Wprowadzenie

Verizon Connect oferuje usługi mobilne zarządzania pracownikami w obszarze kierowania flotą (produkty Fleet Management) i świadczenia usług w terenie (produkty Field Service). Nasze produkty służą analizowaniu wydajności floty pojazdów, która może mieć duży wpływ na Państwa przedsiębiorstwo. Informują o tym, gdzie znajdują się Państwa pojazdy firmowe, jak ich kierowcy zachowują się na drodze i ile paliwa zużywają. Informacje te są następnie prezentowane w łatwo przyswajalnych tabelach, które pozwalają na podejmowanie szybkich działań. Reveal to bardzo przydatne narzędzie, które pomoże Państwu osiągnąć więcej w krótszym czasie, zapewnić lepszą obsługę klienta i, w dłuższej perspektywie, poprawić wyniki przedsiębiorstwa. Dzięki naszym produktom Field Service mamy również możliwość zarządzania pełnym cyklem życia zgłoszeń serwisowych naszych klientów, począwszy od pierwszego kontaktu z klientem, poprzez przygotowanie wyceny zlecenia, zaplanowanie pracy, wysłanie na miejsce pracownika, aż po ustalenie optymalnego przebiegu trasy kierowcy i przyjęcie płatności za wykonaną pracę.

Niniejszy eBook odpowiada na najczęściej zadawane pytania dotyczące usług Reveal („usługi" lub „Reveal") dostarczanych Państwu przez Verizon Connect za pośrednictwem platformy Reveal, a także przedstawia przegląd najważniejszych kwestii związanych z ochroną danych oraz wymogów, które należy spełnić przed, podczas oraz po skorzystaniu z usługi. Niniejszy podręcznik koncentruje się głównie na kwestiach ochrony danych, jednak należy rozważyć, czy wdrożenie i korzystanie z usług omawianych powyżej podlega także innym wymogom prawnym. Na przykład w niektórych państwach korzystanie z usług w pojazdach prowadzonych przez pracowników wywołuje określone skutki na gruncie prawa pracy.

W razie potrzeby, w treści znajdują się odniesienia do wytycznych organów dostępnych w chwili publikacji. Organy nadzorcze regularnie dokonują przeglądu i modyfikują swoje wytyczne, dlatego należy śledzić rozwój sytuacji w tym obszarze, ponieważ to Państwo, jako Administrator danych osobowych zbieranych i wykorzystywanych za pośrednictwem usługi, odpowiadają za przestrzeganie obowiązującego prawa.

Zawarte w niniejszym eBooku informacje nie mają charakteru porady prawnej lub innego specjalistycznego doradztwa. W razie potrzeby należy zasięgnąć porady odpowiednio wyspecjalizowanego prawnika. Verizon Connect nie odpowiada za informacje zawarte w niniejszym eBooku i wyłącza wszelką odpowiedzialność prawną za treść tych informacji.

Najczęściej zadawane pytania na temat usługi Reveal

1. Czyje informacje są zbierane za pośrednictwem usług?
Przede wszystkim zbierane będą informacje o pracownikach i współpracownikach, którzy korzystają z pojazdów objętych zakresem usług. Informacje mogą być również gromadzone na temat innych osób (np. pasażerów lub innych domowników kierowcy, które mają dostęp do pojazdu) w zależności od przyczyn i sposobów korzystania z usługi.

2. W jaki sposób gromadzone są informacje dla potrzeb usługi?
Usługa zbiera informacje z dwóch źródeł:

- Urządzenie pokładowe zainstalowane w Państwa pojazdach: Zbiera informacje na temat lokalizacji i aktywności pojazdów. Jeśli kierowca, do którego przypisany jest dany pojazd, jest znany lub możliwy do ustalenia, informacje na jego temat również stanowią dane osobowe.
- Na naszych platformach dostępnych jest kilka aplikacji mobilnych, które można zainstalować, aby efektywnie korzystać z naszych usług, np. aplikacje w obszarze pracy w terenie (Work, Workforce, Field) oraz aplikacje związane z zarządzaniem flotą (Manager\Spotlight, Video, ELD). Aby móc korzystać z aplikacji, każdy kierowca musi podczas rejestracji podać pewne informacje.

W niniejszym eBooku wszystkie dane osobowe zebrane za pośrednictwem usługi nazywamy zbiorczo „Danymi Osobowymi Reveal".

3. Jakie dane osobowe są gromadzone za pośrednictwem usługi?
Większość danych osobowych, które będą zbierane za pośrednictwem usługi, określają Państwo. Zakres

zbieranych informacji może się różnić w zależności od przyczyn i sposobów korzystania z rozwiązania. Mają Państwo pełną kontrolę nad rodzajami zbieranych danych. W związku z tym są Państwo prawnie zobowiązani do zapewnienia, że zbieranie danych osobowych jest konieczne w celu umożliwienia korzystania z usługi.
Dane osobowe zgromadzone za pośrednictwem urządzenia pokładowego pojazdu mogą obejmować:

- Dane dotyczące lokalizacji (GPS) pojazdów i osób;
- Informacje z tachografu (dane o czasie jazdy);
- Prędkość i zachowanie się kierowcy pojazdu;
- Dane dotyczące zdarzeń z udziałem pojazdów (np. uczestnictwo w wypadku drogowym, wjazd na teren określonej strefy geograficznej lub jej opuszczenie);
- Inne informacje o pojeździe (np. zużycie paliwa, ciśnienie w oponach, dane eksploatacyjne).

Dane osobowe zbierane za pośrednictwem aplikacji mogą obejmować:

- Imię i nazwisko kierowcy;
- Numer telefonu, adres e-mail i adres domowy kierowcy;
- Dane uwierzytelniające kierowców na potrzeby logowania;
- Zapisy dotyczące kierowców (np. przydzielenie pojazdu, numer kierowcy, określone strefy geograficzne);
- Geolokalizacja GPS.

4. Czy Reveal zbiera jakiejkolwiek "szczególne kategorie danych" lub dane dotyczące naruszeń prawa?
Zgodnie z przepisami o ochronie danych, szczególne kategorie danych obejmują dane osobowe dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, wyznania, członkostwa w związkach zawodowych, dane genetyczne, dane biometryczne (wykorzystywane do celów identyfikacji), informacje dotyczące zdrowia, seksualności i orientacji seksualnej. Podobnie jak w przypadku danych dotyczących naruszeń prawa, przetwarzanie szczególnych kategorii danych podlega dalej idącym ograniczeniom.

Za pośrednictwem usługi nie są zbierane żadne dane szczególnej kategorii ani dotyczące naruszeń prawa (np. kierowcy nie są proszeni o wprowadzanie do aplikacji żadnych informacji tego rodzaju). O ile pewne szczególne kategorie danych można wywnioskować na podstawie informacji o lokalizacji (np. dane z geolokalizacji mogą wskazywać, że kierowca rutynowo odwiedza dany ośrodek religijny lub zdrowotny), nie powoduje to powstania wymogów RODO w odniesieniu do przetwarzania szczególnych kategorii danych, chyba że informacje dotyczące lokalizacji są w rzeczywistości wykorzystywane do kompilowania wyżej wspomnianych szczególnych kategorii danych. Jednak w zależności od przyczyn i sposobów korzystania z usługi, (domniemane) dane dotyczące naruszeń prawa mogą być przetwarzane na podstawie zebranych informacji (np. informacje o aktywności pojazdu mogą wskazywać, że kierowca przekroczył ograniczenie prędkości).

Definicja naruszenia prawa różni się w zależności od państwa, podobnie jak uznanie informacji za „szczególne kategorie" danych lub dane dotyczące naruszeń prawa. W przypadku zbierania przez Państwa danych, które mogą być uznane za dane dotyczące naruszeń prawa, zgodnie z przepisami o ochronie danych podlegają Państwo dodatkowym obowiązkom wynikającym z prawa krajowego i postanowień RODO jako administrator tych danych osobowych.

5. Kto ma dostęp do Danych Osobowych Reveal?
Dane Osobowe Reveal przetwarzane w trakcie świadczenia usługi są udostępniane jedynie upoważnionym pracownikom Verizon na zasadzie „ograniczonego dostępu". Dane Osobowe Reveal są także udostępniane podmiotom zewnętrznym będącym dostawcami Verizon w celu umożliwienia Verizon administrowania usługą (np. osobom trzecim, które świadczą usługi hostingowe). Verizon może również ujawniać Dane Osobowe Reveal osobom trzecim, jeżeli jest to wymagane przepisami prawa (np. organom ścigania).

Oprócz przyczyn opisanych powyżej, mogą Państwo zdecydować się na ujawnienie Danych Osobowych Reveal dla własnych celów. Decydują Państwo o tym, kto w Państwa organizacji powinien mieć dostęp do Danych Osobowych Reveal (m. in. muszą Państwo wyznaczyć osoby uprawnione do dostępu do portalu online, aby móc przeglądać informacje o lokalizacji pojazdu i aktywności w czasie rzeczywistym). Mogą Państwo również zdecydować się na udostępnienie Danych Osobowych Reveal osobom trzecim, takim jak inne organizacje w ramach Państwa grupy kapitałowej lub dostawcy innych usług online (np. w przypadku, gdy inna platforma łączy się z usługą Reveal).

