on Geolocation services on smart mobile devices*

[14] WP29 *Opinion 5/2005 on the use of location data with a view to providing value-added services*

[15] WP29 *Opinion 2/2017 on data processing at work*

EU or national laws, so you will need to consult local laws to identify relevant requirements, for example:

Users of the service in France
Under the French Data Protection Act, collection of personal data relating the behaviour of a person which may or is likely to be classified as an offence or crime is forbidden. As a result, it is forbidden to collect the fact that the person has exceeded speed limits or information relating to the behaviour of a person which may reveal violations of traffic rules.

Users of the service in Germany
The current position in Germany is that normal processing of Reveal Personal Data does not constitute processing of criminal offences information. Use of the services specifically to uncover criminal offences would however be restricted by section 26(1) BDSG (for example if the vehicles movements are monitored to uncover theft, fraud or drug dealing by employees – note that speeding infringements are not criminal acts within this meaning). This would not be a "normal" use case of Reveal, and therefore it is likely that processing for this purpose will only take place very exceptionally (e.g. if an employer investigates cases in which it suspects that an employee has committed a criminal act), but if you do use the services for this purpose then section 26(1) BDSG should be consulted.

Users of the service in Italy
Generally, processing of Reveal Personal Data does not constitute processing of criminal offences information as understood in Italy (only infringements which would be punishable by administrative fine). However, you should monitor whether any changes in local law introduce any criminal offence for which Reveal Personal Data may be relevant.

Users of the service in Poland
Certain specific requirements apply to the processing criminal offence information relating to employees under the Polish Labour Code 1974, namely you cannot rely on an employee's consent for the processing of his/her criminal offence data. An alternative lawful basis is required, most likely that the information is processed in order to comply with a legal obligation, or for the establishment, exercise or defence of legal claims.

Users of the service in Portugal
The processing of criminal offences data for the prevention or detection of an unlawful act (such as, potentially, the commission of speeding/traffic offences) is permitted in certain circumstances, and where this is necessary for the purposes of or in connection with any legal proceedings, legal advice, or as necessary to establish, exercise or defend legal rights. The personal data must, however, be pseudonymized within seven days of collection.

Users of the service in Spain
Generally, processing of Reveal Personal Data does not constitute processing of criminal offences information as understood in Spain (only the infringement of traffic rules). However, you should monitor whether any changes in local laws introduce any criminal offences for which Reveal Personal Data may be relevant, as the processing of criminal offences information in Spain is restricted - the only (potentially) relevant circumstances in which processing of criminal offences information could take place in this context are where (i) the purpose is prevention, investigation, detection or prosecution of criminal offences or enforcements, (ii) the processing is covered by a rule with statutory force and effect or by EU law.

Users of the service in the UK
In the UK, you will need to ensure that, in addition to a lawful basis, a condition for processing is met under either Article 9 GDPR or Schedule 1 of the Data Protection Act 2018. For example, in respect of criminal offence data, the Data Protection 2018 permits processing of personal data for the prevention or detection of an unlawful act (such as, potentially, the commission of a speeding/traffic offence) in certain circumstances, and where this is necessary for the purposes of or in connection with any legal proceedings, legal advice, or as necessary to establish, exercise or defend legal rights.

F. Data Minimisation

You must ensure that you only use Reveal Personal Data that is adequate, relevant and limited to what is necessary (in light of your purposes). Ultimately, this means that you should identify and use the minimum amount of Reveal Personal Data that you need to fulfil your purposes.

If you allow employees to make personal use of vehicles, then there is usually no need to collect information about where the vehicle is taken outside of working hours. The service has the functionality to ensure that employees are not monitored when out of working hours. This is known as the Privacy Switch and it is a simple and cost effective way for you to ensure compliance. In some countries (such as France, Germany and Portugal) enabling employees to use the Privacy Switch is required under regulatory guidance.[16]

G. Data Accuracy

You will need to ensure that the Reveal Personal Data you use is not incorrect or factually misleading. In the context of Reveal Personal Data, it is particularly important that you take steps to ensure the accuracy of personal data (for example, ensuring that records of vehicles assigned to employees are made accurately) and carefully consider any challenges to the accuracy of the personal data (for example, a driver contesting his or her location at a particular time).

H. Retention of Reveal Personal Data

Reveal Personal Data should only be kept for as long as necessary for your specified purpose. You will need to consider whether any legal retention requirements apply (for example, to retain working time records). These will need to be addressed in your retention policy.

