Einführung

Verizon Connect bietet mobile Lösungen zum Management Ihrer mobil eingesetzten Mitarbeiter im Bereich Flottenmanagement und Außendienst. Unsere Produkte messen die Leistungen Ihrer Fahrzeugflotte und können hierdurch einen großen Einfluss auf Ihr Geschäft haben. Dies betrifft den Einsatzort Ihrer Fahrzeuge, wie Ihre Fahrer sich im Straßenverkehr verhalten und wie viel Treibstoff sie dabei verbrauchen. Diese Informationen werden Ihnen in übersichtlichen Benutzeroberflächen angezeigt, sodass Sie ggf. schnell reagieren können. Reveal kann Ihnen dabei helfen, mehr Aufgaben in weniger Zeit zu erledigen, besseren Kundendienst zu bieten und letztlich Ihr Unternehmensergebnis zu verbessern. Durch unsere Außendienstprodukte bieten wir Ihnen außerdem die Möglichkeit, den vollen Lebenszyklus einer Kundenanfrage zu steuern, beginnend beim ersten Kundenkontakt über die Erstellung eines Kostenvoranschlags, über die Zeitplanung, die Auftragserteilung und –zuweisung bis hin zur optimalen Routenführung des Fahrers und Abwicklung der Bezahlung.

Dieses eBook beantwortet Ihnen häufig gestellte Fragen (FAQs) über die ortbezogenen Flottenmanagementservices („der Dienst“ oder „die Dienste“), die Verizon Connect („VzC“) Ihnen auf der Reveal Plattform anbietet. Es gibt Ihnen einen Überblick über die wichtigsten Datenschutzbestimmungen und Anforderungen, die Sie vor, während und nach Ihrem Einsatz des Dienstes beachten müssen. Bitte beachten Sie außerdem, dass dieses eBook sich vor allem auf datenschutzrechtliche Anforderungen bezieht. Sie sollten prüfen, ob für Ihre Nutzung des Dienstes zusätzlich auch andere rechtliche Anforderungen gelten. Beispielsweise gelten in einigen Ländern arbeitsrechtliche Anforderungen in Bezug auf die Nutzung der Fahrzeuge durch angestellte Mitarbeiter.

In einigen Fällen sind in dem Text Verweise auf Handreichungen durch zuständige Behörden aufgenommen worden. Diese Behörden überarbeiten ihre Handlungsempfehlungen regelmäßig. Sie sollten deshalb selbstständig darauf achten, ob sich neue Entwicklungen ergeben. Dies ist letztlich Ihre Verantwortung, da Sie der Verantwortliche für die Erhebung und Verarbeitung personenbezogener Daten durch den Dienst sind und deshalb dafür sorgen müssen, dass dabei die einschlägigen Gesetze eingehalten werden.

Die Informationen aus diesem eBook stellen keine Rechtsberatung dar. Falls Sie konkrete rechtliche Probleme oder Anfragen haben, sollten Sie sich immer an einen ausreichend qualifizierten Rechtsanwalt wenden. VzC übernimmt keine Verantwortung oder Haftung für die Informationen aus diesem eBook.

Connect FAQs

1. Welche Informationen werden im Rahmen des Dienstes gesammelt?
In erster Linie werden Informationen über die Personen gesammelt, die die Fahrzeuge steuern, in denen der Dienst eingesetzt wird. Eventuell werden auch über weitere Personen Daten erhoben, z. B. Mitfahrer oder Haushaltsmitglieder des von Ihnen eingesetzten Fahrers, je nachdem wie Sie den Dienst einsetzen.

2. Auf welchen Wegen werden Informationen für den Dienst gesammelt?
Der Dienst sammelt Informationen aus zwei Quellen:

- Das Gerät, das an Board der Fahrzeuge installiert wird: Dieses Gerät sammelt Informationen darüber, wo Ihr Fahrzeug sich befindet und welche Aktivitäten es jeweils ausführt. Falls Sie zuordnen können, welchem Fahrer das Fahrzeug jeweils zugewiesen ist, handelt es sich hierbei um personenbezogene Daten.
- Wir bieten außerdem mehrere mobile Apps an, die Sie verwenden können, um unseren Dienst effektiv im Zusammenhang mit Außendienstmitarbeitern (Work, Workforce, Field) und Flottenmanagement (Manager/Spotlight, Video, ELD) zu

verwenden. Um diese Apps zu verwenden, muss ein Fahrer sich registrieren und dabei bestimmte Informationen angeben.

In diesem eBook bezeichnen wir personenbezogene Daten, die durch den Dienst erhoben werden, gemeinsam als „personenbezogene Reveal-Daten".

3. Welche personenbezogenen Daten werden über den Dienst erhoben?
Sie entscheiden hauptsächlich selbst darüber, welche personenbezogenen Daten durch den Dienst erhoben werden. Welche Daten Sie erheben, hängt davon ab, auf welche Weise Sie die Lösung einsetzen, Sie kontrollieren dies selbst. Es ist deshalb Ihre eigene rechtliche Verantwortung, sicherzustellen, dass Sie ein legitimes Interesse an der Nutzung der Daten im Rahmen des Dienstes haben.

Personenbezogene Daten, die durch das in den Fahrzeugen eingebaute Telematikgerät gesammelt werden, können sein:

- Standortdaten (GPS) von Fahrzeugen und Personen;
- Informationen des Fahrtenschreibers (Lenkzeiten);
- Daten zu Geschwindigkeit des Fahrzeugs und zum Fahrverhalten des jeweiligen Fahrers;
- Daten zu bestimmten Ereignissen im Zusammenhang mit dem Fahrzeug, beispielsweise falls das Fahrzeug in einen Unfall verwickelt ist oder einen bestimmten geografischen Bereich betritt oder verlässt;
- Weitere Informationen zum Zustand es Fahrzeugs (beispielsweise Treibstoffverbrauch, Reifendruck, Betriebsdaten).

Zu den personenbezogenen Daten, die über die App erfasst werden können, gehören:

- Name des Fahrers;
- Telefonnummer des Fahrers, E-Mail-Adresse und Anschrift;
- Anmeldedaten des Fahrers;
- Weitere Informationen in Bezug auf den Fahrer (beispielsweise Informationen zum zugewiesenen Fahrzeug, die Fahrernummer und die dem Fahrer zugewiesenen geografischen Gebiete, sog. Geofences);
- GPS-Standortdaten.

4. Werden durch Reveal personenbezogene Daten gesammelt, die zu den „besonderen Kategorien personenbezogener Daten" gehören oder sich auf Straftaten beziehen?
Nach dem geltenden Datenschutzrecht gehören zu den „besonderen Kategorien personenbezogener Daten" Daten in Bezug auf die Rasse, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische, biometrische oder Gesundheitsdaten, sowie Daten zum Sexualleben oder der sexuellen Orientierung eines Menschen. Die Möglichkeiten zur Verarbeitung dieser besonders geschützten Daten sind rechtlich eingeschränkt. Ähnlich gilt dies auch für Daten, die sich auf Straftaten beziehen.

Der Dienst erfordert weder Daten aus diesen besonders geschützten Kategorien, noch Daten zu Straftaten (z. B. werden die Fahrer nicht aufgefordert solche Informationen in die App einzugeben). Zwar können sich aus den Ortsangaben u.U. Daten ableiten lassen, die in diese speziellen Kategorien fallen (z. B. könnte sich aus den Ortsdaten ergeben, dass ein Fahrer häufig eine bestimmte medizinische oder religiöse Einrichtung anfährt). Dies löst die Rechtspflichten der DSGVO in Bezug auf solche sensitiven Daten jedoch nur dann aus, wenn Sie aus den Ortsdaten tatsächlich Daten ableiten, die sich auf die oben genannten speziellen Kategorien beziehen. Bitte beachten Sie aber, dass je nachdem wie und mit welchen Zielen Sie den Dienst einsetzen, aus den Daten sich auch Informationen über (eventuelle) Straftaten ergeben können, beispielsweise wenn Informationen über das Fahrverhalten darauf

hinweisen, dass ein Fahrer eine Geschwindigkeitsbegrenzung überschritten hat.

Was eine „Straftat" darstellt, hängt von dem in Ihrem Land anwendbaren Recht ab. Gleiches gilt für die Einordung von Daten als „besonders geschützte Kategorie" oder „Daten, die sich auf Straftaten beziehen". Für den Fall, dass die personenbezogenen Daten als „Daten über Straftaten" gelten, ergeben sich aus der DSGVO sowie den übrigen anwendbaren Datenschutzrecht für Sie als Verantwortlicher weitere Rechtspflichten.

5. Wer hat Zugriff auf die personenbezogenen Reveal-Daten?
Soweit personenbezogene Daten verarbeitet werden, um den Dienst zu erbringen, können die jeweils zuständigen Mitarbeiter von Verizon darauf zugreifen, soweit dies zur Erfüllung des Dienstes notwendig ist („Need-to-know-Prinzip"). Die Reveal-Daten werden außerdem auch weiteren Unternehmen zur Verfügung gestellt, die als Subunternehmer Dienstleistungen für Verizon erbringen, damit Verizon den Dienst betreuen und anbieten kann (beispielsweise Anbieter, die Hosting-Dienste anbieten). Wenn dies gesetzlich vorgeschrieben ist, kann Verizon personenbezogene Daten auch an Dritte weitergeben (z. B. Strafverfolgungsbehörden).

Zusätzlich zu den oben beschriebenen Fällen können Sie selbst darüber entscheiden, wie und an wen Sie personenbezogene Daten aus Reveal für Ihre eigenen Zwecke weitergeben. Sie bestimmen selbst darüber, wer innerhalb Ihrer Organisation auf Reveal-Daten zugreifen kann (beispielsweise legen Sie fest, welche Administratoren auf das Online-Portal zugreifen können und dort Fahrzeugdaten und sonstige Aktivitätsdaten in Echtzeit einsehen können). Falls Sie dies wollen, können Sie Reveal-Daten auch an Dritte weitergeben, beispielsweise an andere Gesellschaften aus Ihrer Unternehmensgruppe oder an weitere Dienstleistungsplattformen (beispielsweise wenn ein solcher Dienst eine Schnittstelle zu Reveal hat).

6. Verschickt Verizon personenbezogene Reveal-Daten an Orte außerhalb des Europäischen Wirtschaftsraums (EWR)?
Verizon speichert personenbezogene Reveal-Daten in Rechenzentren sowohl innerhalb als auch außerhalb des EWR. Eine Liste dieser Länder ist hier abrufbar: https://www.verizon.com/about/privacy/data-processing-activities.

Soweit Verizon personenbezogene Reveal-Daten innerhalb der Verizon-Gruppe an Orte außerhalb des EWR überträgt, erfolgt dies auf Basis von EU-rechtsgenehmigten Verbindlichen Unternehmensregeln („Binding Corporate Rules") für Verantwortliche und Auftragsverarbeiter.