6. Czy Verizon przekazuje Dane Osobowe Reveal poza granice Europejskiego Obszaru Gospodarczego ("EOG")?
Firma Verizon przechowuje Dane Osobowe Reveal w centrach danych zlokalizowanych zarówno na terenie EOG, jak i poza jego granicami. Lista państw jest dostępna tutaj: https://www.verizon.com/about/privacy/data-processing-activities. W przypadku, gdy Verizon przekazuje dane osobowe poza terytorium EOG w ramach grupy Verizon, przekazywanie danych jest realizowane zgodnie z zatwierdzonymi przez UE wiążącymi regułami korporacyjnymi dla administratora i podmiotu przetwarzającego.

7. Jak długo Verizon przechowuje Dane Osobowe Reveal?
Dane Osobowe Reveal będą przechowywane tak długo, jak przewiduje umowa i zgodnie z ustawieniami przechowywania danych wybranymi przez Państwa podczas konfiguracji produktu. Różni się to w zależności od wymogów prawnych dotyczących przechowywania informacji lub Państwa wymagań w zakresie sprawozdawczości. Państwa obowiązkiem jako administratora jest ustalenie obowiązującego w Państwa przypadku okresu przechowywania Danych Osobowych Reveal. Po zakończeniu świadczenia usług Verizon Connect bezpiecznie usunie Dane Osobowe Reveal.

8. Czy firma Verizon wykorzystuje Dane Osobowe Reveal do własnych celów?
Dane Osobowe Reveal są gromadzone przez Verizon w celu świadczenia Państwu usługi Reveal na Państwa żądanie. W powyższym zakresie Verizon jest podmiotem przetwarzającym dane osobowe.

W zakresie dozwolonym przepisami prawa Verizon wykorzystuje w pewnym stopniu zanonimizowane informacje zebrane za pośrednictwem usługi Reveal do własnych celów oraz w celu usprawnienia dostarczanych przez siebie produktów i usług. Powyższe obejmuje prowadzenie analiz w celu optymalizacji usługi Reveal oraz ujawnianie informacji towarzystwom ubezpieczeniowym. Na podstawie zanonimizowanych informacji nie jest możliwe zidentyfikowanie jakichkolwiek osób lub organizacji.

9. W jaki sposób firma Verizon zapewnia bezpieczeństwo Danych Osobowych Reveal?
Prosimy zapoznać się z dokumentem Verizon Internal Systems Information Security Exhibit, który zawiera opis technicznych i organizacyjnych środków bezpieczeństwa, które Verizon stosuje w celu wykonania swoich zobowiązań wynikających z RODO, znajdującym się na stronie internetowej *https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit*

Wymogi w zakresie ochrony danych

W tym rozdziale wyjaśniono, w jaki sposób wymagania dotyczące ochrony danych mają zastosowanie do korzystania z usługi Reveal.

Na końcu tej części dokumentu znajduje się lista kontrolna właściwych artykułów RODO oraz odniesienie do fragmentów niniejszego eBooka, w których są one powołane. Pozwoli to na sprawdzenie, czy dany przepis RODO ma zastosowanie do Reveal, oraz w której części niniejszego eBooka został omówiony. Zamieściliśmy również listę źródeł, z których można uzyskać dodatkowe informacje.

A. Ocena skutków dla ochrony danych

Ocena skutków dla ochrony danych („DPIA") jest procesem mającym na celu opisanie i dokonanie oceny przetwarzania danych osobowych oraz identyfikację i zarządzenie ryzykiem, jakie przetwarzanie danych niesie dla osób fizycznych.

Organy nadzorujące ochronę danych osobowych zgodnie stoją na stanowisku, że DPIA musi być przeprowadzane, gdy organizacja przetwarza dane osobowe w celu oceny efektów pracy, lokalizacji lub przemieszczania się pracowników[1]. Jest prawdopodobne, że korzystanie przez Państwa z usługi będzie

[1] WP29 *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679* (WP248), s. 10

wymagało przeprowadzenia DPIA, ale każdy organ nadzorczy podaje do wiadomości własne kryteria w tym zakresie. Należy zapoznać się z kryteriami właściwego organu nadzorczego w celu ustalenia, czy wymagane jest DPIA.

Państwa DPIA powinno:

- Określać, jakie przetwarzanie Danych Osobowych Reveal będzie miało miejsce;
    - Informacje zawarte w niniejszym e-Booku na temat tego, jakie dane są gromadzone, w jaki sposób są one gromadzone i w jaki sposób są przetwarzane, powinny okazać się pomocne w tym zakresie.
- Określać cele przetwarzania - a jeśli podstawą prawną korzystania z usługi jest to, że przetwarzanie jest niezbędne do celu, który leży w Państwa uzasadnionym interesie - jaki jest ten interes.
- Oceniać, czy przetwarzanie danych jest niezbędnym i proporcjonalnym sposobem osiągnięcia wyżej wspomnianych celów;
    - Oznacza to rozważenie, czy możliwe jest osiągnięcie celu w inny sposób, który wiąże się z przetwarzaniem danych osobowych w mniejszym zakresie.
    - Na przykład, jeśli firma chce śledzić godziny przepracowane przez daną osobę, to czy można to osiągnąć inaczej, niż poprzez śledzenie jej miejsca pobytu przez cały czas pracy, co byłoby oczywiście nieproporcjonalne.
- Oceniać zagrożenia dla osób fizycznych, jakie stwarza przetwarzanie danych, i w jaki sposób można im zaradzić;
    - Na przykład jeżeli pracownik może używać pojazdu do użytku prywatnego, to śledzenie pojazdu w czasie, gdy pracownik nie pracuje, byłoby uciążliwe i niepotrzebne z punktu widzenia pracodawcy. Ryzyko to można złagodzić umożliwiając pracownikowi wyłączenie usługi poza godzinami pracy poprzez uruchomienie „Privacy Switch" („Funkcji Prywatności") i zapewnienie, że pracownicy są świadomi możliwości jej użycia.
- Opisywać środki bezpieczeństwa; oraz
- Opisywać inne środki stosowane w celu zapewnienia ochrony danych osobowych i wykazania zgodności z obowiązującymi wymogami.
    - DPIA powinno ponadto odnosić się do innych zagadnień wymienionych w niniejszym eBooku.
    - W szczególności DPIA powinno określać w jaki sposób realizowane są prawa osób, których dane dotyczą.

Dokonując DPIA należy postępować w porozumieniu z inspektorem ochrony danych osobowych (o ile został przez Państwa powołany). W razie potrzeby należy również porozumieć się z osobami, których dane będą przetwarzane, lub z ich przedstawicielami - np. poprzez konsultacje z pracownikami, związkami zawodowymi lub radami zakładowymi - a następnie uwzględnić wyniki tych konsultacji w DPIA.

Jeśli DPIA wykaże, że wykorzystanie danych osobowych do planowanych celów wiąże się z wysokim i niemożliwym do zminimalizowania ryzykiem dla osób fizycznych, należy skonsultować się z właściwym organem nadzorczym (w Wielkiej Brytanii jest to Information Commissioner's Office).

Każde DPIA należy poddawać okresowemu przeglądowi. Ponadto konieczne jest okresowe badanie sposobu korzystania usługi z punktu widzenia wykorzystania Danych Osobowych Reveal w kontekście DPIA.

B. Informacje o ochronie prywatności

Podobnie jak w przypadku wszystkich operacji przetwarzania danych osobowych, są Państwo zobowiązani zapewnić osobom fizycznym jasne i wyczerpujące informacje na temat gromadzenia i wykorzystywania przez Państwa Danych Osobowych Reveal.

W niniejszej części opisano treści, które należy zawrzeć w informacji o ochronie prywatności, aby spełnić obowiązujące wymogi prawne w zakresie ochrony danych osobowych. Należy jednak rozważyć, czy treść informacji o ochronie prywatności i sposób wdrożenia usługi podlega jakimkolwiek innym przepisom prawnym. Na przykład w niektórych państwach prawo pracy wymaga zamieszczenia w treści informacji o ochronie prywatności lub innych dokumentach wewnętrznych przedsiębiorstwa pewnych dodatkowych

informacji.
Postanowienia RODO przewidują, że w informacji o ochronie prywatności powinny znaleźć się następujące informacje:

- Państwa tożsamość i dane kontaktowe (oraz dane kontaktowe inspektora ochrony danych osobowych, jeśli został powołany);
- Cele i podstawy prawne przetwarzania (oraz, w przypadku przetwarzania danych osobowych w celu, który leży w „prawnie uzasadnionym interesie", określenie tego interesu);
    - Pomogą w tym Państwu informacje zawarte w części niniejszego eBooka poświęconej celom i podstawom prawnym.
- Kategorie przetwarzanych Danych Osobowych Reveal (a także ich źródła), jeżeli nie zostały uzyskane bezpośrednio od osoby fizycznej;
    - Pomoże w tym Państwu rozdział 3: „Dane osobowe są zbierane za pośrednictwem usługi".
- Odbiorcy Danych Osobowych Reveal oraz wszystkie państwa nienależące do EOG, do których przekazywane są Dane Osobowe Reveal (wraz ze szczegółowymi informacjami na temat obowiązujących na ich terytorium zabezpieczeń);
- Okres przechowywania Danych Osobowych Reveal;
- Czy ujawnianie Danych Osobowych Reveal jest obowiązkowe, a także jakie są możliwe konsekwencje odmowy ich ujawnienia;
- Istnienie zautomatyzowanego podejmowania decyzji (w tym profilowania), oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
- Określenie praw osób, których dane dotyczą (w tym prawa do wycofania zgody, jeśli przetwarzają Państwo dane osobowe na podstawie zgody udzielonej przez osobę fizyczną) oraz możliwości złożenia skargi do organu nadzorczego.