I. Security of Reveal Personal Data

You will need to implement "appropriate technical and organisational" measures to ensure the confidentiality, integrity and availability of Reveal Personal Data, in accordance with Art. 32 of the GDPR. A risk assessment can be used to identify particular issues presented by your deployment of Reveal and use Reveal Personal Data, to determine the 'appropriate' level of security (taking into account the state of the art and costs of implementation). Once implemented, you should regularly test your technical and organisational measures to ensure that they continue to be appropriate. Where you share Reveal Personal Data with another organisation which acts as a Data Processor on your behalf, you will need to ensure that the Data Processor provides sufficient guarantees (and agrees contractually) to also implement appropriate technical and organisational measures to protect the data.

In the event of a security breach involving personal data, you will need to comply with Art. 33 and 34 of the GDPR. We will notify you without undue delay. You may be required to then notify the competent supervisory authority within 72 hours of becoming aware of the incident (unless you consider it unlikely to be a risk to the rights and freedoms of individuals). Where the breach is likely to result in high risk to the rights and freedoms of individuals, you will also need to notify affected individuals without undue delay. You should consider how you would identify that a breach involving Reveal Personal Data had occurred, what steps you would take to mitigate the breach, and how you would escalate and evaluate a breach to determine whether notification is required.

<u>Users of the service in France</u>
According to the CNIL guidelines on geolocation of employees' vehicles[17], you should implement, in particular, the following:

- an access clearance policy;
- measures for secure data transfers; and
- a log of data access and processing operations.

[16] Bavarian Commissioner for Data Protection, 27th Activity Report 2016, p. 241; CNIL Guidelines on geolocation of employee vehicles, 2018; CNPD Deliberation 7680/2014

[17] CNIL *Guidelines on geolocation of employee vehicles,* 2018

Users of the service in Spain
When personal data is being rectified or erased, the Spanish Data Protection Act requires Controllers to 'block' the data as part of the technical and organisational measures that they implement to comply with Art. 32 – this means that the relevant personal data must be extracted and stored in a separate database, and technical and organisational measures need to be adopted to prevent processing of the data (including any access or viewing). The relevant personal data needs to be maintained in a separate and protected database in order to comply with any requests that may be received from competent public bodies (such as courts, the public prosecutor, data protection supervisory authorities etc.) or in the event that transfer of the data to such public bodies is necessary for the exercise or defence of legal claims. In order to calculate the period for which personal data needs to be kept 'blocked', the limitation periods for different legal claims that may arise as a consequence of the data processing of the relevant data need to be considered. The personal data can be fully deleted once the relevant limitation periods have elapsed.

As the Data Controller of Reveal Personal Data, you need to ensure that you can fulfil this obligation. Verizon assists you with meeting this obligation by enabling you to download copies of certain Reveal Personal Data via the Reveal self-service dashboard, and provide other Reveal Personal Data to you upon request.

J. Data Subject Rights

You will need to identify how you will satisfy your obligation to respond to requests from individuals. Under the GDPR, individuals have the following rights in respect of their personal data:

- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

You must inform individuals that these rights exist in your privacy notice.

The applicability of these rights can be limited (e.g. the right to data portability only exists where personal data are processed on the lawful basis of contractual necessity, or consent) and you may be able to apply exemptions (e.g. if releasing information would adversely affect the rights of others, which could include protection of trade secrets).

Generally, you need to respond to these requests within one month and ensure that your response meets additional requirements under Art. 12 GDPR (e.g. the information you provide to individuals is concise, transparent, intelligible and easily accessible, and in clear and plain language).

Where practical to do so, Verizon can assist you in complying with requests from individuals which relate to the service.

Users of the service in France
Under the French Data Protection Act, individuals have the right to define guidelines regarding the use of their personal data after their death. You need to ensure that you are able to respond to this type of request.

K. Sharing Reveal Personal Data

In addition to individuals requesting access to their own data, you will need to determine how you will respond to requests for access to Reveal Personal Data from third parties. This might include, for example, requests from law enforcement bodies and insurers, where a vehicle has been involved in an accident.

Any sharing of Reveal Personal Data (including, e.g., with other organisations within your corporate group or to another service provider) will need to satisfy all the data protection requirements set out in this eBook (e.g.,

sharing must be lawful, proportionate, transparent etc.). You will need to consider whether contracts or other arrangements need to be put in place with the organization (for example, where the other organization is acting as a Data Processor on your behalf, or a joint Data Controller with you). Where this sharing involves a transfer of Reveal Personal Data outside the European Economic Area ('**EEA'**), you will need to ensure that the transfer is permitted per the GDPR.