7. Wie lange speichert Verizon personenbezogene Reveal-Daten?
Personenbezogene Reveal-Daten werden so lange gespeichert, wie dies in den Vertragsbedingungen vereinbart ist und den Einstellungen zur Aufbewahrungsdauer entspricht, die Sie innerhalb des Produktes vornehmen können. Dies kann unter anderem davon abhängen, ob und ggf. welchen rechtlichen Verpflichtungen Sie unterliegen, die Daten aufzubewahren, und welche Reporting-Funktionen Sie nutzen möchten. Als Verantwortlicher für die Datenverarbeitung ist es Ihre Aufgabe zu prüfen, für welche Zeiträume Sie verpflichtet und berechtigt sind, die personenbezogenen Reveal-Daten aufzubewahren. Im Fall einer Kündigung des Dienstes wird VzC alle personenbezogenen Reveal-Daten löschen.

8. Nutzt Verizon personenbezogene Reveal-Daten für eigene Zwecke?
Verizon erhebt die personenbezogenen Reveal-Daten, um Ihnen den Dienst „Reveal" anbieten zu können, so wie Sie ihn beauftragt haben. Zu diesem Zweck agiert Verizon als Auftragsverarbeiter.

Soweit rechtlich zulässig, unternimmt Verizon einige Zweitverwertungen von anonymisierten Daten, die über Reveal erhoben wurden, für eigene Zwecke und um die Produkte und Dienste zu verbessern. Dies betrifft Analysen, um die Nutzung der Reveal-Lösung zu verbessern sowie Übermittlungen an Versicherungsgesellschaften. Über diese anonymisierten Daten sind weder

Einzelpersonen noch Unternehmen oder Organisationen, die Reveal nutzen, identifizierbar.

9. Wie stellt Verizon sicher, dass personenbezogene Reveal-Daten sicher aufbewahrt werden?

Die technisch und organisatorischen Maßnahmen, die Verizon umgesetzt hat, um sicherzustellen, dass es die eigenen Verpflichtungen nach der DSGVO erfüllt, sind im *Verizon Internal Systems Information Security Exhibit* zusammengefasst.

Sie finden diesen hier: *https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit.*

Datenschutzrechtliche Anforderungen

Dieser Abschnitt beschreibt, welche datenschutzrechtlichen Anforderungen für Ihre Nutzung von Reveal gelten.

Am Ende dieses Abschnitts befindet sich eine Checkliste von Artikeln der Datenschutzgrundverordnung und der dort jeweils zugehörigen Beschreibung in diesem eBook. Auf Basis dieser Liste können Sie prüfen, ob eine bestimmte Vorschrift der DSGVO relevant für Ihre Nutzung von Reveal ist und an welcher Stelle in diesem eBook sie besprochen wird. Wir haben außerdem eine Liste mit weiteren Informationsquellen beigefügt.

A. Datenschutzfolgeabschätzung

Eine Datenschutzfolgeabschätzung („DSFA“) ist ein Verfahren, das dazu dient, die Risiken, die von einer Datenverarbeitungsaktivität für Betroffene entstehen können, zu beschreiben und zu kontrollieren.

Die zuständigen Datenschutzbehörden sind der gemeinsamen Auffassung, dass DSFAs dann durchzuführen sind, wenn eine Organisation personenbezogene Daten verarbeitet, um die Leistung, den Ort oder die Bewegungen von angestellten Mitarbeitern nachzuvollziehen[1]. Es ist wahrscheinlich, dass Ihre Nutzung des Dienstes dazu führt, dass Sie verpflichtet sind, eine Datenschutzfolgeabschätzung durchzuführen, allerdings hat jede Datenschutzbehörde ihre eigenen Kriterien zur Durchführung einer DSFA veröffentlicht. Um zu prüfen, ob Sie nach den Kriterien der für Sie zuständigen Datenschutzaufsichtsbehörde eine DSFA durchführen müssen, sollten Sie die von der für Sie zuständigen Behörde veröffentlichten Kriterien prüfen.

Ihre DSFA sollte:

- Ihre Datenverarbeitungsaktivitäten im Kontext von Reveal beschreiben;
    - Die Informationen aus diesem eBook dazu, welche Daten gesammelt werden und wie diese weiterverarbeitet werden, unterstützen Sie hierbei.
- Die Zwecke der Verarbeitung beschreiben sowie, falls Sie für die Datenverarbeitung die Rechtsgrundlage der Interessenabwägung nutzen, den von Ihnen verfolgten legitimen Zweck.
- Die DSFA sollte prüfen, ob die Datenverarbeitung für die Erreichung dieser Zwecke notwendig und angemessen ist.
    - Dies bedeutet, dass Sie prüfen sollten, ob Sie diesen Zweck auch auf eine andere angemessene Art und Weise erreichen können, bei der Sie weniger personenbezogene Daten verarbeiten.
    - Falls beispielsweise ein Unternehmen Daten zu den Arbeitszeiten von Mitarbeitern erheben möchte, wäre es eindeutig nicht angemessen, zu diesem Zweck die Aufenthaltsorte der Mitarbeiter während ihrer gesamten

[1] Datenschutzgruppe nach Artikel 29, *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 "wahrscheinlich ein hohes Risiko mit sich bringt"* (WP248) S.10, 1.

Arbeitszeit nachzuvollziehen.

- Die DSFA sollte prüfen, welche Risiken für die Betroffenen entstehen und wie diesen Risiken begegnet werden kann.
    - Falls beispielsweise Mitarbeiter Fahrzeuge auch für private Zwecke nutzen dürfen, wäre es unangemessen, Fahrzeugdaten auch während Zeiten zu erheben, zu denen die jeweiligen Mitarbeiter nicht arbeiten. Dies wäre für die Zwecke eines Arbeitgebers auch nicht notwendig. Diesem Risiko kann begegnet werden, indem den Mitarbeitern ermöglicht wird, den Dienst über den ihnen zur Verfügung stehenden „Privacy Switch“ („Privatschalter“) abzuschalten, wenn sie nicht arbeiten. Sie sollten sicherstellen, dass die Angestellten diese Option kennen.
- Die DSFA sollte die anwendbaren Sicherheitsmaßnahmen beschreiben; und
- Die DSFA sollte weitere Maßnahmen beschreiben, die dazu dienen den Datenschutz sicherzustellen und die Einhaltung datenschutzrechtlicher Vorschriften nachweisen zu können.
    - Die DSFA sollte dabei auch auf die übrigen Aspekte eingehen, die in diesem eBook beschrieben sind.
    - Insbesondere sollte die DSFA auch darauf eingehen, wie die datenschutzrechtlichen Betroffenenrechte umgesetzt sind.

Falls es in Ihrem Betrieb einen betrieblichen Datenschutzbeauftragten gibt, müssen Sie diesen einbeziehen. Dort, wo dies angemessen ist, sollten Sie außerdem Betroffene oder deren Vertreter beteiligen, beispielsweise Vertreter des Betriebsrats oder von Gewerkschaften. Das Ergebnis von deren Beteiligung sollte in der DSFA dokumentiert sein.

Sollte die DSFA zu dem Ergebnis führen, dass Ihre Nutzung von personenbezogenen Reveal-Daten für die von Ihnen geplanten Zwecke zu einem hohen Risiko für Betroffene führt, das durch weitere Maßnahmen nicht abgemildert werden kann, sollten Sie sich an die für Sie zuständige Datenschutzaufsichtsbehörde wenden.

Sie müssen die DSFA immer aktuell halten und zu diesem Zweck regelmäßig prüfen, ob sich Ihre Datenverarbeitung in Bezug auf personenbezogene Reveal-Daten verändert hat.

B. Datenschutzinformationen

Wie immer, wenn Sie personenbezogene Daten verarbeiten, ist es auch in Bezug auf die personenbezogenen Reveal-Daten Ihre Pflicht, sicherzustellen, dass alle Betroffenen in klarer und verständlicher Form über die Datenverarbeitung informiert werden.

Dieser Abschnitt beschreibt, worüber Sie die Betroffenen in Ihrer Datenschutzerklärung informieren müssen, um datenschutzrechtlichen Pflichten Rechnung zu tragen. Sie sollten darüber hinaus allerdings auch prüfen, ob weitere rechtliche Verpflichtungen für die Inhalte Ihrer Datenschutzerklärung gelten. Beispielsweise gelten in einigen Ländern zusätzliche Anforderungen in Bezug auf die Transparenz von Datenverarbeitungen, die sich aus dem jeweils geltenden Arbeitsrecht ergeben.

Nach der DSGVO sind Sie verpflichtet, die folgenden Informationen in Ihre Datenschutzerklärung aufzunehmen:

- Namen und Kontaktmöglichkeiten über Sie, als die Organisation, die personenbezogene Reveal-Daten verarbeitet (sowie Kontaktdaten Ihres Datenschutzbeauftragten, falls in Ihrem Betrieb ein solcher benannt ist);
- Die Zwecke und Rechtsgrundlagen Ihrer Datenverarbeitung (sowie, falls Sie personenbezogene Reveal-Daten für einen Zweck verarbeiten, der Ihrem „legitimen Interesse“ entspricht, welches Interesse dies ist);
    - Die Abschnitte zu Zwecken und Rechtsgrundlagen in diesem eBook unterstützen Sie dabei, dies zu prüfen und zu beschreiben.

- Soweit personenbezogene Daten nicht unmittelbar beim Betroffenen erhoben wurden, eine Beschreibung der Kategorien dieser personenbezogenen Daten und der Datenquellen;
    - Abschnitt 3 oben zu der Frage „Welche personenbezogenen Daten werden über den Dienst erhoben?“ unterstützt Sie hierbei.
- Empfänger der personenbezogenen Reveal-Daten sowie eventuelle Länder außerhalb des EWR, zu denen personenbezogene Reveal-Daten übertragen werden (sowie Informationen zu den geeigneten Garantien, die verwendet wurden, um den Schutz der Daten im Drittland sicherzustellen);
- Die Aufbewahrungsfristen für die personenbezogenen Reveal-Daten;
- Falls es für die Betroffenen zwingend vorgeschrieben ist, dass diese die personenbezogenen Reveal-Daten zur Verfügung stellen, eine Beschreibung der Konsequenzen, die drohen, falls Sie diese Daten nicht zur Verfügung stellen;
- Falls in Ihrem Betrieb „automatisierte Entscheidungsfindung im Einzelfall (einschließlich Profiling)“ stattfindet, aussagekräftige Informationen über die involvierte Logik sowie Tragweite und angestrebten Auswirkungen dieser Datenverarbeitung auf den Betroffenen;
- Eine Beschreibung der Betroffenenrechte (einschließlich einer Beschreibung des Rechtes darauf, eine etwaige Einwilligung zurückziehen zu können, falls Sie personenbezogene Reveal-Daten auf Basis der Einwilligung der Betroffenen verarbeiten), sowie ein Hinweis, darauf, dass Betroffene sich bei der zuständigen Aufsichtsbehörde beschweren können.