Informacja o ochronie prywatności musi również spełniać dodatkowe wymogi określone w art. 12 RODO (np. informacje przekazywane osobom fizycznym muszą być zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne oraz wyrażone jasnym i prostym językiem).

Osoby korzystające z usługi na terytorium Francji
Poza wymienionymi powyżej wymogami RODO, francuska ustawa o ochronie danych osobowych nakłada na Państwa obowiązek poinformowania osób fizycznych o ich prawie do określenia wytycznych dotyczących wykorzystania ich danych osobowych po ich śmierci.

Informacje dostępne w pojeździe

Biorąc pod uwagę fakt, że zbieranie Danych Osobowych Reveal jest mniej widocznym rodzajem zbierania danych dla osób fizycznych, a jednocześnie może mieć dla nich istotne konsekwencje, należy dołożyć szczególnych starań, aby zwrócić uwagę kierowców na korzystanie z usługi. Oprócz wyczerpującej informacji o ochronie prywatności opisanej powyżej, wymogi prawne przewidują, że są Państwo dodatkowo zobowiązani wyraźnie informować kierowców, że w pojeździe zainstalowano urządzenie śledzące pojazd, który prowadzą, a także że trasa (oraz zachowanie na drodze, o ile zastosowana technologia na to pozwala) jest monitorowana. Najlepiej byłoby, gdyby informacje te były umieszczone w widocznym miejscu w każdym pojeździe, w polu widzenia kierowcy[2]

Osoby korzystające z usługi na terytorium Polski
Oprócz treści wymienionych powyżej, w przypadku, gdy wdrożenie usługi jest równoznaczne z monitorowaniem pracowników, informacja znajdująca się w pojeździe musi uwzględniać ponadto:

- Informację o tym, jakie dane są gromadzone i rejestrowane;
- Gdzie i jak długo te dane są przechowywane; oraz
- Kto ma dostęp do tych danych[3].

Egzekwowanie polityki

[2] WP29 *Opinia 2/2017 w sprawie przetwarzania danych w miejscu pracy* (WP249), s. 20

[3] (polski) Urząd Ochrony Danych Osobowych, *Ochrona danych w miejscu pracy. Wytyczne dla pracodawców,* s. 37

W przypadku wykorzystywania Danych Osobowych Reveal do egzekwowania obowiązujących u Państwa zasad i standardów, należy upewnić się, że jest to zgodne z prawem, a pracownicy wiedzą, jakie są odpowiednie zasady i mają świadomość monitorowania zgodności z nimi za pomocą usługi.

C. Rejestr czynności przetwarzania

Jako administrator danych są Państwo zobowiązani prowadzić Rejestr Czynności Przetwarzania („RPA") określony w art. 30 RODO. Będą Państwo odpowiedzialni za zapewnienie, że przetwarzanie Danych Osobowych Reveal jest objęte zakresem Państwa RPA. Konieczne będzie uwzględnienie następujących informacji:

- Nazwa i dane kontaktowe organizacji (oraz, w stosownych przypadkach, nazwisko/nazwę i dane kontaktowe inspektora ochrony danych, przedstawiciela i/lub współadministratora);
- Cel, dla którego wykorzystują Państwo Dane Osobowe Reveal;
- Opis kategorii Danych Osobowych Reveal oraz kategorii osób, których dane są przetwarzane;
    - Pomoże w tym Państwu rozdział 3: „Jakie dane osobowe są zbierane za pośrednictwem usługi?".
- Kategorie odbiorców, którym przekazywane są Dane Osobowe Reveal;
    - W tym przypadku pomocny okaże się rozdział 5: "Kto ma dostęp do Danych Osobowych Reveal?". Należy również wymienić odbiorców, którym udzielają Państwo dostępu do Danych Osobowych Reveal
- Przekazywanie danych osobowych do krajów spoza terytorium EOG;
    - Rozdział 6: „Czy Verizon przekazuje dane osobowe poza terytorium EOG?" wyjaśnia, gdzie dane są przekazywane i jakie zabezpieczenia są stosowane w celu ochrony Danych Osobowych Reveal
- Ograniczenia czasowe;
    - Rozdział 7: „Jak długo Verizon przechowuje Dane Osobowe Reveal" wyjaśnia tę kwestię.
- Informacje o środkach bezpieczeństwa, w miarę możliwości.
    - Opis technicznych i organizacyjnych środków bezpieczeństwa, które Verizon wdraża w celu wypełnienia swoich zobowiązań wynikających z RODO: https://www.verizon.com/about/privacy/verizon-internal-systems-information-security-exhibit

Firma Verizon posiada informacje, które mogą pomóc Państwu w wywiązaniu się z tego obowiązku, dostępne pod adresem https://www.verizon.com/about/privacy/data-processing-activities

Osoby korzystające z usługi na terytorium Zjednoczonego Królestwa
Jeśli przetwarzają Państwo dane dotyczące naruszeń prawa, a podstawy przetwarzania, na które się Państwo powołują, obejmują jeden z warunków określonych w załączniku 1 do Data Protection Act 2018, są Państwo zobowiązani do uwzględnienia w RPA dodatkowych rubryk (dotyczących podstaw i warunków przetwarzania oraz przechowywani/usuwania odpowiednich danych zgodnie z Państwa polityką - jeśli są wymagane).

D. Cele

Konieczne będzie określenie celu (celów), dla których zamierzają Państwo korzystać z usługi i wykorzystywać Dane Osobowe Reveal, np.:

- Wykrywanie i zapobieganie stratom mienia przedsiębiorstwa;
- Poprawa wydajności pracowników;
- Optymalizacja tras i zasobów oraz oszczędność paliwa;
- Dostarczanie klientom informacji na temat lokalizacji pojazdów w czasie rzeczywistym;
- Zapewnienie bezpieczeństwa i ochrony pracowników, np. poprzez zapewnienie korzystania z przerw na odpoczynek i posiłki.

Świadomość celów, dla których usługa jest wdrażana od samego początku jest kwestią o znaczeniu kluczowym.

- Potrzebują Państwo „podstawy prawnej" dla każdego odrębnego celu, dla którego przetwarzane są dane osobowe;

- Należy upewnić się, że nie przetwarzają Państwo większej ilości Danych Osobowych Reveal, niż jest to rozsądnie niezbędne do osiągnięcia danego celu;
- Ponadto należy poinformować osoby fizyczne o celach przetwarzania.

Po zebraniu Danych Osobowych Reveal do wspomnianych celów, mogą Państwo je wykorzystywać wyłącznie do wyżej wspomnianych celów lub do innych celów, które są zgodne z tymi celami. W pewnych przypadkach obowiązujące prawo dopuszcza wyjątki od tej zasady.

Osoby korzystające z usługi na terytorium Francji

Urządzenia geolokalizacyjne mogą być instalowane wyłącznie w pojazdach wykorzystywanych przez pracowników do następujących celów[4]:

- Śledzenie, uzasadnianie i fakturowanie usług transportu pasażerskiego;
- Zapewnienie bezpieczeństwa i ochrony pracowników, towarów i pojazdów (w szczególności lokalizowanie skradzionych pojazdów);
- Optymalizacja alokacji zasobów w przypadku świadczenia usług na rozległym obszarze geograficznym, w szczególności w odniesieniu do służb ratowniczych;
- Śledzenie czasu pracy (wyłącznie w przypadkach, gdy nie ma innych możliwości śledzenia czasu pracy);
- Przestrzeganie obowiązków prawnych lub regulacyjnych;
- Zapewnienie przestrzegania przepisów pracodawcy dotyczących korzystania z pojazdów służbowych.