Users of the service in France
Under CNIL guidelines, you must limit access to information relating to (or resulting from) geolocation devices to (as relevant): (i) your own authorised personnel, (ii) the employer of the individual to whom geolocation information relates; and (ii) authorised personnel of a customer to which you provide relevant services. As a matter of principle, the name of the driver must not be shared, unless this information is particularly relevant and necessary.

L. Automated Decision Making

Data protection law prohibits organisations from taking decisions based solely on automated processing of personal data where the decision would have legal or similarly significant effects. You will need to identify any such uses of the service. This might be relevant where:

- A driver's salary is automatically calculated based on the time that they start/finish driving a vehicle;
- A driver is automatically issued with a warning for entering a geofenced area;
- A driver's eligibility for a bonus is automatically calculated based on the number of jobs assigned to and completed by them, as recorded by the service.

If there is meaningful human review of a decision before it is taken, these restrictions do not apply.

Organisations are allowed to take these kinds of solely automated decisions where the decision is:

- Necessary for the performance of or entering into a contract;
- Authorised by Union or Member State law to which the Controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- Based on the data subject's explicit consent.

Where automated individual decision-making takes place, you need to provide clear information to individuals about this (see 'Privacy Notice', above) and, at least, give individuals the right to obtain human intervention in the decision making process, to express their point of view and to contest the decision.

Users of the service in Portugal
Use of geolocation and vehicle telemetry data for solely automated decision-making is not permitted.[18]

M. Employee/Works Council/Trade Union Consultation

You may be required under employment law to consult with your employees, works council, or trade union about the implementation of the service, or further uses that you choose to make of Reveal Personal Data. Alternatively, you may be required to consult with trade unions or employee representatives under the terms of any voluntary agreements that are in place. Even if not required, you might consider it appropriate to consult with staff about the deployment of the service and use of Reveal Personal Data as part of the DPIA process.

If you agree with your works council on a binding agreement, then this agreement would constitute a "more specific rule" to ensure the data protection rights of employees according to Article 88(1) GDPR. This means that such an agreement can, under some circumstances, provide legal certainty regarding how Reveal can be used in your organisation. In order to meet the requirement for a "more specific rule" according to Article 88(1) GDPR, the works agreement must be binding according to your local employment laws, and must appropriately address the data protection interests of the employees (see Article 88(2) GDPR). In case of

[18] CNPD guideline on use of geo-localization tolls in the context of employment and strict interpretation of Labour Code dispositions

doubt, you should seek legal advice.

Users of the service in France
According to Art. L2312-38 of the French Labour Code, you must inform and consult with Works Councils (*Conseil Economique et Social*) before implementing any systems or means which enable monitoring employees' activity, such as geolocation tracking.

Users of the service in Germany
Under Section 87(6) Works Constitution Act (Betriebsverfassungsgesetz -BetriebsVG), the works council, if one exists within your organisation, has a right to co-determie the introduction and use of technical equipment designed to monitor employees' behaviour or performance. Permanent 'control' of employees' behaviour and performance through monitoring is not permissible – if you are the employer, you are required to exclude such permanent employee 'control' by means of works council agreements or unilaterally binding regulations.[19]

Section 26(4) of the Federal Data Protection Act states explicitly that data processing can be permitted on the basis of works agreements, if these works agreements comply with the requirements of Article 88(2) GDPR.
Users of the service in Italy
You may need to consult your organisation's trade union(s), if any, or obtain authorisation from the competent Labour Office about the implementation of the service and your use of the Reveal Personal Data to comply with Art. 4 (2) of the Law no. 300/1970 (Italian Worker Statute), unless the Reveal Personal Data which you process is limited to the data that is strictly necessary to you to comply with legal obligations.

Users of the service in Poland
You should set out the purpose, scope and methods of monitoring in your Work Regulation (a mandatory internal policy for employers with 50+ employees in Poland) or the Corporate Collective Labour Agreement. If there are trade unions at your organisation, changes to the Work Regulation or Corporate Collective Labour Agreement will require cooperation with trade unions.

As far as existing employees are concerned, you should inform them that you intend to launch a monitoring system. This should be done no later than two weeks before the monitoring system is launched.