Die Datenschutzerklärung muss außerdem den weiteren Anforderungen gem. Artikel 12 der DSGVO entsprechen (beispielsweise muss die Erklärung in präziser, transparenter Form und verständlicher und leicht zugänglicher Sprache erfolgen).

Nutzer des Dienstes in Frankreich
Zusätzlich zu den Anforderungen der DSGVO, die oben beschrieben sind, ergibt sich aus dem französischen Datenschutzgesetz eine Pflicht, dass Sie die Betroffenen darüber informieren müssen, dass diese Richtlinien dafür festlegen können, wie mit Ihren personenbezogenen Daten nach Ihrem Tod umgegangen werden soll.

Datenschutzerklärung im Fahrzeug

Da die Erhebung von personenbezogenen Reveal-Daten auf eine Weise erfolgt, die für Betroffene nicht ohne weiteres erkennbar ist, allerdings erhebliche Folgen auslösen kann, sollten Sie zusätzliche Maßnahmen einsetzen, um die Betroffenen auf Ihre Nutzung des Dienstes hinzuweisen. Handreichungen der Datenschutzbehörden verlangen deshalb, dass Sie (zusätzlich zur umfangreichen Datenschutzerklärung, die oben beschrieben wurde) die Betroffenen deutlich darauf hinweisen, dass ein datenerhebendes Gerät in dem betreffenden Fahrzeug installiert ist und dass hierüber sowohl die Bewegungen des Fahrzeugs als auch Informationen zum Fahrverhalten erhoben werden (soweit dies erfolgt). Idealerweise ist diese Information an einer deutlich sichtbaren Stelle des Fahrzeugs angebracht, möglichst innerhalb des durch den Fahrer unmittelbar einsehbaren Bereichs.[2]

Nutzer des Dienstes in Polen
In den Fällen, in denen die Nutzung des Dienstes zu „Arbeitnehmerüberwachung“ führt, sollte der Hinweis im Inneren des Fahrzeugs zusätzlich die folgenden Informationen enthalten:

- Welche Daten werden erhoben und gespeichert;
- Wo und für wie lange werden diese Daten gespeichert; und
- Wer hat Zugriff auf diese Daten[3].

[2] Datenschutzgruppe nach Artikel 29 Stellungnahme *2/2017 Datenverarbeitung im Arbeitsumfeld* (WP249), S.20.
[3] (Polnische) Datenschutzbehörde, *Datenschutz am Arbeitsplatz. Leitlinien für Arbeitgeber*, S. 37.

Durchsetzung von arbeitsrechtlichen Weisungen

Falls Sie personenbezogene Reveal-Daten nutzen wollen, um die Einhaltung Ihrer Regeln und Richtlinien zu überwachen, müssen Sie sicherstellen, dass dies rechtlich zulässig ist, und insbesondere, dass die betroffenen Arbeitnehmer darüber informiert worden sind, welche Regeln mittels des Dienstes überwacht und durchgesetzt werden sollen.

C. Verzeichnis der Verarbeitungstätigkeiten

Als Verantwortlicher für die Datenverarbeitung sind Sie verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten („VVT") gem. Art. 30 der DSGVO zu führen. Diesbezüglich sind Sie verpflichtet, sicherzustellen, dass Ihre Verarbeitung von personenbezogenen Reveal-Daten im VVT berücksichtigt ist. Sie müssen die folgenden Informationen dort aufnehmen:

- Den Namen Ihres Unternehmens sowie Kontaktdaten (sowie ggf. den Namen und Kontaktdaten Ihres betrieblichen Datenschutzbeauftragten, Vertreters in der Union sowie andere gemeinsame Verantwortliche);
- Den Zweck, für den Sie personenbezogene Reveal-Daten verwenden;
- Eine Beschreibung der personenbezogenen Reveal-Daten und der Kategorien der Betroffenen, deren Daten verarbeitet wird;
    - Abschnitt 3 oben zu „Welche personenbezogenen Daten werden durch den Dienst verarbeitet?" unterstützt Sie hierbei.
- Die Kategorien der Betroffenen, an die personenbezogene Reveal-Daten offengelegt werden;
    - Hierbei unterstützen Sie die Angaben in Abschnitt 5 oben, „Wer hat Zugriff auf die personenbezogenen Reveal-Daten?" Sie sollten auch die Empfänger nennen, denen Sie selbst Zugriff auf die personenbezogenen Reveal-Daten geben.
- Übermittlungen von personenbezogenen Reveal-Daten an Länder außerhalb des EWR;
    - Abschnitt 6 oben zu „Übermittelt Verizon personenbezogene Reveal-Daten an Länder außerhalb des EWR?" erklärt für Sie, welche Daten übermittelt werden und welche Schutzmaßnahmen genutzt werden, um die Daten dabei abzusichern.
- Die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
    - Abschnitt 7 oben zu „Wie lange speichert Verizon die personenbezogenen Reveal-Daten?" erklärt dies.
- Informationen zu technischen und organisatorischen Maßnahmen, falls möglich.
    - Die betreffenden Informationen können Sie dem *Verizon Internal Systems Information Security Exhibit* entnehmen, den Sie unter der folgenden URL finden: https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit

Verizon stellt unter der folgenden Internetadresse Informationen bereit, um Sie in Bezug auf Ihr Verfahrensverzeichnis zu unterstützen: https://www.verizon.com/about/privacy/data-processing-activities

Nutzer des Dienstes im Vereinigten Königreich

Falls Sie Daten zu Straftaten auf Basis einer der beiden Voraussetzungen des Anhang 1 des (UK) Data Protection Acts 2018 verarbeiten, dann sind Sie verpflichtet, weitere zusätzliche Informationen in Ihr VVT einzufügen (in Bezug auf die Rechtsgrundlage und Bedingungen für die Verarbeitung sowie Aufbewahrungspflicht- und Löschungsfristen der betreffenden Daten, jeweils im Einklang mit Ihnem „Appropriate Policy Document", wo anwendbar).

D. Zwecke

Sie sind verpflichtet, den Zweck oder die Zwecke festzulegen, für den Sie den Dienst nutzen

und hierbei personenbezogene Reveal-Daten verarbeiten, beispielsweise:

- Erkennen und Verhindern des Verlusts von Eigentum im Bereich Ihres Unternehmens;
- Verbesserung der Produktivität der Mitarbeiter;
- Optimierung der Routenführung und des Ressourcenverbrauchs, insbesondere Kraftstoffeinsparung;
- Angebot von Live-Informationen zum Aufenthaltsort Ihrer Fahrzeuge an Ihre Kunden;
- Gewährleistung der Sicherheit Ihrer Mitarbeiter, z. B. durch die Einhaltung von Pausenzeiten.

Es ist wichtig, dass Sie sich von Anfang an über die Zwecke im Klaren sind, für die der Dienst bereitgestellt wird.

- Sie benötigen eine Rechtsgrundlage für jeden einzelnen Zweck, für den Sie personenbezogene Daten verarbeiten;
- Sie müssen sicherstellen, dass Sie nicht mehr personenbezogene Daten verarbeiten, als es für diesen Zweck vernünftigerweise erforderlich ist;
- Sie müssen den Betroffenen mitteilen, was diese Zwecke sind.

Sobald Sie personenbezogene Daten für diese Zwecke erhoben haben, können Sie diese nur noch für diese Zwecke oder für andere Zwecke verwenden, die mit diesen Zwecken vereinbar sind. Manchmal lässt das geltende Recht allerdings Ausnahmen von diesem Grundsatz zu.

Nutzer des Dienstes in Frankreich

Geolokalisierungsgeräte dürfen nur in Fahrzeugen eingebaut werden, die von Mitarbeitern für folgende Zwecke genutzt werden:[4]

- Verfolgung, Begründung und Abrechnung von Personentransportleistungen;
- Gewährleistung der Sicherheit von Mitarbeitern, Gütern und Fahrzeugen (insbesondere das Auffinden gestohlener Fahrzeuge);
- Optimierung des Ressourceneinsatzes bei der Erbringung von Dienstleistungen in räumlich großen Gebieten, insbesondere im Rahmen von Rettungsdiensten;
- Nachverfolgung der Arbeitszeit (aber nur, wenn keine alternativen Methoden zur Arbeitszeitverfolgung verfügbar sind);
- Erfüllung gesetzlicher oder regulatorischer Verpflichtungen;
- Sicherstellen, dass die Vorschriften des Arbeitgebers über die Verwendung von Arbeitsfahrzeugen eingehalten werden.

Bitte beachten Sie, dass die Nutzung von ortsbezogenen Tracking-Geräten in Mitarbeiterfahrzeugen unzulässig für die folgenden Zwecke ist:

- Zur Überwachung der Einhaltung von Geschwindigkeitsbegrenzungen;
- Zur dauerhaften Überwachung von Angestellten;
- Zur Nachverfolgung und Messung von Arbeitszeit, wo dies auch durch alternative Methoden umgesetzt werden kann;
- In Bezug auf Fahrzeuge von Mitarbeitern, die ihre betrieblichen Abläufe selbst organisieren können (beispielsweise als Handelsvertreter);
- In Bezug auf Fahrzeuge, die durch Mitarbeiter auch privat genutzt werden können, soweit diese Fahrzeuge gerade privat genutzt werden (beispielsweise in Pausenzeiten, oder durch Mitarbeiter, die ihre Fahrten frei gestalten können); oder
- Zur Überwachung von Gewerkschaftsvertretern oder von Personen, die im Rahmen einer ähnlichen Rolle handeln.

Nutzer des Dienstes in Deutschland

Überwachungseinrichtungen, durch die Angestellte dauerhaft überwacht werden können, sind grundsätzlich nicht zulässig[5].

[4] CNIL *Leitlinien zur Geolokalisierung von Mitarbeiterfahrzeugen*, 2018

Nutzer des Dienstes in Polen

Falls und soweit die Nutzung des Dienstes zu einer Überwachung von Arbeitnehmern führt, dürfen Unternehmen personenbezogene Reveal-Daten nur für den legitimen Zweck einsetzten „sicherzustellen, dass Arbeitnehmer ihre Arbeitszeit effektiv einsetzen und dabei die Werkzeuge und Ausrüstung ordnungsgemäß verwenden“. Die polnische Datenschutzaufsichtsbehörde ist der Auffassung, dass dieser legitime Zweck breit zu verstehen ist und unter anderem die folgenden Zwecke zulässt:

- Feststellung, an welchem Ort sich ein Fahrzeug im Falle eines Diebstahls befindet;
- Prüfung, ob ein Mitarbeiter für einen Schaden an einem Fahrzeug haftet; oder
- Optimierung der Routenplanung, Nutzung von Ressourcen und Einsparung von Treibstoff.