I odwrotnie, wykorzystywanie urządzeń do geolokalizacji zainstalowanych w pojazdach służbowych jest zabronione[5]:

- Do monitorowania przestrzegania ograniczeń prędkości;
- Do stałego śledzenia pracowników;
- Do śledzenia czasu pracy, w przypadku gdy dostępne są inne możliwości w tym zakresie;
- W pojeździe pracownika, którego stanowisko służbowe przewiduje swobodę działania (np. przedstawiciela handlowego);
- Do dozwolonego śledzenia prywatnego wykorzystania pojazdu (np. podczas przerw lub przez pracowników, którzy są uprawnieni do samodzielnego planowania swoich przejazdów); a także
- Do śledzenia przedstawicieli związków zawodowych lub podobnych osób działających w ramach pełnionych przez siebie funkcji.

Osoby korzystające z usługi na terytorium Niemiec

Korzystanie z systemów śledzenia, za pomocą których pracownicy mogą być stale monitorowani, jest co do zasady niedozwolone.[6]

Osoby korzystające z usługi na terytorium Polski

O ile wdrożenie usługi może być uznane za monitorowanie pracowników oraz w zakresie, w jakim ma to miejsce, organizacje mogą przetwarzać Dane Osobowe Reveal w celu „zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy". Polski organ nadzorczy sugeruje, że wyżej wspomniany cel przetwarzania jest dość szeroki i może pozwolić na:

- Lokalizowanie pojazdu w przypadku kradzieży;
- Ustalenie odpowiedzialności pracownika za uszkodzenie pojazdu; lub
- Optymalizację tras i zasobów oraz zapewnienie oszczędności paliwa.

Osoby korzystające z usługi na terytorium Portugalii

Usługi nie mogą być wykorzystywane do monitorowania zachowań pracowników i mogą być wykorzystywane

[4] Wytyczne CNIL w sprawie geolokalizacji pojazdów służbowych, 2018 r

[5] Wytyczne CNIL w sprawie geolokalizacji pojazdów służbowych, 2018 r

[6] Komisarz ds. ochrony danych i swobodnego przepływu informacji w Nadrenii-Palatynacie, *„W sprawie legalności śledzenia pracowników przez GPS"*; Komisarz ds. ochrony danych i swobodnego przepływu informacji w Badenii-Wirtembergii, *„Ochrona danych dotyczących pracowników"*, 2018, s. 36-37

wyłącznie w pojazdach wykorzystywanych przez pracowników do następujących dozwolonych celów[7]:

- **Zarządzanie flotą w przypadku korzystania z usług zewnętrznych dostawców:**
  - Usługi pomocy technicznej;
  - Dystrybucja towarów;
  - Transport pasażerski;
  - Przewóz towarów; oraz
  - Prywatne usługi w zakresie ochrony.

- **Ochrona towarów:**
  - Transport materiałów niebezpiecznych; oraz
  - Transport towarów wartościowych.

W przypadku wykorzystywania usług w celu zlokalizowania pojazdów prowadzonych przez pracowników w razie kradzieży, pracodawca może uzyskać dostęp do zebranych danych geolokalizacyjnych dopiero wtedy, gdy pojazd został skradziony. Inne dane dotyczące pojazdu (takie jak średnia prędkość, hamowanie, zużycie paliwa) mogą być gromadzone, ale tylko w taki sposób, aby nie były powiązane z żadnymi danymi osobowymi, które umożliwiają identyfikację kierowcy.

E. Ważne podstawy prawne

Konieczne będzie określenie podstawy prawnej na mocy art. 6 RODO dla każdego celu, dla którego będą Państwo wykorzystywać Dane Osobowe Reveal. W zależności od danej sytuacji mogą Państwo wykorzystywać Dane Osobowe Reveal gdy jest to niezbędne do:

- **Wywiązania się z obowiązku prawnego:** na przykład w przypadku, gdy są Państwo zobowiązani do kontrolowania czasu użytkowania/ruchu pojazdów poprzez zamontowanie w pojeździe tachografu;
- **Wykonania umowy zawartej z osobą, której dane dotyczą**: na przykład, gdy dobra jazda jest warunkiem zatrudnienia;
- **Osiągnięcia celu, który leży w Państwa prawnie uzasadnionym interesie:** na przykład zapewnienie bezpieczeństwa kierowców (i innych użytkowników dróg), egzekwowanie dobrych nawyków kierowców, monitorowanie floty, oszczędność kosztów paliwa i serwisu, ochrona przed wypadkami i fałszywymi oskarżeniami, zapewnienie zdrowia i bezpieczeństwa pracowników oraz pomoc i wsparcie w zakresie składek ubezpieczeniowych.

Należy koniecznie zapewnić, że posiadają Państwo ważną podstawę prawną do przetwarzania danych i mogą Państwo, w razie potrzeby, uzasadnić istnienie wspomnianej podstawy wobec organu nadzorującego ochronę danych.

Należy wykazać, że przetwarzanie Danych Osobowych Reveal jest „niezbędne". „Niezbędne" oznacza, że przetwarzanie Danych Osobowych Reveal musi być ukierunkowanym i proporcjonalnym sposobem osiągnięcia celu; przetwarzanie musi być "bardziej niż pożądane, ale mniej niż nieodzowne lub absolutnie konieczne"[8]. Państwa ocena powinna być oparta na faktach i uwzględniać charakter realizowanego celu i mniej inwazyjne możliwości jego osiągnięcia. Jeżeli istnieją realistyczne, mniej inwazyjne alternatywy, wówczas przetwarzanie nie może być uznane za „niezbędne".[9]

Jeżeli powołują się Państwo na prawnie uzasadniony interes, są Państwo zobowiązani przeprowadzić i udokumentować tzw. „równowagi interesów", który ma za zadanie wykazać, czy interesy, prawa i wolności osób fizycznych są nadrzędne w stosunku do Państwa uzasadnionego interesu. Przetwarzanie powinno być niezbędne do osiągnięcia założonego celu (tj. proporcjonalne do potrzeb przedsiębiorstwa), przy czym należy

[7] Wytyczne CNPD i kodeksu pracy

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

[9] Europejska Rada Ochrony Danych (EDPB), *Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na mocy artykułu 6 ust. 1 lit. b) RODO w kontekście świadczenia usług internetowych osobom, których dane dotyczą, przyjęte w dniu 9 kwietnia 2019 r.*, s. 7

uwzględnić odpowiednie zabezpieczenia w celu ochrony prawa do prywatności po stronie osób fizycznych. Jeśli interesy osób fizycznych są nadrzędne w stosunku do Państwa interesów, przetwarzanie danych nie powinno być kontynuowane.

***Zgoda*:** Są Państwo uprawnieni do przetwarzania Danych osobowych, jeżeli osoba, której dane dotyczą, wyraziła na to zgodę. Jednakże zgoda jest ważna tylko wtedy, gdy jest udzielona dobrowolnie. Osoby fizyczne muszą mieć również możliwość wycofania udzielonej zgody bez jakichkolwiek negatywnych konsekwencji. Utrudnia to uzyskanie ważnej zgody na przetwarzanie danych w sprawach pracowniczych[10]
Wiele organów nadzorujących ochronę danych wyraża zastrzeżenia na temat podstaw prawnych przetwarzania w kontekście telematyki. Na przykład:

- W Wielkiej Brytanii i w Polsce, gdzie prywatne użytkowanie pojazdu jest dozwolone, monitorowanie ruchu pojazdów używanych prywatnie, bez dobrowolnie udzielonej zgody użytkownika, rzadko będzie uznane za uzasadnione[11]
- W Portugalii zgoda nie stanowi ważnej podstawy prawnej przetwarzania danych pochodzących z geolokalizacji[12]
- Urządzenia lokalizacyjne w pojazdach nie powinny być traktowane jako urządzenia służące do śledzenia lub monitorowania zachowania lub miejsca pobytu kierowców lub innego personelu, na przykład poprzez wysyłanie ostrzeżeń dotyczących prędkości pojazdu[13]
- Przetwarzanie danych dotyczących lokalizacji może być uzasadnione w przypadku, gdy odbywa się to w ramach monitorowania transportu osób lub towarów, poprawy dystrybucji zasobów lub w celu zapewnienia bezpieczeństwa pracowników, pojazdu lub przewożonych towarów, ale może być uznane za nadmierne w przypadku, gdy pracownicy mogą dowolnie organizować swoje podróże, lub gdy odbywa się to wyłącznie w celu monitorowania pracy pracownika, którą można kontrolować za pomocą innych środków[14]
  Wysyłanie klientowi nadmiernych informacji na temat kierowcy dostarczającego towar zamówiony przez klienta, np. zdjęcia paszportowego (oprócz nazwiska i lokalizacji kierowcy) w celu umożliwienia klientowi zweryfikowania tożsamości kierowcy dostarczającego towar po dotarciu na miejsce prawdopodobnie nie będzie uznane za uzasadnione ważną podstawą prawną (o ile można uznać „uzasadniony interes" w kontekście zdjęcia do celów identyfikacyjnych, byłoby to uznane za nieproporcjonalne w kontekście rezultatu testu równowagi interesów).[15]