Users of the service in Portugal
Under Art. 21 of the Portuguese Labour Code, you must inform and consult with Works Councils (Comissão de Trabalhadores) before implementing any systems or means which enable monitoring of employees' activity, such as geolocation tracking.

Users of the service in Spain
Under Art. 64(1) of the Spanish Workers Statute, you will need to inform the workers' representatives prior to the implementation of any measure that may affect the workers, which is understood to include the implementation of geolocation devices or any other monitoring solution.

In support of the above, Art. 90(2) of the Organic Law 3/2018, of 5 December, on the Protection of Personal Data and granting the digital rights states that prior to the implementation of geolocation devices employees' and workers' representatives need to be informed about the existence and features of these devices.

N. Risk Mitigation and Data Protection by Design and Default

You must ensure that any steps needed to mitigate risks to individuals (as identified during the DPIA process) and to comply with 'data protection by design and by default' requirements have been taken. Data protection by design means that privacy issues should be considered and addressed at the outset of a data processing activity (i.e. the design phase), and during the lifecycle of that processing activity. Data protection by default requires you to ensure that the minimum data necessary to achieve your purpose(s) is processed (for example,

[19] Commissioner for Data Protection and Freedom-of-Information Baden-Wuerttemberg, *Employment data protection*, 2018 ; Independent Centre for Data Protection Schleswig-Holstein, Activity Report 2017-2018, 103

rather than permitting broad access to Reveal Personal Data, access should be restricted to particular individuals on a 'need-to-know' basis).

Guidance from data protection supervisory authorities sets out examples of risk mitigation in the context of telematics and employee monitoring:

- Drivers should be permitted to temporarily disable location tracking in certain circumstances (e.g. when visiting a medical clinic), where employees are permitted to make personal use of the organisation's vehicles.[20]
- Where a need to monitor a vehicle's location outside of an employee's working hours exists (e.g. to prevent vehicle theft), implementation should be proportionate to the risks e.g. the location of the vehicle is not registered (or visible to you) outside working hours, unless it leaves a widely defined circle (e.g. region).[21]
- The number of personnel with access to Reveal Personal Data should be minimised. Personnel must be appropriately trained and subject to confidentiality and security obligations.[22]
  Consider which personnel are most appropriate to access Reveal Personal Data (this might not, for example, be line managers).[23]

O. Designation of a Data Protection Officer (DPO)

Several triggers for appointing a data protection officer ('DPO') are set out at Art. 37 GDPR. Your existing processing activities might not already require you to appoint a DPO. However, your use of the services may trigger the need for you to have a DPO in light of Art 37(1)(b), which requires appointment of a DPO where an organisation's core activities consist of regular and systematic monitoring of data subjects on a large scale. Use of the services for monitoring drivers and their driving behaviour is likely to fall within the scope of Art. 37(1)(b), in which case you will be required to appoint a DPO. Further GDPR provisions (Art. 38 and 39) set out requirements relating to the DPO's position and tasks - you will also need to comply with these if a DPO appointment is required.

Users of the service in Germany
Under Section 38 of the Federal Data Protection Act (BDSG) you are required to designate a DPO if you permanently employ at least 20 persons for the automated processing of personal data or if the personal data processing you perform requires you to conduct a DPIA. You are likely to need to appoint a DPO if you use the services in Germany.

Further Information

Legislation

- General Data Protection Regulation (EU) 2016/679 ('GDPR')
- Data Protection Act 2018 (UK)
- Law 58/2019, 8 August of 2019 (Portugal)[24]
- Labour Code (Portugal)
- Constitutional Act 3/2018, 5 December of 2018, on Protection of Personal Data and Guarantee of Digital Rights (Spain)
- Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) 2018 (Germany)
- Works Constitution Act (Betriebsverfassungsgesetz -BetriebsVG) (Germany)
- Legislative Decree no 196/2003 (Italian Data Protection Code) (Italy)
- Law no. 300/1970 (Italian Workers' Statute) (Italy)
- Legislative Decree 101/2018 (Italy)
- French Data Protection Act n°78-17(France)

[20] Article 29 Working Party *Opinion 2/2017 on data processing at work* (WP249), p.20

[21] Article 29 Working Party *Opinion 2/2017 on data processing at work* (WP249), p.20

[22] Information Commissioner's Office *Employment practices code*, p. 67

[23] Information Commissioner's Office *Employment practices code*, p. 67

- French Labour Code (France)