Nutzer des Dienstes in Portugal

Der Dienst darf nicht genutzt werden um das Verhalten der Arbeitnehmer zu überwachen und darf in Fahrzeugen nur für die folgenden zulässigen Zwecke eingesetzt werden[6]:

- **Flottenmanagement, falls externe Dienste erbracht werden:**
  - Technische Hilfeleistung;
  - Auslieferung von Waren;
  - Personenbeförderung;
  - Gütertransport; und
  - Private Sicherheitsdienste.

- **Schutz von Waren:**
  - Transport von Gefahrstoffen; und
  - Transport von wertvollen Transportgütern.

Falls der Dienst speziell dafür eingesetzt wird, Fahrzeuge, die üblicherweise von Arbeitnehmern bewegt werden, im Falle eines Diebstahls wieder aufspüren zu können, dürfen Arbeitgeber nur dann auf ortsbezogene Daten zugreifen, falls ein Fahrzeug gestohlen wurde. Andere Fahrzeugdaten (beispielsweise Durchschnittsgeschwindigkeit, Bremsverhalten, Kraftstoffverbrauch) dürfen erhoben werden, jedoch nicht in einer Weise, in der der jeweilige Fahrer identifizierbar wäre.

E. Rechtsgrundlagen

Sie sind verpflichtet, für jeden Zweck, zu dem Sie personenbezogene Reveal-Daten einsetzen, eine Rechtsgrundlage festzulegen. Je nachdem, in welcher Situation Sie den Dienst einsetzen, kommen insbesondere die folgenden Rechtsgrundlagen infrage:

- **Erfüllung einer rechtlichen Verpflichtung**: Beispielsweise, um eine rechtliche Verpflichtung zu erfüllen, die Mitarbeiter bei ihrer Nutzung der Fahrzeuge zu überwachen (Fahrtenschreiber);
- **Erfüllung eines Vertrages mit dem Betroffenen**: Beispielsweise dort, wo gutes Fahrverhalten eine Voraussetzung für das Arbeitsverhältnis darstellt;
- **Erfüllung eines Zwecks, der in Ihrem legitimen Interesse ist**: Beispielsweise zum Schutz Ihrer Fahrer (und anderer Verkehrsteilnehmer), zur Durchsetzung guten Fahrverhaltens, Überwachung einer Fahrzeugflotte, Verbesserung der Fahrzeugnutzung und der notwendigen Wartungsintervalle, Schutzvorkehrungen für den Fall von Unfällen und falschen Beschuldigungen, Schutz der Gesundheit und der Sicherheit der Mitarbeiter, und Erfüllung von Versicherungsverträgen.

[5] Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, *Positionspapier GPS-Ortung*; Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, *Der Ratgeber – Beschäftigtendatenschutz,* 2018, S. 36- 37.

[6] Richtlinie der portugiesischen Datenschutzkommission (CNPD) und portugiesisches Arbeitsgesetz.

Es ist zwingend erforderlich, dass Sie sicherstellen, eine ausreichende Rechtsgrundlage für die Verarbeitung der Daten zu haben. Sie müssen dies ggf. auch gegenüber der Datenschutzbehörde nachweisen können.

Sie werden nachweisen müssen, dass Ihre Verarbeitung von personenbezogenen Reveal-Daten „erforderlich" ist. „Erforderlich" bedeutet, dass die Verarbeitung von personenbezogenen Reveal-Daten direkt dafür erforderlich ist, den jeweiligen Zweck zu erfüllen und die Datenverarbeitung hierfür auch angemessen ist. Die Datenverarbeitung muss „mehr als nur wünschenswert sein, jedoch nicht unbedingt unverzichtbar oder absolut notwendig"[7]. Ob dies der Fall ist, sollten Sie auf Basis der vorliegenden Fakten prüfen und dabei berücksichtigen, ob Ihnen Methoden zur Verfügung stehen, das von Ihnen verfolgte Ziel mit weniger stark eingreifenden Mitteln zu erreichen. Falls es realistischerweise weniger stark eingreifende Alternativen gibt, dann ist das Verarbeiten personenbezogener Daten nicht „erforderlich"[8].

Soweit Sie sich auf die Rechtsgrundlage der Interessenabwägung stützen, müssen Sie die Durchführung dieser Interessenabwägung dokumentieren. Hierbei ist zu prüfen (und nachzuweisen), dass Ihre legitimen Interessen nicht durch entgegenstehende Interessen, Rechte oder Freiheiten der Betroffenen überwogen werden. Die Datenverarbeitung muss für den von Ihnen verfolgten Zweck erforderlich sein, (d. h. angemessen für die Erreichung Ihrer unternehmerischen Zwecke), außerdem sollten weitere Maßnahmen umgesetzt sein, um die Privatsphärenrechte der Betroffenen zu schützen. Falls die Interessen der von der Datenverarbeitung betroffenen Personen Ihre Interessen überwiegen, dann sollte die Datenverarbeitung nicht durchgeführt werden.

Einwilligung: Sie können außerdem personenbezogene Reveal-Daten verarbeiten, falls die Betroffenen hierzu ihre Einwilligung gegeben haben. Eine datenschutzrechtliche Einwilligung ist allerdings nur dann wirksam, wenn sie freiwillig erfolgt ist. Den Betroffenen muss es freistehen, ihre Einwilligung auch zu widerrufen – und zwar ohne Nachteile. Dies führt dazu, dass es in der Regel sehr schwierig ist, im Rahmen eines Arbeitsverhältnisses eine wirksame Einwilligung einzuholen[9].

Eine Reihe von Datenschutzbehörden haben in Bezug auf die Rechtsgrundlagen der Datenverarbeitung bei Telematikdiensten weitere Hinweise veröffentlicht.

Beispielsweise:

- Im Vereinigten Königreich und Polen ist die Überwachung von Fahrzeugen, die auch privat genutzt werden können, während dieser Privatnutzungszeit in der Regel unzulässig, es sei denn, es liegt eine wirksame Einwilligung des Nutzers vor[10].
- In Portugal ist die Einwilligung generell keine wirksame Rechtsgrundlage für die Verarbeitung von Geolokations-Daten[11].
- Geräte zur Fahrzeugüberwachung dürfen nicht eingesetzt werden, um auch das Verhalten

[7] *South Lanarkshire Council* gegen den *Schottischen Datenschutzbeauftragten* [2013] UKSC 55.

[8] Europäischer Datenschutzausschuss (EDPB), *Leitlinien 2/2019 zur Datenverarbeitung nach Artikel 6(1) (b) DSGVO im Zusammenhang mit dem Anbieten von Onlinediensten an Betroffene, angenommen am 9. April 2019*, S. 7.

[9] Beispielsweise werden Einwilligungen von Arbeitnehmern in Deutschland regelmäßig nicht als wirksam angesehen (Landesbeauftragte für Datenschutz und Informationsfreiheit (LDi) NRW, 24. *Datenschutz- und Informationsfreiheitsbericht 2017-2018*, S. 65, 66) und die Einwilligung ist keine wirksame Rechtsgrundlage zur Verarbeitung personenbezogener Daten im Beschäftigungskontext in Portugal (CNPD Leitlinien zur Nutzung von Instrumenten zur Geolokalisierung im Beschäftigungskontext und strenge Auslegung der Bestimmungen des portugiesischen Arbeitsgesetzes).

[10] UK Datenschutzbeauftragter, *Kodex zur Beschäftigungspraxis*, S. 76; (Polnische) Datenschutzbehörde, *Datenschutz am Arbeitsplatz. Leitlinien für Arbeitgeber*, S. 38.

[11] CNPD *Leitlinien zur Nutzung von Instrumenten zur Geolokalisierung im Beschäftigungskontext* und strenge Auslegung der Bestimmungen des portugiesischen Arbeitsgesetzes.

oder den Aufenthaltsort der Fahrzeuge oder anderer Mitarbeiter zu überwachen, beispielsweise indem Benachrichtigungen in Bezug auf die Geschwindigkeit des Fahrzeugs versendet werden[12].

- Die Verarbeitung von Standortdaten kann gerechtfertigt sein, wenn dies im Rahmen der Überwachung des Personen- oder Warenverkehrs, der Verbesserung der Ressourcennutzung oder der Sicherheit des Arbeitnehmers, des Fahrzeugs oder der beförderten Güter dient. Die Verarbeitung von Standortdaten ist allerdings wahrscheinlich exzessiv und damit unzulässig, wenn es den Arbeitnehmern freisteht, ihre Reisen eigenständig zu planen und zu gestalten oder wenn dies erfolgt, um Mitarbeiter zu überwachen, obwohl dies auch mit anderen Mitteln erfolgen kann[13].
  Auch wäre es exzessiv und damit unzulässig, an einem Kunden bei der Auslieferung von Gegenständen nicht nur den Namen und den Aufenthaltsort Ihres Fahrers zu übermitteln, sondern auch dessen Foto. Zwar hätten Sie im Ausgangspunkt ein legitimes Interesse daran, dieses Foto zu übermitteln, sodass Ihre Kunden den Fahrer identifizieren können, allerdings überwiegen in diesem Fall die Gegeninteressen des Betroffenen[14].

Daten über Straftaten

Falls in den personenbezogenen Reveal-Daten, die Sie verarbeiten, auch Daten über Straftaten (entsprechend der jeweils örtlich anwendbaren Gesetze und Interpretation des Begriffs Straftaten) enthalten sind, ergeben sich aus Art. 10 DSGVO zusätzliche Einschränkungen. Die Verarbeitung solcher Daten darf nur unter behördlicher Aufsicht vorgenommen werden, oder falls im Recht der EU oder im nationalen Recht hierfür eine gesonderte Rechtsgrundlage besteht. Hierzu müssen Sie ggf. das örtlich anwendbare Recht prüfen, beispielsweise:

Nutzer des Dienstes in Frankreich
Nach dem französischen Datenschutzgesetz ist es unzulässig, personenbezogene Daten zum Verhalten von Personen zu sammeln, das möglicherweise oder wahrscheinlicherweise als Vergehen oder Verbrechen eingestuft werden könnte. Demzufolge ist es unzulässig, Informationen über die Frage zu sammeln, ob eine bestimmte Person Geschwindigkeitsbegrenzungen überschritten hat, oder weitere Informationen zu einem Verhalten von Personen, das möglicherweise Verkehrsregeln verletzt.

Nutzer des Dienstes in Deutschland
Nach derzeitigem Stand gilt in Deutschland die Nutzung von personenbezogenen Reveal-Daten nicht als Verarbeitung von Daten zu Straftaten. Die Nutzung des Dienstes speziell mit dem Zweck, Straftaten aufzudecken, unterfällt allerdings der Einschränkung in § 26 Abs. 1 BDSG (beispielsweise falls die Bewegungen eines Fahrzeugs überwacht werden um Diebstähle, Betrugshandlungen oder Drogengeschäfte von Angestellten aufzudecken). Die Nutzung von Reveal zur Aufdeckung von Straftaten wäre keine „übliche“ Nutzung von Reveal, sodass eine Datenverarbeitung für diesen Zweck nur in Ausnahmefällen stattfinden wird. Falls Sie als Arbeitgeber Reveal nutzen wollen, um zu ermitteln, ob Angestellte Straftaten begangen haben, sollten Sie vorher § 26 Abs. 1 BDSG prüfen.