Dane dotyczące naruszeń prawa

Jeśli przetwarzane przez Państwa Dane Osobowe Reveal zawierają dane dotyczące naruszeń prawa (w świetle lokalnie obowiązującego prawa i interpretacji pojęcia „naruszenie prawa"), wówczas art. 10 RODO ogranicza przetwarzanie tych danych osobowych. Dane dotyczące naruszeń prawa mogą być przetwarzane tylko wtedy, gdy przetwarzanie odbywa się pod nadzorem „władz publicznych" lub gdy przetwarzanie jest dozwolone prawem UE lub prawem krajowym. Dlatego też konieczne jest zapoznanie się z lokalnymi przepisami w celu określenia odpowiednich wymogów, na przykład:

Osoby korzystające z usługi na terytorium Francji
Zgodnie z francuską ustawą o ochronie danych osobowych, gromadzenie danych osobowych dotyczących

[10] Na przykład zgoda pracowników zwykle nie jest uznawana za ważną w Niemczech (Komisarz ds. ochrony danych i swobodnego przepływu informacji (LDi) NRW, 24 *Sprawozdanie na temat ochrony danych i* swobodnego przepływu *informacji 2017-2018*, s. 65, 66), a ponadto zgoda nie stanowi ważnej podstawy prawnej przetwarzania danych osobowych w sprawach pracowniczych w Portugalii (wytyczne CNPD w sprawie stosowania opłat geolokalizacyjnych w kontekście zatrudnienia i ścisłej interpretacji przepisów kodeksu pracy)

[11] Biuro Komisarza ds. Informacji *Kodeks praktyk pracowniczych*, s. 76; (polski) Urząd Ochrony Danych Osobowych, *Ochrona danych w miejscu pracy - wytyczne dla pracodawców,* s. 38

[12] Wytyczne CNPD dotyczące stosowania opłat geolokalizacyjnych w kontekście zatrudnienia i ścisłej interpretacji przepisów kodeksu pracy

[13] WP29 *Opinia 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych*

[14] WP29 *opinia 5/2005 w sprawie wykorzystania danych dotyczących lokalizacji w celu świadczenia usług tworzących wartość dodaną*

[15] WP29 *Opinia 2/2017 w sprawie przetwarzania danych w miejscu pracy*

zachowania osoby, które może być lub może zostać zaklasyfikowane jako naruszenie prawa lub przestępstwo, jest zabronione. W związku z tym zabronione jest zbieranie informacji o przekroczeniu przez daną osobę ograniczenia prędkości lub informacji dotyczących zachowania osoby, które mogą ujawnić naruszenie przepisów ruchu drogowego.

Osoby korzystające z usługi na terytorium Niemiec

Zgodnie z aktualną stanowiskiem obowiązującym w Niemczech normalne przetwarzanie Danych Osobowych Reveal nie stanowi przetwarzania danych dotyczących naruszeń prawa. Korzystanie z usług specjalnie w celu wykrywania naruszeń prawa byłoby jednak ograniczone przez ust. 26 (1) BDSG (na przykład jeżeli ruch pojazdów jest monitorowany w celu wykrywania kradzieży, oszustw lub handlu narkotykami przez pracowników - należy zauważyć, że wykroczenia związane z przekroczeniem prędkości nie są w tym kontekście uznawane za naruszenia prawa). Nie byłby to przypadek "normalnego" wykorzystania Danych Osobowych Reveal, a zatem prawdopodobne jest, że przetwarzanie danych w tym celu będzie miało miejsce jedynie w nadzwyczajnych sytuacjach (np. gdy pracodawca bada przypadki podejrzenia, że pracownik dopuścił się naruszenia prawa), natomiast w przypadku faktycznego korzystania z usług w tym celu należy zapoznać się z postanowieniami ust. 26(1) BDSG.

Osoby korzystające z usługi na terytorium Włoch

Ogólnie rzecz biorąc, przetwarzanie Danych Osobowych Reveal nie stanowi przetwarzania danych dotyczących naruszeń prawa (z wyjątkiem wykroczeń, które podlegałyby administracyjnej karze pieniężnej). Należy jednak sprawdzić, czy zmiany w przepisach prawa miejscowego nie wprowadzają żadnych nowych kategorii czynów zabronionych, w kontekście których Dane Osobowe Reveal mogą mieć istotne znaczenie.

Osoby korzystające z usługi na terytorium Polski

W odniesieniu do przetwarzania informacji o czynach zabronionych w kontekście pracowników na podstawie Kodeksu Pracy z 1974 r. obowiązują pewne szczególne wymagania, a mianowicie nie można powoływać się na zgodę pracownika na przetwarzanie jego danych osobowych w formie informacji o czynach zabronionych. Wymagana jest w tym przypadku inna, podstawa prawna przetwarzania, najprawdopodobniej przetwarzanie informacji w celu wywiązania się z obowiązku prawnego lub w celu ustalenia, dochodzenia lub obrony roszczeń.

Osoby korzystające z usługi na terytorium Portugalii

Przetwarzanie danych o czynach zabronionych w celu zapobiegania takim czynom lub ich wykrywania (np. możliwość popełniania wykroczeń związanych z nadmierną prędkością lub innych wykroczeń drogowych) jest dozwolone w pewnych okolicznościach, a także w przypadkach, gdy jest to konieczne dla celów lub w związku z postępowaniem sądowym, poradą prawną, lub gdy jest to konieczne do ustalenia, dochodzenia lub obrony praw. Jednakże dane osobowe muszą być poddane pseudonimizacji w ciągu siedmiu dni od ich zebrania.

Osoby korzystające z usługi na terytorium Hiszpanii

Ogólnie rzecz biorąc, przetwarzanie Danych Osobowych Reveal nie stanowi przetwarzania danych dotyczących naruszeń prawa w rozumieniu prawa hiszpańskiego (a jedynie przetwarzanie informacji na temat wykroczenia drogowego). Należy jednak sprawdzać, czy jakiekolwiek zmiany w przepisach prawa miejscowego nie wprowadzają żadnych kategorii czynów zabronionych, dla których Dane Osobowe Reveal mogą mieć znaczenie, ponieważ przetwarzanie danych dotyczących naruszeń prawa jest w Hiszpanii ograniczone - jedynymi (potencjalnie) istotnymi okolicznościami, w których przetwarzanie dotyczących naruszeń prawa może mieć miejsce w tym kontekście są (i) cel polegający na zapobieganiu, prowadzeniu dochodzenia, wykrywaniu lub ściganiu przestępstw, (ii) przetwarzanie jest objęte przepisem o mocy ustawowej lub jest przewidziane przepisami prawa UE.

Osoby korzystające z usługi na terytorium Zjednoczonego Królestwa

W Zjednoczonym Królestwie należy zapewnić, że oprócz podstawy prawnej spełniono warunek przetwarzania danych wynikający z art. 9 RODO lub załącznika 1 do Data Protection Act 2018. Na przykład w odniesieniu do danych dotyczących naruszeń prawa, Data Protection Act 2018 pozwala na przetwarzanie danych osobowych w celu zapobiegania lub wykrywania naruszeń prawa (takiego jak, potencjalnie, popełnienie wykroczenia polegającego na przekroczeniu dozwolonej prędkości lub innego wykroczenia drogowego) w pewnych okolicznościach oraz w przypadkach, gdy jest to konieczne dla celów lub w związku z postępowaniem sądowym, poradą prawną lub ustaleniem, dochodzeniem lub obroną praw.

F Minimalizacja danych

Należy zapewnić, że wykorzystują Państwo tylko takie dane osobowe, które są adekwatne, stosowne i ograniczone do tego, co jest niezbędne (w świetle Państwa celów). Oznacza to, że należy zidentyfikować i wykorzystać minimalną możliwą ilość Danych Osobowych Reveal, jaka jest niezbędna do osiągnięcia założonych celów.

W przypadku, gdy umożliwiają Państwo swoim pracownikom korzystanie z pojazdów dla celów prywatnych, zazwyczaj nie ma potrzeby zbierania informacji o tym, dokąd nim jeżdżą poza godzinami pracy. Usługa posiada funkcję zapewniającą, że pracownicy nie są monitorowani poza godzinami pracy. Jest to „Privacy Switch" („Funkcja Prywatności"), która stanowi prosty i opłacalny sposób zapewnienia zgodności z obowiązującymi przepisami. W niektórych krajach (takich jak Francja, Niemcy i Portugalia) udostępnienie pracownikom „Privacy Switch" („Funkcji Prywatności") jest wymagane na mocy wytycznych regulacyjnych[16]

G. Prawidłowość danych

Należy zapewnić, że wykorzystywane przez Państwa Dane Osobowe Reveal nie są nieprawidłowe i nie wprowadzają w błąd. W kontekście Danych Osobowych Reveal szczególnie ważne jest podjęcie kroków w celu zapewnienia prawidłowości danych osobowych (np. zapewnienie, że rejestry pojazdów przydzielonych pracownikom są prowadzone poprawnie) oraz rozważenie wszelkich możliwych problemów związanych z prawidłowością danych osobowych (np. w przypadku zakwestionowania przez kierowcę swojej lokalizacji w danym momencie).