Case Law

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

Regulatory Guidance

EU

- Article 29 Working Party *Opinion 5/2005 on the use of location data with a view to providing value-added services* (WP115)
- Article 29 Working Party *Opinion 13/2011 on Geolocation services on smart mobile devices* (WP 185)
- Article 29 Working Party *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248)
- Article 29 Working Party *Opinion 2/2017 on data processing at work* (WP249)
- Article 29 Working Party *Opinion 2016/679 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation* (WP251)
- European Data Protection Board *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (version for public consultation)*

France

- CNIL Guidelines on geolocation of employees' vehicles, 2018

Germany

- Commissioner for Data Protection and Freedom-of-Information Rhineland-Palatinate, *On the lawfulness of GPS-tracking of employees*
- Commissioner for Data Protection and Freedom-of-Information Baden-Wuerttemberg, *Employment data protection* 2018
- Data Protection Conference of the independent Federal and State (Länder) data protection authorities (Datenschutzkonferenz - DSK), Short paper No. 14: *Employment data protection* (17 December 2018)
- Bavarian Commissioner for Data Protection, *27th Activity Report 2016*
- Data Protection Conference of the independent Federal and State (Länder) data protection authorities (Datenschutzkonferenz - DSK), Short paper No. 17: *Special categories of personal data* (27 March 2018)
- Data Protection Conference of the independent Federal and State (Länder) data protection authorities (Datenschutzkonferenz - DSK), Short paper No. 19: *Information and commitment of employees to comply with the data protection requirements under the GDPR* (29 May 2018)
- Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia (LDi NRW), 24th Report on Data protection and information freedom 2017-2018, *Satellite-based positioning for determining the position of company vehicles - no permissible means of monitoring employees*
- Berlin Data Protection and Privacy Commissioner freedom of information, *Annual report 2018*
- Independent Centre for Data Protection Schleswig-Holstein, Activity Report 2017-2018
- The Commissioner for Data Protection Lower Saxony, 24th Activity Report 2017-2018, *GPS monitoring of company vehicles*

Poland

- Data Protection Office, *Data protection in the workplace. Guidelines for employers*

Portugal

- CNPD Deliberation 7680/2014 (Guideline on use of geo-localisation in the context of employment).

UK

- Information Commissioner's Office *Employment Practices Code* and *Supplementary Guidance*

GDPR Checklist

GDPR Article	Topic	Relevance to Reveal	eBook Reference
Art. 1, 2 or 3	Subject matter and objectives; material; and territorial scope	No specific relevance	N/A
Art. 4	Definitions	Defines concepts of 'personal data' and 'special category' personal data	"*Reveal FAQs*", sections 3 and 4
Art. 5	Principles and accountability	Processing of Reveal Personal Data must comply with data protection principles, and the Controller must be able to demonstrate compliance	"*Addressing Data Protection Requirements*", generally
Art. 6 and 7	Lawfulness of processing and conditions for consent	A lawful basis must exist for each purpose of processing Reveal Personal Data	"*Addressing Data Protection Requirements*", section E
Art. 8	Conditions for Child's Consent in ISS	No specific relevance	N/A
Art. 9 and 10	Processing special categories of personal data and criminal offences information	A condition must exist for each purpose of processing Reveal Personal Data, where the personal data is special category data or criminal offences information	"*Reveal FAQs*", section 4, and "*Addressing Data Protection Requirements*", section E
Art. 11	Processing which does not require identification	No specific relevance	N/A
Art. 12	Transparent information, communication and modalities for the exercise of the rights of the data subject	Any information provided to individuals about whom Reveal Personal Data is processed must be concise, transparent, intelligible and easily accessible, using clear and plain language.	"*Addressing Data Protection Requirements*", sections B and J
Art. 13 and 14	Information to be provided to the data subject	Data protection notice must be provided to individuals about whom Reveal Personal Data is processed	*"Addressing Data Protection Requirements*", section B
Art. 15	Right of access	Access to Reveal Personal Data must be provided to individuals upon request (subject to exemptions)	*"Addressing Data Protection Requirements*", section J
Art. 16	Right to rectification	Reveal Personal Data must be rectified upon request by individuals	*"Addressing Data Protection Requirements*", section J
Art. 17	Right to erasure	Reveal Personal Data must be erased upon request by individuals, if	*"Addressing Data Protection Requirements*", section J