Nutzer des Dienstes in Italien
Nutzung von personenbezogenen Reveal-Daten, nicht als die Verarbeitung von „Daten über Straftaten“, so wie dieser Begriff in Italien verstanden wird (es handelt sich lediglich um Ordnungswidrigkeiten). Sie sollten allerdings beobachten, ob etwaige Änderungen im örtlichen Recht dazu führen, dass Straftaten eingeführt werden, für die personenbezogene Reveal-Daten relevant sein könnten.

Nutzer des Dienstes in Polen

[12] WP29 *Stellungnahme 13/2011 zu den Geolokalisierungsdiensten intelligenter mobiler Endgeräte.*

[13] WP29 *Stellungnahme 5/2005 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen.*

[14] WP29 *Stellungnahme 2/2017 Datenverarbeitung im Arbeitsumfeld.*

Nach dem polnischen Arbeitsgesetz 1974, gelten für die Verarbeitung von Daten zu Straftaten von Angestellten zusätzliche rechtliche Anforderungen. Diesbezüglich können Sie Ihre Verarbeitung von Daten über die Angestellten nicht auf deren Einwilligung stützen. Sie müssen deshalb eine alternative Rechtsgrundlage heranziehen, höchstwahrscheinlich die Vertragserfüllung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Nutzer des Dienstes in Portugal

Die Verarbeitung von Daten über Straftaten (wie möglicherweise Verkehrsdelikte) ist unter bestimmten Zuständen zulässig, wenn dies für die Zwecke der Rechtsverteidigung, der Rechtsberatung, oder zur Begründung oder der Durchführung von Gerichtsverfahren erforderlich ist. Die personenbezogenen Daten müssen jedoch innerhalb von 7 Tagen nach der Erhebung pseudonymisiert werden.

Nutzer des Dienstes in Spanien

Allgemein gilt die Verarbeitung von personenbezogenen Reveal-Daten nicht als Verarbeitung von Daten über Straftaten, so wie dieser Begriff in Spanien interpretiert wird (lediglich als Verletzung von Verkehrsregeln). Sie sollten allerdings überwachen, ob es hier zu Rechtsänderungen im spanischen Recht kommt, laut denen die Verarbeitung von personenbezogenen Daten in Reveal in dem Zusammenhang mit Straftaten kommen könnte. Die Verarbeitung von Daten über Straftaten ist in Spanien rechtlich nur eingeschränkt möglich. Die einzigen zulässigen Zwecke der Verarbeitung solcher Daten sind (i) die Vorbeugung, Ermittlung, oder das Vorgehen gegen Straftaten oder die Durchsetzung der Strafe, (ii) falls die Datenverarbeitung durch ein Gesetz oder durch EU-Recht abgedeckt ist.

Nutzer des Dienstes im Vereinigten Königreich

Im Vereinigten Königreich müssen Sie sicherstellen, dass Sie zusätzlich zur Rechtsgrundlage der Datenverarbeitung auch entweder die Bedingungen von Art. 9 DSGVO oder von Anhang 1 des Data Protection Acts 2018 erfüllen. Beispielsweise erlaubt der Data Protection Act 2018 die Verarbeitung von Daten über Straftaten, zum Zweck, gegen solche rechtswidrigen Handlungen vorzugehen oder ihnen vorzubeugen (dies gilt potentiell auch für Verstöße gegen Geschwindigkeitsbegrenzungen oder sonstige Verkehrsregeln). Außerdem können Sie Daten verarbeiten, falls dies im Zusammenhang mit der Durchführung von rechtlichen Maßnahmen, Rechtsberatung oder der Geltendmachung von Rechtsansprüchen steht.

F. Datenminimierung

Sie müssen sicherstellen, dass Sie personenbezogene Reveal-Daten nur in dem Umfang verwenden, wie es dem Zweck angemessen ist. Die Datenverarbeitung muss für den Zweck erheblich sowie auf das für diesen Zweck notwendige Maß beschränkt sein. Dies bedeutet, dass Sie prüfen und klären müssen, welches der minimale Umfang der personenbezogenen Reveal-Daten ist, den Sie verwenden müssen, um Ihre Zwecke zu erreichen.

Falls Sie Mitarbeitern erlauben, die ihnen überlassenen Fahrzeuge auch privat zu verwenden, besteht üblicherweise kein Anlass dazu, Daten über diese Fahrzeuge auch außerhalb der Arbeitszeiten zu erheben. Der Dienst beinhaltet die Möglichkeit, die Datenerhebung über Angestellte außerhalb der Arbeitszeiten zu deaktivieren. Diese Funktion heißt „Privacy Switch“ („Privatschalter“) und ist eine simple und günstige Möglichkeit für Sie, die Einhaltung des anwendbaren Rechts sicherzustellen. In einigen Ländern (so wie Frankreich, Deutschland und Portugal) ist es nach Handreichungen der zuständigen Behörden notwendig, dass Sie den Angestellten den „Privacy Switch“ („Privatschalter“) zugänglich machen[15].

G. Datenrichtigkeit

[15] Der Bayerische Landesbeauftragte für den Datenschutz, 27. Aktivitätsbericht 2016, S. 241; CNIL *Leitlinien zur Geolokalisierung von Mitarbeiterfahrzeugen*, 2018; CNPD Deliberation 7680/2014.

Sie müssen sicherstellen, dass personenbezogene Reveal-Daten weder falsch noch irreführend sind. In Bezug auf personenbezogene Reveal-Daten sollten Sie deshalb Maßnahmen umsetzen, um sicherzustellen, dass personenbezogene Daten sachlich zutreffen sind (beispielsweise indem Sie sicherstellen, dass die Informationen dazu, wem Fahrzeuge jeweils zugewiesen sind, korrekt eingetragen werden). Sie sollten berücksichtigen, dass Betroffene die Richtigkeit der personenbezogenen Daten auch anzweifeln können (beispielsweise könnte ein Fahrer eines Fahrzeugs bestreiten, dass er sich zu einer bestimmten Zeit an einem bestimmten Ort aufgehalten hat).

H. Aufbewahrung der personenbezogenen Reveal-Daten

Sie sollten personenbezogene Reveal-Daten nur so lange aufbewahren, wie dies für den jeweils anwendbaren Zweck der Datenverarbeitung notwendig ist. Sie müssen dabei berücksichtigen, ob rechtliche Vorschriften zur Aufbewahrung dieser Daten gelten (beispielsweise in Bezug auf Arbeitszeiten). Diese rechtlichen Vorschriften müssen Sie auch in Bezug auf Ihr Datenaufbewahrungs- und Löschkonzept berücksichtigen.

I. Datensicherheit der personenbezogenen Reveal-Daten

Sie sind gemäß Art. 32 der DSGVO verpflichtet, zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Reveal-Daten „angemessene technische und organisatorische“ Maßnahmen umzusetzen. Um festzustellen, ob bei Ihrer Benutzung von Reveal und der Verarbeitung von personenbezogenen Reveal-Daten besondere Risiken entstehen, sowie um festzustellen, welche Datensicherheitsmaßnahmen „angemessen“ sind, können Sie eine Risiko-Prüfung durchführen. Nachdem Sie Ihre technischen und organisatorischen Maßnahmen implementiert haben, sollten Sie in regelmäßigen Abständen prüfen, ob diese weiterhin angemessen sind. Falls Sie personenbezogene Reveal-Daten an einen Dritten weitergeben, der als Auftragsverarbeiter für Sie tätig wird, sind Sie verpflichtet, zu prüfen, ob dieser Auftragsverarbeiter ebenfalls angemessene technische und organisatorische Maßnahmen umgesetzt hat, um die personenbezogenen Daten zu schützen (und sich hierzu auch vertraglich verpflichtet).

Im Fall einer Sicherheitsverletzung, die sich auf personenbezogene Daten bezieht, ergeben sich Ihre Pflichten aus Art. 33 und 34 der DSGVO. Wir werden Sie hierüber ohne schuldhaftes Zögern informieren. In diesem Fall könnten Sie verpflichtet sein, die zuständige Datenschutzaufsichtsbehörde innerhalb von 72 Stunden, nachdem Sie auf den Vorfall aufmerksam geworden sind, zu informieren (es sei denn, Sie sind der Auffassung, dass der Vorfall voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt). In Fällen, in denen der Vorfall voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten betroffener Personen führen könnte, sind Sie außerdem verpflichtet, diese Betroffenen unverzüglich zu benachrichtigen. Sie sollten Schritte unternehmen, um sicherzustellen, dass Sie in der Lage sind, eine Sicherheitsverletzung in Bezug auf personenbezogene Reveal-Daten korrekt einzustufen, und danach die notwendigen Schritte zu unternehmen, um Folgen dieser Sicherheitsverletzung einzudämmen. Sie sollten sich außerdem darauf vorbereiten, wie Sie einen Verstoß ggf. eskalieren würden und wie Ihre Organisation bewerten würde, ob eine Benachrichtigung der Behörde oder von Betroffenen erforderlich ist.

<u>Nutzer des Dienstes in Frankreich</u>
Nach den Vorschriften der CNIL über die Verarbeitung von Geolokationsdaten von Mitarbeiterfahrzeugen[16], sollten Sie insbesondere die folgenden Maßnahmen umsetzen:

- Ein Zugangs- und Berechtigungskonzept;
- Maßnahmen zur Datensicherheit bei Übermittlung; und

[16] CNIL *Leitlinien zur Geolokalisierung von Mitarbeiterfahrzeugen,* 2018.

- Ein Protokoll über den Datenzugriff und die Datenverarbeitungsvorgänge.

Nutzer des Dienstes in Spanien

Für den Fall, dass personenbezogene Daten berichtigt oder gelöscht werden, schreibt das spanische Datenschutzgesetz vor, dass Verantwortliche diese Daten im Rahmen ihrer Umsetzung von Art. 32 DSGVO „sperren" müssen. Dies bedeutet, dass die betreffenden Daten aus der Datenbank entnommen und in einer separaten Datenbank gespeichert werden müssen. Es sind technische und organisatorische Maßnahmen umzusetzen, dass die Verarbeitung solcher Daten nicht erfolgt (einschl. des Datenzugriffs und der Einsehbarkeit der Daten). Um sicherzustellen, dass der Verantwortliche ggf. Anordnungen durch zuständige öffentliche Stellen (beispielsweise Gerichte, Staatsanwaltschaften oder Datenschutzaufsichtsbehörden, etc.) erfüllen kann oder für den Fall, dass die Übermittlung solcher Daten an solche öffentliche Stellen notwendig ist, um Rechtsansprüche geltend zu machen oder sich dagegen zu verteidigen, sind die betreffenden personenbezogenen Daten in einer getrennten und besonders geschützten Datenbank zu speichern. Um zu ermitteln, für welchen Zeitraum die personenbezogenen Daten „gesperrt" aufzubewahren sind, ist auf die jeweils anwendbaren Verjährungsvorschriften abzustellen. Sobald die anwendbaren Verjährungsvorschriften abgelaufen sind, können die personenbezogenen Daten vollständig gelöscht werden.