H. Zatrzymywanie Danych Osobowych Reveal

Dane Osobowe Reveal powinny być przechowywane tylko przez okres, jaki jest potrzebny do osiągnięcia założonego celu. Należy przeanalizować istnienie wszelkich dodatkowych wymogów prawnych dotyczących dalszego przechowywania danych (np. w związku z archiwizowaniem ewidencji czasu pracy). Powyższe kwestie należy uwzględnić w polityce przechowywania danych.

I. Bezpieczeństwo danych osobowych Reveal

Zgodnie z art. 32 RODO należy wdrożyć "odpowiednie środki techniczne i organizacyjne" w celu zapewnienia poufności, integralności i dostępności Danych Osobowych Reveal. W celu zidentyfikowania konkretnych zagadnień związanych z wdrożeniem usług Reveal oraz wykorzystaniem Danych Osobowych Reveal, można skorzystać z oceny ryzyka, co pozwoli na określenie "odpowiedniego" poziomu bezpieczeństwa (uwzględniając stan wiedzy technicznej, koszt wdrażania). Po wdrożeniu, należy regularnie sprawdzać techniczne i organizacyjne środki w celu zapewnienia ich odpowiedniości. W przypadku udostępniania Danych Osobowych Reveal innym organizacjom, działającym w Państwa imieniu jako podmiot przetwarzający, należy zapewnić, że podmiot przetwarzający zapewnia również wystarczające gwarancje (na mocy zwartych umów) wdrożenia technicznych i organizacyjnych środków ochrony danych.

W przypadku naruszenia bezpieczeństwa dotyczącego danych osobowych, należy postępować zgodnie z art. 33 i art. 34 RODO. Zawiadomienie o naruszeniu otrzymacie Państwo od nas bez zbędnej zwłoki. W takim przypadku, stosownie do wymogów, należy powiadomić właściwe organy nadzorcze, w ciągu co najwyżej 72 godzin od momentu uzyskania informacji o zdarzeniu (chyba że uznacie Państwo, że nie może ono stanowić zagrożenia dla praw i wolności osób fizycznych). W przypadku, gdy naruszenie może skutkować wysokim ryzykiem naruszenia praw i wolności osób fizycznych, należy bez zbędnej zwłoki powiadomić osoby fizyczne, których naruszenie dotyczy. Należy rozważyć, w jaki sposób będziecie Państwa identyfikować powstanie naruszenia dotyczącego Danych Osobowych Reveal, jakie kroki zostaną przez Państwa podjęte w celu wyeliminowania naruszenia, a także jak powiadomić właściwe osoby o naruszeniu i ocenić naruszenie w celu stwierdzenia czy w związku z nim wymagane będzie powiadomienie.

[16]Bawarski komisarz ds. ochrony danych osobowych, 27. sprawozdanie z działalności za rok 2016, s. 241; Wytyczne CNIL w sprawie geolokalizacji pojazdów służbowych, 2018; Narada CNPD 7680/2014

Osoby korzystające z usługi na terytorium Francji
Zgodnie z wytycznymi CNIL w sprawie geolokalizacji pojazdów pracowników[17], wdrożyć należy, przede wszystkim:

- politykę udzielania dostępu;
- środki zapewniające bezpieczne przekazywanie danych; oraz
- rejestr dostępu do danych i operacji przetwarzania.

Osoby korzystające z usługi na terytorium Hiszpanii
W przypadku sprostowania lub usunięcia danych osobowych, hiszpańska ustawa o ochronie danych wymaga aby administratorzy 'blokowali" dane w ramach środków technicznych i organizacyjnych, które wdrażają zgodnie z art. 32 - oznacza to, że właściwe dane osobowe muszą zostać wyodrębnione i być przechowane w oddzielnej bazie danych, i konieczne jest wdrożenie środków technicznych i organizacyjnych w celu zapobieżenia przetwarzaniu danych (w tym ich przeglądaniu, a także dostępu do nich). Odpowiednie dane osobowe muszą być przechowywane w oddzielnej i chronionej bazie danych, tak aby administrator był w stanie odpowiadać na jakiekolwiek zapytania i żądania właściwych władz (takich jak sądy, prokuratura, organy nadzorujące ochronę danych itp.) lub w przypadku, gdy przekazywanie danych takim władzom jest niezbędne w celu egzekucji albo ochrony roszczeń prawnych. W celu obliczenia okresu przechowywania 'zablokowanych' danych osobowych należy wziąć pod uwagę okresy przedawnienia różnego rodzaju roszczeń, które mogą powstać w następstwie przetwarzania odpowiednich danych osobowych. Dane osobowe mogą zostać całkowicie usunięte po upłynięciu właściwych okresów przedawnienia.

Jako administrator Danych Osobowych Reveal, musicie Państwo zapewnić, że jesteście w stanie sprostać temu wymogowi. Verizon wspiera Państwa w sprostaniu temu wymogowi poprzez umożliwienie pobierania kopii niektórych Danych Osobowych Reveal na samoobsługowym panelu sterowania Reveal, a także udzielanie pozostałych wymaganych przez Państwa Danych Osobowych Reveal.

J. Prawa osób, których dane dotyczą

Należy ustalić, w jaki sposób będzie wypełniany obowiązek udzielenia odpowiedzi na żądania osób fizycznych. Zgodnie z RODO, osoby fizyczne mają następujące prawa w odniesieniu do ich danych osobowych:

- prawo dostępu;
- prawo do sprostowania;
- praw do usunięcia;
- prawo do ograniczenia przetwarzania;
- prawo do przenoszenia danych;
- prawo sprzeciwu;
- prawa związane ze zautomatyzowanym podejmowaniem decyzji i profilowaniem.

Należy poinformować osoby fizyczne o przysługujących im powyższych prawach w Państwa informacji o ochronie prywatności.

Stosowanie powyższych praw może być ograniczone (np. prawo do przenoszenia danych przysługuje wyłącznie wówczas, gdy dane osobowe są przetwarzane w oparciu o odpowiednią podstawę prawną, tj. niezbędność do wykonania umowy albo zgodę), a także mogą Państwo powołać się na wyjątki (np. jeżeli zwolnienie informacji wpływałoby negatywnie na prawa innych, co mogłoby obejmować ochronę tajemnic handlowych).

Co do zasady, na żądania należy odpowiadać w terminie jednego miesiąca. Należy ponadto zapewnić, że Państwa odpowiedź spełnia dodatkowe wymogi wynikające z art. 12 RODO (np. informacje przekazywane osobom fizycznym są zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne oraz sformułowane jasnym i prostym językiem).

Jeżeli będzie to możliwe, Verizon może udzielić Państwu pomocy w spełnianiu żądań osób fizycznych, które

[17] *Wytyczne* CNIL *w sprawie geolokalizacji pojazdów pracowników,* 2018

odnoszą się do usług.

Osoby korzystające z usługi na terytorium Francji
Zgodnie z francuską ustawą o ochronie danych, osoby fizyczne mają prawo do określenia wytycznych w zakresie wykorzystania ich danych osobowych po ich śmierci. Należy zapewnić, że jesteście Państwo w stanie sprostać takiemu wymogowi.

K. Dzielenie się Danymi Osobowymi Reveal

Poza sytuacjami, w których osoby fizyczne żądają dostępu do własnych danych, konieczne jest określenie w jaki sposób będziecie Państwo odpowiadać na wnioski o dostęp do Danych Osobowych Reveal, pochodzące od osób trzecich. Mogą one obejmować, przykładowo, wnioski od organów ścigania i ubezpieczycieli, w związku z wypadkiem z udziałem pojazdu.

Przekazywanie Danych Osobowych Reveal (w tym np. innym organizacjom w Państwa grupie kapitałowej albo na rzecz innego dostawcy usług) musi spełniać wszelkie wymogi ochrony danych osobowych określone w niniejszym eBooku (np. przekazywanie musi być zgodne z prawem, proporcjonalne, przejrzyste itp.). Należy rozważyć, czy z tymi organizacjami zawarte zostały umowy lub inne porozumienia (na przykład, w przypadku gdy inna organizacja działa w Państwa imieniu jako podmiot przetwarzający albo gdy działa wspólnie z Państwem jako współadministartor). W przypadku, gdy takie przekazywanie obejmuje przekazywanie Danych Osobowych Reveal poza Europejski Obszar Gospodarczy (‘**EOG’**), konieczne będzie zapewnienie, że przekazywanie danych jest dozwolone zgodnie z RODO.

Osoby korzystające z usługi na terytorium Francji
Zgodnie z wytycznymi CNIL, należy ograniczyć dostęp do informacji dotyczących (lub wynikających z) urządzeń geolokalizacyjnych przez (odpowiednio): (i) Państwa własny upoważniony personel, (ii) pracodawcę osoby fizycznej, którego dane o geolokalizacji dotyczą; oraz (ii) upoważniony personel klienta, na rzecz którego świadczycie Państwo usługi. Co do zasady nie przekazuje się imienia i nazwiska kierowcy, chyba że informacje takie są szczególnie właściwe albo niezbędne.