		the right applies	
Art. 18	Right to restriction	Reveal Personal Data must be restricted upon request by individuals, if the right applies	*"Addressing Data Protection Requirements*", section J
Art. 19	Notification obligation regarding rectification, erasure or restriction	Where a request for rectification, erasure or restriction is received relating to Reveal Personal Data, third parties to which data has been disclosed must be notified of the request	*"Addressing Data Protection Requirements*", section J
Art. 20	Right to data portability	Reveal Personal Data must be ported to individuals (or nominated third parties) upon request by individuals, if the right applies	*"Addressing Data Protection Requirements*", section J
Art. 21	Right to object	Reveal Personal Data must no longer be processed upon request by individuals, if the right applies	*"Addressing Data Protection Requirements*", section J
Art. 22	Automated individual decision-making, including profiling	Solely automated decisions about individuals which create legal or similarly significant effects for individuals can only be taken in accordance with Art. 22	*"Addressing Data Protection Requirements*", section L
Art. 23	Restrictions	No specific relevance	N/A
Art. 24	Responsibility of the Controller	Appropriate technical and organizational measures should be implemented to ensure (and demonstrate) that processing is performed in compliance with the GDPR	"*Addressing Data Protection Requirements*", generally
Art. 25	Data protection by design and default	Data protection issues should be addressed at the outset and during the lifecycle of processing Reveal Personal Data, and the minimum personal data necessary to achieve your purpose should be processed.	*"Addressing Data Protection Requirements*", sections F and N
Art. 26	Joint Controllers	No specific relevance	N/A
Art. 27	Representatives of Controllers or Processors not	No specific relevance	N/A

	established in the Union		
Art. 28	Processor	Only Processors providing sufficient guarantees must be engaged to process Reveal Personal Data and obligations must be imposed on these Processors under contract	*"Addressing Data Protection Requirements*", section I
Art. 29	Processing under the authority of the Controller or Processor	No specific relevance	N/A
Art. 30	Records of processing activities	Processing of Reveal Personal Data must be reflected in the record of processing activities	*"Addressing Data Protection Requirements*", section C
Art. 31	Cooperation with the supervisory authority	No specific relevance	N/A
Art. 32	Security of processing	Appropriate technical and organisational measures must be implemented to protect the security of Reveal Personal Data	*"Addressing Data Protection Requirements*", section I
Art. 33 and 34	Data breach notification (to supervisory authority and individuals)	In the event of a personal data breach involving Reveal Personal Data, notification must be made to supervisory authorities and affected individuals if thresholds are met	*"Addressing Data Protection Requirements*", section I
Art. 35 and 36	Data protection impact assessment and prior consultation	A data protection impact assessment must be run for processing of Reveal Personal Data and consultation with supervisory authorities may be required if the processing presents high and unmitigated risks to individuals	*"Addressing Data Protection Requirements*", section A
Art. 37, 38 and 39	Data protection officer	relevance data protection officer must be appointed if the core activities of the Controller amount to 'regular and systematic' monitoring of data subjects on a large scale or processing of special category/criminal offence data on a large scale.	"*Addressing Data Protection Requirements",* section Q

Art. 40, 41, 42 and 43	Codes of conduct, certification and accreditation	No specific relevance	N/A
Art. 44 - 50	Transfers	Any transfers of Reveal Personal Data outside the EEA to countries which are not 'adequate' (e.g. to other platform providers or group companies) must only be performed where a transfer mechanism is in place or a derogation exists	"*Reveal FAQs*", section 6, and *"Addressing Data Protection Requirements*", section K
Art. 51 - 59	Supervisory authority and competence, tasks, powers and reports	No specific relevance	N/A
Art. 60 - 67	Cooperation and consistency	No specific relevance	N/A
Art. 68 - 76	European Data Protection Board	No specific relevance	N/A
Art. 77	Right to lodge complaint with supervisory authority	No specific relevance	N/A
Art. 78	Right to judicial remedy against a supervisory authority	No specific relevance	N/A
Art. 79 - 82	Right to effective judicial remedy against a Controller or Processor, and compensation	No specific relevance	N/A
Art. 83 - 84	Administrative fines and penalties	No specific relevance	N/A
Art. 85 - 91	Provisions relating to specific processing situations	No specific relevance	N/A
Art. 92 - 93	Delegated acts and implementing acts	No specific relevance	N/A
Art. 94 - 99	Final provisions	No specific relevance	N/A