Als Verantwortlicher für die Verarbeitung von personenbezogenen Reveal-Daten sind Sie dafür zuständig, diese Verpflichtungen umzusetzen. Verizon wird Sie hierbei unterstützen. Dies erfolgt entweder, indem Ihnen die Möglichkeit gewährt wird, personenbezogene Reveal-Daten über die für Sie nutzbare Weboberfläche von Reveal herunterzuladen. Auf Anforderung kann Ihnen Verizon auch andere personenbezogene Reveal-Daten zur Verfügung stellen.

J. Betroffenenrechte

Sie sind verpflichtet dazu, zu prüfen, auf welche Weise Sie mit Betroffenen umgehen, die ihre Betroffenenreche geltend machen. Nach der DSGVO können Betroffene die folgenden Rechte in Bezug auf ihre personenbezogenen Daten geltend machen:

- Das Recht auf Auskunft;
- Das Recht auf Berichtigung;
- Das Recht auf Löschung;
- Das Recht auf Einschränkung der Verarbeitung;
- Das Recht auf Datenübertragbarkeit;
- Das Widerspruchsrecht;
- Rechte in Bezug auf automatische Entscheidungen im Einzelfall und Profiling.

Sie müssen die Betroffenen in Ihrer Datenschutzerklärung darauf hinweisen, dass diese die oben genannten Rechte geltend machen können.

Die Anwendbarkeit dieser Rechte kann eingeschränkt sein (beispielsweise gilt das Recht auf Daten-Portabilität nur in Fällen, wo personenbezogene Daten auf Basis der Rechtsgrundlage der Vertragserfüllung oder der Einwilligung verarbeitet werden). Sie können außerdem unter bestimmten Voraussetzungen die Erfüllung der Betroffenenrechte verweigern (beispielsweise im Fall der Anforderung einer Datenkopie, falls dies die Rechte Dritter beeinträchtigen könnte, was auch den Schutz von Geschäftsgeheimnissen beinhalten kann).

Sie sind verpflichtet, üblicherweise auf solche Anfragen innerhalb eines Monats zu reagieren. Für die Beantwortung der Anfrage gelten zusätzliche Anforderungen nach Art. 12 DSGVO (beispielsweise müssen Informationen, die Sie den Betroffenen überlassen präzise, transparent, verständlich, leicht zugänglich und in einer klaren und einfachen Sprache verfasst sein).

Wo dies möglich ist, kann Verizon Sie dabei unterstützen, derartige Anfragen von Betroffenen

in Bezug auf den Dienst umzusetzen.

Nutzer des Dienstes in Frankreich
Nach dem französischen Datenschutzgesetz, haben Betroffene das Recht, Richtlinien in Bezug auf den Umgang mit personenbezogenen Daten nach Ihrem Tod festzulegen. Die müssen sicherstellen, dass Sie diese Art von Anfrage ggf. erfüllen können.

K. Übermittlung von personenbezogenen Reveal-Daten

Sie sollten sich darauf vorbereiten, personenbezogene Daten nicht nur an Betroffene herauszugeben, sondern auch an Dritte. Dies gilt beispielsweise falls zuständige Strafverfolgungsbehörden oder Versicherer Daten anfordern, nachdem ein Fahrzeug in einen Unfall verwickelt war.

Jede Übermittlung von personenbezogenen Reveal-Daten muss die datenschutzrechtlichen Anforderungen erfüllen, die in diesem eBook beschrieben sind (beispielsweise muss die Übermittlung der Daten rechtmäßig, angemessen und transparent sein, etc.). Die gilt auch für die Übermittlung von Daten innerhalb einer Unternehmensgruppe (Konzern) oder an andere Dienstleister. Sie sollten prüfen, ob in Bezug auf die Übermittlung dieser Daten der Abschluss von Verträgen oder anderen Vereinbarungen notwendig ist (beispielsweise wenn es sich bei dem anderen um einen Auftragsverarbeiter in Ihrem Auftrag oder um einen „gemeinsamen Verantwortlichen" handelt). Falls personenbezogenen Reveal-Daten in einen Staat außerhalb des Europäischen Wirtschaftsraums („EWR") übermittelt werden, müssen Sie sicherstellen, dass diese Übermittlung nach der DSGVO zulässig ist.

Nutzer des Dienstes in Frankreich
Nach Richtlinien der CNIL, müssen Sie den Zugriff auf personenbezogenen Daten, die über Geolokations-Geräte erhoben worden sind, wie folgt einschränken: (i) auf Ihre eigenen dafür bevollmächtigten Mitarbeiter, (ii) den Arbeitgeber des Mitarbeiters, auf den sich die Ortsdaten beziehen, sowie (iii) autorisierte Mitarbeiter eines Kunden, an den Sie jeweils Dienstleistungen erbringen. Allgemein ist es unzulässig, den Namen des jeweiligen Fahrers zu übermitteln, es sei denn, diese Information ist besonders relevant und erforderlich.

L. Automatisierte Entscheidungsfindung

Es ist datenschutzrechtlich untersagt, wenn Unternehmen gegenüber Betroffenen Entscheidungen treffen, die ausschließlich auf einer automatisierten Verarbeitung beruhen, gegenüber den Betroffenen aber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen. Sie sollten prüfen, ob Ihre Nutzung des Dienstes in den Anwendungsbereich dieser Vorschrift fällt. Dies könnte in den folgenden Fällen der Fall sein:

- Das Gehalt eines Fahrers ergibt sich automatisch aus der Zeit, in der ein betreffendes Fahrzeug in Betrieb war;
- Es wird automatisch eine Warnmeldung an den Fahrer geschickt, falls dieser ein bestimmtes geografisch eingeschränktes Gebiert verlässt (Geo Fence);
- Ob der betreffende Mitarbeiter ein Bonus erhält, ergibt sich automatisch daraus, in welchem Umfang an diesen Mitarbeiter Aufgaben zugewiesen und erfüllt worden sind, wobei sich dies aus Daten ergibt, die aus dem Dienst stammen.

Falls eine ausreichende Prüfung der Entscheidung durch einen Menschen erfolgt, bevor sie getroffen wird, sind die oben genannten Einschränkungen nicht anwendbar.

Es ist für Unternehmen zulässig, die oben genannten automatisierten Entscheidungen zu treffen, falls die Entscheidungen notwendig sind, um:

- Für den Abschluss oder die Erfüllung eines Vertrags mit dem Betroffenen erforderlich sind;
- Wo dies aufgrund von Rechtsvorschriften der EU oder des auf Sie anwendbaren

nationalen Rechts zulässig ist, falls dieses Recht angemessene Maßnahmen zur Wahrung und Rechte der Freiheiten der betroffenen Personen enthält; oder
- Auf Basis der ausdrücklichen Einwilligung der betroffenen Person.

Falls eine automatisierte Entscheidungsfindung erfolgt, sind Sie verpflichtet, die Betroffenen hierauf in transparenter Form hinzuweisen (siehe oben, Datenschutzerklärung). Im Übrigen, sind Sie verpflichtet, sicherzustellen, dass die automatisierte Entscheidung ggf. durch eine menschliche Person überprüft wird, wobei die Betroffenen auch ein Recht haben, ihren eigenen Standpunkt darzulegen.

Nutzer des Dienstes in Portugal
Die Nutzung von Geolokationsdaten sowie Daten, die aus Fahrzeug-Telematik-Geräten erhoben wurden, zum Zweck der automatisierten Entscheidungsfindung ist nicht zulässig[17].

M. Konsultationen mit Mitarbeitern, Betriebsräten und Gewerkschaften

Nach dem anwendbaren Arbeitsrecht können Sie verpflichtet sein, Ihre Angestellten, Betriebsräte oder ggf. Gewerkschaften in Bezug auf die Nutzung des Dienstes oder weiterer Nutzung der personenbezogenen Reveal-Daten zu konsultieren. Eine solche Pflicht kann sich evtl. auch aus Vereinbarungen zwischen Ihnen und Gewerkschaften oder Betriebsräten ergeben, falls diese bestehen. Selbst in Fällen, wo dies rechtlich nicht vorgeschrieben ist, kann es für Sie angemessen sein, den Austausch mit Mitarbeitern in Bezug auf ihre Nutzung des Dienstes und der personenbezogenen Reveal-Daten zu suchen, während Sie eine DSFA durchführen.

Falls Sie mit Ihrem Betriebsrat eine verbindliche Betriebsvereinbarung abschließen, dann stellt dies eine „spezifischere" Vorschrift im Sinn von Art. 88 Abs. 1 DSGVO dar. Aus einer solchen Vereinbarung kann sich demzufolge unter bestimmten Umständen Rechtssicherheit darüber ergeben, unter welchen Umständen Reveal in Ihrem Unternehmen eingesetzt werden kann. Um als „spezifischere" Vorschrift zu gelten, muss die Betriebsvereinbarung im Rahmen des anwendbaren Arbeitsrechts verbindlich gelten und angemessene und besondere Maßnahmen der datenschutzrechtlichen Interessen der betroffenen Personen enthalten (siehe Art. 88 Abs. 2 DSGVO). Im Fall von Zweifeln, sollten Sie Rechtsrat einholen.

Nutzer des Dienstes in Frankreich
Gem. Art. L2312-38 des Französischen Arbeitsgesetzes, müssen Sie einen Betriebsrat (*Conseil Economique et Social*) sowohl informieren als auch konsultieren, bevor Sie Systeme einführen, die die Überwachung von Mitarbeitern am Arbeitsplatz ermöglichen würden, einschl. der Überwachung von Orten und Bewegungen.

Nutzer des Dienstes in Deutschland
Nach § 87 Abs. 6 des Betriebsverfassungsgesetzes (BetriebsVG) hat ein Betriebsrat, falls ein solcher in Ihrem Betrieb besteht, das Recht auf Mitbestimmung bei der Einführung und Nutzung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Eine dauerhafte Überwachung des Verhaltens von Arbeitnehmern und deren Leistung durch Überwachungseinrichtungen ist nicht zulässig. Falls Sie der Arbeitgeber sind, sind Sie verpflichtet, eine solche permanente Überwachung von Arbeitnehmern im Rahmen einer Betriebsvereinbarung oder durch eine ggf. einseitig bindende Erklärung auszuschließen[18].

[17] CNPD Leitlinien zur Nutzung von Instrumenten zur Geolokalisierung im Beschäftigungskontext und strenge Auslegung der Bestimmungen des portugiesischen Arbeitsgesetzes.

[18] Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, *Der Ratgeber - Beschäftigtendatenschutz*, 2018 ; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Aktivitätsbericht 2017-2018, 103.