L. Zautomatyzowane podejmowanie decyzji

Prawo o ochronie danych osobowych zabrania organizacjom podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych w przypadku, gdy decyzja miałaby wywierać skutki prawne lub w podobny sposób istotnie wpływać na osobę fizyczną. Konieczne jest zidentyfikowanie takiego wykorzystywania usług. Powyższe może mieć znaczenie w przypadku gdy:

- wynagrodzenie kierowcy jest automatycznie obliczane na podstawie czasu rozpoczęcia/zakończenia prowadzenia pojazdu;
- kierowca otrzymuje automatycznie ostrzeżenie o wjechaniu na określony obszar geograficzny;
- uprawnienie kierowcy do premii obliczane jest automatycznie na podstawie liczby zadań przypisanych kierowcy i przez niego wykonanych, zgodnie ze wskazaniami usługi.

Jeżeli decyzję podjęto z istotnym udziałem człowieka, powyższe ograniczenia nie mają zastosowania.

Organizacje są uprawnione do podejmowania wyłącznie takich zautomatyzowanych decyzji, jakie:

- są konieczne w celu wykonania lub zawarcia umowy;
- są uprawnione na mocy prawa unijnego lub prawa państwa członkowskiego, któremu podlega administrator, a także które przewidują odpowiednie zabezpieczenia praw osób, których dane dotyczą i ich wolności oraz uzasadnionych interesów; albo
- opierają się na wyraźnej zgodzie osoby, której dane dotyczą.

W przypadku podejmowania zautomatyzowanych decyzji, konieczne jest udzielenie osobom fizycznym wyraźnych informacji na ten temat (zob. ‘Informacje o ochronie prywatności’, powyżej) oraz, przynajmniej, udzielenie osobom fizycznym prawa do uzyskania interwencji ludzkiej w procesie podejmowaniu decyzji, wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

Osoby korzystające z usługi na terytorium Portugalii
Zabrania się korzystania z geolokalizacji i danych telemetrycznych pojazdu do celów całkowicie zautomatyzowanego podejmowania decyzji.[18]

M. Konsultacje pracownicze/z radą pracowniczą/związkiem zawodowym

Zgodnie z prawem pracy może zaistnieć konieczność skonsultowania się przez Państwa z pracownikami, radą pracowniczą albo związkami zawodowymi w sprawie wdrożenia usługi, albo dalszego wykorzystywania Danych Osobowych Reveal. Opcjonalnie, może zaistnieć konieczność konsultowania ze związkami zawodowymi albo przedstawicielami pracowników na mocy warunków dobrowolnych umów, które zostały przez Państwa zawarte. Nawet w przypadku braku wymogu, możecie Państwo uznać za stosowane skonsultowanie się z pracownikami w sprawie uruchomienia usługi i wykorzystywania Danych Osobowych Reveal w ramach procesu DPIA.

Jeżeli zawrzecie Państwo z radą pracowniczą wiążący układ , wówczas wprowadzi on "bardziej szczegółowe przepisy" w celu zapewnienia ochrony praw pracowników dotyczących ich danych osobowych zgodnie z art. 88(1) RODO. Oznacza to, że wspomniany układ może, w pewnych okolicznościach, zapewniać bezpieczeństwo prawne w zakresie tego, w jaki sposób można korzystać z Reveal w Państwa organizacji. W celu dopełnienia wymogu "bardziej szczegółowego przepisu" zgodnie z art. 88(1) RODO, układ pracy musi być zgodny z Państwa lokalnym prawem pracy i musi w sposób odpowiedni odnosić się do interesów pracowników dotyczących ich danych osobowych (zob. art. 88(2) RODO). W razie wątpliwości należy zasięgnąć porady prawnej.

Osoby korzystające z usługi na terytorium Francji
Zgodnie z art. L2312-38 francuskiego kodeksu pracy, jesteście Państwo zobowiązani do powiadomienia i przeprowadzenia konsultacji z radą pracowniczą (*Conseil Economique et Social*) przed wdrożeniem jakichkolwiek systemów albo środków monitorowania działalności pracownika, takich jak śledzenie geolokalizacji.

Osoby korzystające z usługi na terytorium Niemiec
Zgodnie z art. 87 ust. 6 ustawy o konstytucji pracy (*Betriebsverfassungsgesetz -BetriebsVG*), rada pracownicza, o ile została ustanowiona w Państwa organizacji, ma prawo do współdziałania w określaniu sposobu wdrożenia i wykorzystywania urządzeń technicznych zaprojektowanych do celów monitorowania zachowania i wyników pracowników. Stała 'kontrola' zachowania i wykonania przez pracowników w drodze monitoringu nie jest dozwolona - jeżeli jesteście Państwo pracodawcą, wymaga się, aby wykluczyli Państwo taką stałą 'kontrolę' pracowników na mocy umów z radą pracowniczą albo jednostronnie na mocy wiążącego regulaminu.[19]

Art. 26 ust. 4 federalnej ustawy o ochronie danych stwierdza wyraźnie, że przetwarzanie danych może być dozwolone na podstawie umów o pracę, pod warunkiem, że takie umowy o pracę są zgodne z art. 88 ust. 2 RODO.

Osoby korzystające z usługi na terytorium Włoch
W razie potrzeby, istnieje możliwość prowadzenia konsultacji ze związkami zawodowymi w Państwa organizacji (o ile zostały ustanowione) albo uzyskania zgody właściwego Urzędu Pracy, w zakresie wdrożenia usługi i wykorzystywania Danych Osobowych Reveal zgodnie z art. 4 ust. 2 Ustawy nr 300/1970 (włoskiej ustawy pracowniczej), chyba że Dane Osobowe Reveal, które Państwo przetwarzacie są ograniczone do danych ściśle Państwu niezbędnych w celu wywiązania się z obowiązków prawnych.

Osoby korzystające z usługi na terytorium Polski
Należy określić cel, zakres oraz sposób monitorowania w Państwa regulaminie pracy (polityka wewnętrzna, którą muszą mieć pracodawcy posiadający ponad 50 pracowników w Polsce) albo zakładowym układzie zbiorowym pracy. Jeżeli w Państwa organizacji działają związki zawodowe, zmiany w regulaminie pracy albo

[18] Wytyczne CNPD w sprawie wykorzystywania urządzeń geolokalizacyjnych w kontekście zatrudnienia i ścisłej interpretacji postanowień Kodeksu Pracy

[19] Komisarz ds. Ochrony Danych i Swobody Przepływu Informacji w Baden-Wirtenbergii, *Ochrona danych pracowniczych*, 2018 ; Niezależne Centrum Ochrony Danych w Schleswigu-Holsteinie, Sprawozdanie z działalności 2017-2018, 103

zakładowym układzie zbiorowym pracy wymagać będą współpracy ze związkami zawodowymi.

Należy poinformować zatrudnionych pracowników o Państwa zamiarze wdrożeniu systemu monitorowania. Taka informacja nie może zostać udostępniona później niż dwa tygodnie przed wdrożeniem systemu monitorowania.

Osoby korzystające z usługi na terytorium Portugalii
Zgodnie z art. 21 portugalskiego kodeksu pracy, jesteście państwo zobowiązani do poinformowania i przeprowadzenia konsultacji z radą pracowniczą (*Comissão de Trabalhadores*) przed wdrożeniem jakiegokolwiek systemu albo środków umożliwiających monitorowanie działalności pracowników takich, jak śledzenie za pomocą geolokalizacji.

Osoby korzystające z usługi na terytorium Hiszpanii
Zgodnie z art. 64 ust. 1 hiszpańskiej ustawy pracowniczej, konieczne jest poinformowanie przedstawicieli pracowników przed wdrożeniem jakiegokolwiek środka, który może mieć wpływ na pracowników, co zgodnie z interpretacją obejmuje wdrożenie urządzeń geolokalizacyjnych albo jakiegokolwiek innego rodzaju rozwiązań.

Dodatkowo art. 90 ust. 2 ustawy organicznej 3/2018 z dnia 5 grudnia w sprawie ochrony danych osobowych i gwarancji praw cyfrowych stanowi, że przed wdrożeniem urządzeń geolokalizacyjnych konieczne jest poinformowanie pracowników i przedstawicieli pracowników o istnieniu i cechach takich urządzeń.

N. Środki ograniczające ryzyko oraz ochrona danych w fazie projektowania i domyślna ochrona danych

Należy podjąć kroki niezbędne do ograniczenia ryzyka dla osób fizycznych (określonych w ramach procesu DPIA) oraz przestrzegania wymogów ochrony danych w fazie projektowania i domyślnej ochrony danych. Ochrona danych w fazie projektowania oznacza konieczność odniesienia się do kwestii prywatności, a także wzięcia ich pod uwagę na początku czynności przetwarzania danych (tj. w fazie projektowania), oraz przez cały czas trwania takiej czynności przetwarzania. Domyślna ochrona danych wymaga zapewnienia, że przetwarzana jest minimalna ilość danych niezbędnych do osiągnięcia celu (celów) (na przykład, zamiast zezwalać szerokiemu kręgowi osób na dostęp do Danych Osobowych Reveal, dostęp należy ograniczyć do poszczególnych osób zgodnie z zasadą ścisłej potrzeby).