§ 26 Abs. 4 BDSG bestätigt ausdrücklich, dass die Verarbeitung personenbezogener Daten zulässig ist, wenn dies auf Basis einer Betriebsvereinbarung erfolgt, vorausgesetzt, dass diese Betriebsvereinbarung die Kriterien von Art. 88 Abs. 2 DSGVO erfüllt.

Nutzer des Dienstes in Italien
Gem. Art. 4 Abs. 2 des Gesetzes Nr. 300/1970 (Italienisches Arbeitergesetz), sind Sie verpflichtet, die für Ihr Unternehmen zuständige Gewerkschaft zu konsultieren sowie eine Genehmigung des zuständigen Arbeitsamts einzuholen. Dies gilt jedoch nicht, wenn Sie personenbezogene Reveal-Daten ausschließlich einsetzen, um rechtliche Verpflichtungen zu erfüllen.

Nutzer des Dienstes in Polen
Sie sind verpflichtet, den Zweck, den Umfang und die Methoden der Überwachung von Arbeitnehmern entweder in Ihrer Arbeitsordnung (dies ist eine interne Bestimmung, die für Arbeitgeber gilt, die mehr als 50 Angestellte in Polen beschäftigen) oder in Ihrer Betriebsvereinbarung festzuhalten. Falls in Ihrem Betrieb Gewerkschaften aktiv sind, bedarf eine Änderung der Arbeitsordnung oder der Betriebsvereinbarung der Zusammenarbeit mit der Gewerkschaft.

Falls Sie ein Überwachungssystem neu einführen möchten, sollten Sie Ihre Arbeitnehmer hierauf hinweisen. Dies sollte spätestens zwei Wochen erfolgen bevor das betreffende System eingeführt wird.

Nutzer des Dienstes in Portugal
Nach Art. 21 des portugiesischen Arbeitsgesetzes müssen Sie Betriebsräte (Comissão de Trabalhadores) informieren und konsultieren, bevor Sie Systeme oder andere Möglichkeiten einführen, um das Verhalten von Angestellten zu überwachen, einschl. Geolokations-Systemen.

Nutzer des Dienstes in Spanien
Gem. Art. 64 Abs. 1 des spanischen Arbeitsgesetzes sind Sie verpflichtet, die Vertreter der Arbeitnehmer über Änderungen, die sich auf die Arbeitnehmer auswirken könnten, vorab zu informieren. Diese Vorschrift bezieht sich auch auf die Einführung von Geolokations-Systemen oder andere Möglichkeiten zur Überwachung von Arbeitnehmern.

Hinzu kommt, dass auch gem. Art. 90 Abs. 2 des Gesetzes 3/2018 vom 5. Dezember, Angestellte und Arbeiter informiert werden müssen, bevor Geolokations-Systeme in einem Betrieb eingeführt werden. Die Betroffenen sind sowohl über die Existenz solcher Systeme zu informieren, als auch über deren Merkmale.

N. Umgang mit Datenschutz-Risiken und Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Sie sollten sicherstellen, dass alle Schritte, die notwendig sind, um Risiken für die Betroffenen zu beschränken, umgesetzt sind. Die Notwendigkeit solcher Schritte kann sich insbesondere aus einer durchgeführten Datenschutzfolgenabschätzung ergeben. Sie sollten außerdem die rechtlichen Vorgaben zum „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“ beachten. Datenschutz durch Technikgestaltung bedeutet, dass datenschutzrechtliche Themen bereits während der Planung einer Datenverarbeitung (d. h. während der Design Phase) zu berücksichtigen sind. Dies gilt dann auch für alle weiteren Phasen der Datenverarbeitung. Ihre Pflicht zur Umsetzung von datenschutzfreundlichen Voreinstellungen verpflichtet Sie dazu, sich durch Voreinstellungen sicherzustellen, dass grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen Verarbeitungszweck notwendig ist. Beispielsweise sollten Zugriffsrechte auf personenbezogene Reveal-Daten immer nur in dem Umfang eingeräumt werden, wie dies für den jeweiligen Zweck notwendig ist (Need-to-know).

Verschiedene Handreichungen von Datenschutzaufsichtsbehörden enthalten Beispiele für Maßnahmen der Risikobeschränkung im Zusammenhang mit Telematik-Diensten und Arbeitnehmerüberwachung:

- Mitarbeitern sollte möglich sein, die Geolokations-Überwachung von Fahrzeugen ggf. abzuschalten, wenn dies angemessen ist (beispielsweise wenn sie eine medizinische Versorgungseinrichtung aufsuchen). Dies gilt jedenfalls dann, wenn die Arbeitnehmer die betreffenden Fahrzeuge auch für private Zwecke nutzen dürfen[19].
- Falls es notwendig ist, die Orte eines Fahrzeugs außerhalb der Arbeitszeiten der Angestellten zu überwachen (beispielsweise als Vorbeugung gegen Diebstahl), sollte diese Überwachung so umgesetzt werden, dass die Interessen der Betroffenen nicht unverhältnismäßig beeinträchtigt werden. D. h., dass der Standort von Fahrzeugen außerhalb der üblichen Arbeitszeiten nicht erhoben werden sollte bzw. nicht sichtbar sein sollte, es sei denn, das Fahrzeug verlässt ein bestimmtes eingegrenztes Gebiet[20].
- Die Anzahl der Personen, die Zugriff auf personenbezogene Reveal-Daten nehmen können, sollte so klein wie möglich sein. Die Mitarbeiter sollten entsprechend geschult sein, sowie auf die Einhaltung von Vertraulichkeits- und Sicherheitsmaßnahmen verpflichtet sein.[21]
  Sie sollten prüfen, welche Mitarbeiter dafür geeignet sind, auf personenbezogene Reveal-Daten zuzugreifen (dies können beispielsweise die jeweiligen Dienstvorgesetzten sein)[22].

O. Benennung eines Datenschutzbeauftragten

Gem. Art. 37 DSGVO kann sich die Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu benennen, aus verschiedenen Gründen ergeben. Auch dann, wenn Ihre bisherigen Datenverarbeitungsaktivitäten noch nicht dazu geführt haben, dass Sie einen Datenschutzbeauftragten benennen müssten, kann sich eine solche Pflicht gem. Art. 37 Abs. 1 (b) DSGVO aus Ihrer Nutzung des Dienstes ergeben. Dies kann dann der Fall sein, wenn eine Ihrer Kerntätigkeiten in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke ein umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen. Falls Sie den Dienst nutzen, um Fahrer in Bezug auf deren Verhalten zu überwachen, ist dies gem. Art. 37 Abs. 1 (b) DSGVO wahrscheinlich der Fall, sodass Sie verpflichtet sind, einen betrieblichen Datenschutzbeauftragten zu benennen. Die Rechte und Pflichten eines Datenschutzbeauftragten ergeben sich aus den Art. 38 und 39 DSGVO. Falls Sie einen Datenschutzbeauftragten benennen, müssen Sie diese Vorschriften einhalten.

<u>Nutzer des Dienstes in Deutschland</u>
Gem. § 38 BDSG sind Sie außerdem auch dann verpflichtet, einen Datenschutzbeauftragten zu benennen, falls in Ihrem Betrieb in der Regel mind. 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Außerdem gilt diese Pflicht, falls Sie der Pflicht zur Durchführung einer Datenschutzfolgenabschätzung unterliegen. Sie sind demzufolge sehr wahrscheinlich verpflichtet, einen betrieblichen Datenschutzbeauftragten zu benennen, falls Sie die Dienste in Deutschland nutzen.

Weitere Informationen

Gesetzgebung

- Datenschutzgrundverordnung (EU) 2016/679 (“DSGVO”)

[19] Artkel 29 Datenschutzgruppe *Stellungnahme 2/2017 zur Datenverarbeitung im Arbeitsumfeld* (WP249), S.20.
[20] Artkel 29 Datenschutzgruppe *Stellungnahme 2/2017 zur Datenverarbeitung im Arbeitsumfeld* (WP249), S.20.
[21] UK Datenschutzbeauftragter, *Kodex zur Beschäftigungspraxis,* S. 67.
[22] UK Datenschutzbeauftragter, *Kodex zur Beschäftigungspraxis,* S.67.

- Datenschutzgesetz 2018 (UK)
- Gesetz 58/2019, 8. August 2019 (Portugal)
- Arbeitsgesetz (Portugal)
- Verfassungsgesetz 3/2018, 5. Dezember 2018, über den Schutz personenbezogener Daten und die Gewährleistung digitaler Rechte (Spanien)
- Bundesdatenschutzgesetz (BDSG) 2018 (Deutschland)
- Betriebsverfassungsgesetz (BetriebsVG) (Deutschland)
- Gesetzesdekret Nr. 196/2003 (Italienisches Datenschutzgesetz) (Italien)
- Gesetz Nr. 300/1970 (Italienisches Arbeitsgesetz) (Italien)
- Gesetzesdekret Nr. 101/2018 (Italien)
- Französisches Datenschutzgesetz Nr. 78-17(Frankreich)
- Französisches Arbeitsgesetz (Frankreich)

Rechtsprechung

South Lanarkshire Council gegen den Schottischen Datenschutzbeauftragten [2013] UKSC 55 (UK)

Leitlinien zur Regulatorik

EU

- Artikel 29 Datenschutzgruppe Stellungnahme *5/2005 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen* (WP115)
- Artikel 29 Datenschutzgruppe *Stellungnahme 13/2011 zu den Geolokalisierungsdiensten intelligenter mobiler Endgeräte* (WP 185)
- Artikel 29 Datenschutzgruppe *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"* (WP248)
- Artikel 29 Datenschutzgruppe *Stellungnahme 2/2017 Datenverarbeitung im Arbeitsumfeld* (WP249)
- Artikel 29 Datenschutzgruppe *Leitfaden zu Profiling und automatisierten Einzelentscheidungen* (WP251)
- Europäischer Datenschutzausschuss *Leitlinien 2/2019 zur Datenverarbeitung nach Artikel 6 (1) (b) DSGVO im Zusammenhang mit dem Anbieten von Onlinediensten an Betroffene (Version für öffentliche Konsultationen)*

Frankreich

- CNIL *Leitlinien zur Geolokalisierung von Mitarbeiterfahrzeugen*, 2018

Deutschland

- Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, *Positionspapier GPS-Ortung*
- Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, *Der Ratgeber - Beschäftigtendatenschutz*, 2018
- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Kurzpapier Nr. 14: *Beschäftigtendatenschutz* (17. Dezember 2018)
- Der Bayerische Landesbeauftragte für den Datenschutz, *27. Aktivitätsbericht 2016*
- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK), Kurzpapier Nr. 17: *Besondere Kategorien von personenbezogenen Daten* (27. März 2018)
- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK), Kurzpapier Nr. 19: *Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO* (29. May 2018)

- Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDi NRW), 24. Datenschutz- und Informationsfreiheitsbericht 2017-2018, *Satellitengestützte Ortung zur Positionsbestimmung von Firmenfahrzeugen – kein zulässiges Mittel für eine Überwachung von Beschäftigten.*
- Berliner Beauftragte für Datenschutz und Informationsfreiheit, *Jahresbericht 2018*
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Aktivitätsbericht 2017-2018
- Die Landesbeauftragte für den Datenschutz Niedersachsen, 24. Aktivitätsbericht 2017-2018, *GPS-Überwachung von Firmenfahrzeugen*

Polen

- (Polnische) Datenschutzbehörde, *Datenschutz am Arbeitsplatz. Leitlinien für Arbeitgeber*

Portugal

- CNPD Deliberation 7680/2014 (Leitlinien zur Nutzung von Instrumenten zur Geolokalisierung im Beschäftigungskontext).

UK

- UK Datenschutzbeauftragter, *Kodex zur Beschäftigungspraxis und ergänzende Hinweise*

DSGVO Checkliste

DSGVO Artikel	Thema	Relevanz für Reveal	Referenz zum eBook
Art. 1, 2 oder 3	Gegenstand und Ziele; sachlicher ;und räumlicher Anwendungsbereich	Keine spezielle Relevanz	N/A
Art. 4	Begriffsbestimmungen	Definiert die Konzepte von 'Personenbezogen' und 'besonderen' Kategorien von personenbezogenen Daten	"*Reveal FAQs*", Abschnitte 3 und 4
Art. 5	Grundsätze für die Verarbeitung personenbezogener Daten	Die Verarbeitung von personenbezogenen Daten im Rahmen von Reveak muss mit den Grundsätzen für die Verarbeitung übereinstimmen und der Verantwortliche muss in der Lage sein, die Einhaltung dieser Grundsätze nachzuweisen	"*Datenschutzrechtliche Anforderungen*", allgemein
Art. 6 und 7	Rechtmäßigkeit der Verarbeitung und Bedingungen für die Einwilligung	Für jeden Zweck der Datenverarbeitung im Rahmen von Reveal muss eine Rechtsgrundlage vorhanden sein.	"*Datenschutzrechtliche Anforderungen*", Abschnitt E
Art. 8	Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft	Keine besondere Relevanz	N/A
Art. 9 und 10	Verarbeitung besonderer Kategorien personenbezogener Daten	Für jeden Zweck der Verarbeitung von personenbezogenen	"*Reveal FAQs*", Abschnitt 4, and "*Datenschutzrechtliche Anforderungen*", Abschnitt E

	und Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.	Daten im Rahmen von Reveal muss eine Bedingung erfüllt sein, wenn es sich bei den personenbezogenen Daten um Daten einer besonderen Kategorie oder um Informationen über Straftaten handelt.	
Art. 11	Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist	Keine besondere Relevanz	N/A
Art. 12	Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person	Sämtliche Informationen, die den Personen erteilt werden, deren personenbezogene Daten im Rahmen von Reveal verarbeitet werden, müssen präzise, transparent, verständlich und leicht zugänglich sein und sind in einer klaren und einfachen Sprache zu übermitteln.	"*Datenschutzrechtliche Anforderungen*", Abschnitte B and J
Art. 13 und 14	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person; Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden	Den Personen deren personenbezogene Daten im Rahmen von Reveal verarbeitet werden, muss eine Datenschutzerklärung zur Verfügung gestellt werden.	*"Datenschutzrechtliche Anforderungen*", Abschnitt B
Art. 15	Auskunftsrecht der betroffenen Person	Betroffenen muss auf Verlangen Zugang zu Reveal gewährt werden (Ausnahmen vorbehalten)	*"Datenschutzrechtliche Anforderungen*", Abschnitt J
Art. 16	Recht auf Berichtigung	Personenbezogene Reveal-Daten müssen auf Verlangen hin berichtigt werden	*"Datenschutzrechtliche Anforderungen*", Abschnitt J
Art. 17	Recht auf Löschung ("Recht auf Vergessenwerden")	Personenbezogene Reveal-Daten müssen auf Verlangen eines Betroffenen gelöscht werden, wenn das Recht dazu besteht.	*"Datenschutzrechtliche Anforderungen*", Abschnitt J
Art. 18	Recht auf Einschränkung der Verarbeitung	Die Verarbeitung personenbezogener Reveal Daten muss auf Verlangen eines Betroffenen	*"Datenschutzrechtliche Anforderungen*", Abschnitt J

		eingeschränkt werden, wenn das Recht dazu besteht.	
Art. 19	Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Vearbeitung	Wenn ein Verlangen von Berichtigung, Löschung oder Einschränkung erhalten wird, das sich auf personenbezogene Reveal Daten bezieht, muss Dritten, denen gegenüber Daten offenbart wurden über das Verlangen in Kenntnis gesetzt werden.	*"Datenschutzrechtliche Anforderungen*", Abschnitt J
Art. 20	Recht auf Datenübertragbarkeit	Personenbezogene Reveal Daten müssen auf Verlagen an Betroffene übertragen werden (oder an von diesen benannte Dritte), wenn dieses Recht besteht.	*"Datenschutzrechtliche Anforderungen*", Abschnitt J
Art. 21	Widerspruchsrecht	Auf Verlangen eines Betroffenen dürfen personenbezogene Reveal Daten nicht weiter verarbeitet werden, wenn dieses Recht besteht.	*"Datenschutzrechtliche Anforderungen*", Abschnitt J
Art. 22	Automatisierte Entscheidungen im Einzelfall einschließlich Profiling	Automatisierte Entscheidungen im Einzelfall, die rechtliche oder ähnlich bedeutende Auswirkungen für den Betroffenen haben, dürfen nur in Übereinstimmung mit Art. 22 DSGVO getroffen werden.	*"Datenschutzrechtliche Anforderungen*", Abschnitt L
Art. 23	Beschränkungen	Keine besondere Relevanz	N/A
Art. 24	Verantwortung des für die Verarbeitung Verantwortlichen	Es sollten angemessene technische und organisatorische Maßnahmen getroffen werden, um sicherzustellen (und nachzuweisen), dass die Verarbeitung in Übereinstimmung mit den Vorgaben der DSGVO stattfindet.	"*Datenschutzrechtliche Anforderungen*", allgemein
Art. 25	Datenschutz durch	Datenschutzfragen	*"Datenschutzrechtliche*

	Technikgestaltung und durch datenschutzfreundliche Voreinstellung	sollten zu Beginn und während des Lebenszyklus der Verarbeitung von personenbezogenen Reveal Daten geklärt werden und es sollten ausschließlich die zur Erreichung der Zwecke von Verizon Connect notwendigen Daten verarbeitet werden.	*Anforderungen*", Abschnitte F und N
Art. 26	Gemeinsam Verantwortliche	Keine besondere Relevanz	N/A
Art. 27	Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder des Auftragsverarbeiters	Keine besondere Relevanz	N/A
Art. 28	Auftragsverarbeiter	Es sollten nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragt werden, die hinreichende Garantien bieten; die Auftragsverarbeiter müssen hinreichenden vertraglichen Verpflichtungen unterworfen werden.	*"Datenschutzrechtliche Anforderungen*", Abschnitt I
Art. 29	Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters	Keine besondere Relevanz	N/A
Art. 30	Verzeichnis von Verarbeitungstätigkeiten	Die Verarbeitung der personenbezogenen Daten muss sich in dem Verarbeitungsverzeichn is widerspiegeln.	*"Datenschutzrechtliche Anforderungen*", Abschnitt C
Art. 31	Zusammenarbeit mit der Aufsichtsbehörde	Keine besondere Relevanz	N/A
Art. 32	Sicherheit der Verarbeitung	Es müssen angemessene technische und organisatorische Maßnahmen vorhanden sein, um die Sicherheit der personenbezogenen Reveal Daten zu gewährleisten.	*"Datenschutzrechtliche Anforderungen*", Abschnitt I
Art. 33 und 34	Meldung von Verletzungen des Schutzes personenbezogener Daten an	Im Falle einer Datenschutzverletzung müssen die	*"Datenschutzrechtliche Anforderungen*", Abschnitt I

	die Aufsichtsbehörde und Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person	Aufsichtsbehörde und betroffene Personen informiert werden, wenn die Schwellen hierfür überschritten wurden.	
Art. 35 und 36	Datenschutzfolgeabschätzung und vorherige Konsultation	Eine Datenschutzfolgeabschätzung muss durchgeführt werden, um personenbezogene Reveal Daten verarbeiten zu können und Konsultationen mit den Aufsichtsbehörden können notwendig sein, wenn die Verarbeitung ein hohes und uneingeschränktes Risiko für Personen darstellt.	*"Datenschutzrechtliche Anforderungen*", Abschnitt A
Art. 37, 38 und 39	Datenschutzbeauftragter	Ein Datenschutzbeauftragter muss benannt werden, wenn die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsprozessen besteht, die aufgrund ihres Umfangs eine regelmäßige und systematische Überwachung von betroffenen Personen darstellen oder der Verarbeitung besonderer Kategorien personenbezogener Daten/ Daten über Straftaten in großem Ausmaß besteht.	"*Datenschutzrechtliche Anforderungen",* Abschnitt Q
Art. 40, 41, 42 und 43	Verhaltensregeln, Zertifizierungen und Akkreditierung	Keine besondere Relevanz	N/A
Art. 44 - 50	Übermittlungen personenbezogener Daten	Jegliche Übertragung von personenbezogenen Reveal Daten außerhalb des EWRs in Länder, die nicht “adäquat” sind (z.B. zu anderen Plattformbetreibern oder anderen Unternehmen der	"*Reveal FAQs*", Abschnitt 6, und *"Datenschutzrechtliche Anforderungen*", Abschnitt K

		Gruppe) darf nur stattfinden, wenn ein Übertragungsmechanismus vorhanden ist oder eine Ausnahmeregelung besteht.	
Art. 51 - 59	Aufsichtsbehörde und Zuständigkeit, Aufgaben, Befugnisse und Tätigkeitsberichte	Keine besondere Relevanz	N/A
Art. 60 - 67	Kooperation und Kohärenz	Keine besondere Relevanz	N/A
Art. 68 - 76	Europäischer Datenschutzausschuss	Keine besondere Relevanz	N/A
Art. 77	Recht auf Beschwerde bei einer Aufsichtsbehörde	Keine besondere Relevanz	N/A
Art. 78	Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	Keine besondere Relevanz	N/A
Art. 79 - 82	Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	Keine besondere Relevanz	N/A
Art. 83 - 84	Geldbußen und Sanktionen	Keine besondere Relevanz	N/A
Art. 85 - 91	Vorschriften für besondere Verarbeitungssituationen	Keine besondere Relevanz	N/A
Art. 92 - 93	Delegierte Rechtsakte und Durchführungsrechtsakte	Keine besondere Relevanz	N/A
Art. 94 - 99	Schlussbestimmungen	Keine besondere Relevanz	N/A