Wytyczne organów nadzorujących ochronę danych wymieniają przykładowe środki ograniczające ryzyko w kontekście telematyki i monitorowania pracowników:

- Pracownicy powinni mieć możliwość czasowego wyłączenia śledzenia lokalizacji w niektórych przypadkach (np. ilekroć udają się do ośrodka zdrowia), o ile dozwolone jest korzystanie z pojazdu firmowego do celów prywatnych.[20]
- W przypadku konieczności monitorowania lokalizacji pojazdu poza godzinami pracy (np. w celu zapobiegania kradzieżom), wdrożenie powinno być proporcjonalne do ryzyka np. lokalizacja pojazdu nie jest rejestrowana (albo widoczna) poza godzinami pracy, dopóki pojazd nie opuści szeroko zdefiniowanego obszaru (np. regionu).[21]
- należy zminimalizować liczbę personelu mającego dostęp do Danych Osobowych Reveal. Personel musi być odpowiednio przeszkolony i zobowiązany do zachowania poufności oraz przestrzegania zasad bezpieczeństwa.[22]
  Proszę przemyśleć, które osoby są najodpowiedniejsze do uzyskania dostępu do Danych Osobowych Reveal (mogą nimi nie być przykładowo bezpośredni przełożeni).[23]

O. Wyznaczenie Inspektora Ochrony Danych (IOD)

Niektóre źródła obowiązku powoływania inspektora ochrony danych (IOD) określa art. 37 RODO. Być może Państwa obecne czynności przetwarzania nie wymagają jeszcze wyznaczenia IOD. Niemniej jednak korzystanie przez Państwa z usług może stanowić podstawę do ustanowienia IOD w świetle art. 37 ust.1 lit. b, który

[20] Art. 29 Grupa roboczej *Opinia 2/2017 w sprawie przetwarzania danych w pracy* (WP249), s.20

[21] Art. 29 Grupa robocza *Opinia 2/2017 w sprawie przetwarzania danych w pracy* (WP249), s.20

[22] Informacje Urzędu Komisarza *Kodeks praktyk pracowniczych*, s. 67

[23] Informacje Urzędu Komisarza *Kodeks praktyk pracowniczych*, s. 67

wymaga powołania IOD w przypadku, gdy główna działalność organizacji polega na regularnym i systematycznym monitorowaniu osób, których dane dotyczą na szeroką skalę. Korzystanie z usług monitorowania kierowców i ich zachowania w trakcie jazdy może podlegać przepisom art. 37 ust. 1 lit. b, a w takim przypadku wymagane będzie powołanie IOD. Pozostałe postanowienia RODO (art. 38 i art. 39) określają wymogi związane ze statusem i zadaniami IOD - przestrzeganie tych przepisów również będzie wymagane w przypadku wymogu powołania IOD.

Osoby korzystające z usługi na terytorium Niemiec

Zgodnie z art. 38 federalnej ustawy o ochronie danych (BDSG) wymaga się wyznaczenia IOD w przypadku zatrudniania na stałe co najmniej 20 osób do zautomatyzowanego przetwarzania danych osobowych albo jeżeli przetwarzanie przez Państwa danych osobowych wymaga przeprowadzenia DPIA. W przypadku korzystania z usług w Niemczech może zaistnieć potrzeba powołania IOD.

Dodatkowe informacje

Ustawodawstwo

- Ogólne rozporządzenie o ochronie danych (UE) 2016/679 ('RODO)
- Ustawa o ochronie danych (ang.: *Data Protection Act*) 2018 (UK)
- Ustawa nr 58/2019 z dnia 8 sierpnia 2019 r. (Portugalia)
- Kodeks Pracy (Portugalia)
- Ustawa konstytucyjna 3/2018 5 grudnia 2018 w sprawie ochrony danych osobowych i gwarancji praw cyfrowych (Hiszpania)
- Federalna ustawa o ochronie danych (niem.: *Bundesdatenschutzgesetz – BDSG*) 2018 (Niemcy)
- Ustawa o konstytucji pracy (niem.: *Betriebsverfassungsgesetz -BetriebsVG*) (Niemcy)
- Dekret ustawodawczy nr 196/2003 (włoski kodeks o ochronie danych) (Włochy)
- Ustawa nr 300/1970 (włoska ustawa pracy) (Włochy)
- Dekret ustawodawczy 101/2018 (Włochy)
- Francuska ustawa o ochronie danych n°78-17(Francja)
- Francuski kodeks pracy (Francja)

Orzecznictwo

South Lanarkshire Council przeciwko Scottish Information Commissioner [2013] UKSC 55 (Wielka Brytania)

Wytyczne regulacyjne

UE

- Grupa robocza, art. 29 *Opinia 5/2005 w sprawie wykorzystania danych lokalizacyjnych w celu świadczenia usług stanowiących wartość dodaną* (WP115)
- Grupa robocza, art. 29 *Opinia 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych* (WP 185)
- Grupa robocza, art. 29 *Wytyczne w sprawie oceny skutków w zakresie ochrony danych (DPIA) oraz określające czy przetwarzanie "może powodować ryzyko" do celów Rozporządzenia 2016/679* (WP248)
- Grupa robocza, art. 29 *Opinia 2/2017 w sprawie przetwarzania danych w pracy* (WP249)
- Grupa robocza, art. 29 *Opinia 2016/679 Wytyczne w sprawie zautomatyzowanego podejmowania indywidulanych decyzji i profilowania do celów Rozporządzenia* (WP251)
- *Wytyczne* Europejskiej Rady Ochrony Danych *2/2019 w sprawie przetwarzania danych osobowych na mocy art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online na rzecz osób, których dane dotyczą (wersja do konsultacji publicznej)*

Francja

- Wytyczne CNIL w sprawie geolokalizacji pojazdów pracowników, 2018

Niemcy

- Komisarz do spraw Ochrony Danych i Swobodnego Przepływu Informacji w Nadrenii Palatynatu, *O zgodności z prawem śledzenia GPS pracowników*
- Komisarz do spraw Ochrony Danych i Swobodnego Przepływu Informacji w Badenii Wirtembergii, *Ochrona danych pracowniczych* 2018
- Konferencja w sprawie Ochrony Danych niezależnych federalnych władz ochrony danych i władz ochrony danych w landach (*Länder*) (*Datenschutzkonferenz - DSK*), Krótkie opracowanie Nr 14: *Ochrona danych pracowniczych* (17 grudnia 2018)
- Bawarski Komisarz Ochrony Danych, *27. Sprawozdanie z działalności 2016*
- Konferencja w sprawie Ochrony Danych niezależnych federalnych władz ochrony danych i władz ochrony danych w landach (*Länder*) (*Datenschutzkonferenz - DSK*), Krótkie opracowanie Nr 17: *Szczególne kategorie danych osobowych* (27 marca 2018)
- Konferencja w sprawie Ochrony Danych niezależnych federalnych władz ochrony danych i władz ochrony danych w landach (*Länder*) (*Datenschutzkonferenz - DSK*), Krótkie opracowanie Nr 19: *Informacje i zobowiązanie pracowników do przestrzegania wymogów ochrony danych na mocy RODO* (29 maja 2018)
- Komisarz do spraw Ochrony Danych i Swobodnego Przepływu Informacji Północnej w Nadrenii Westfalii (LDi NRW), 24, Raport w sprawie ochrony danych i swobodnego przepływu informacji 2017-2018, *Pozycjonowanie w oparciu o satelitę w celu określenia lokalizacji pojazdów służbowych - brak dozwolonych środków monitorowania pracowników*
- Berliński Komisarz ds. Ochrony Danych Swobodnego Przepływu Informacji, *Sprawozdanie roczne 2018*
- Niezależne Centrum Ochrony Danych w Schleswig-Holstein, Sprawozdanie z działalności 2017-2018
- Komisarz Ochrony Danych w Dolnej Saksonii, 24. Sprawozdanie z działalności 2017-2018, M*onitorowanie GPS pojazdów służbowych*

Polska

- Urząd Ochrony Danych, *Ochrona danych w miejscu pracy. Wytyczne dla pracodawców*

Portugalia

- Obrady CNPD 7680/2014 (Wytyczne w sprawie wykorzystywania geolokalizacji w kontekście zatrudnienia).

Zjednoczone Królestwo

- Urząd Komisarza ds. Informacji *Kodeks Praktyk Zatrudnienia* oraz *Wytyczne Uzupełniające*

Lista kontrolna RODO

Art. RODO	Temat	Znaczenie dla Reveal	Gdzie szukać w eBooku
Art. 1, 2 albo 3	Przedmiot i cele; materialny i terytorialny zakres stosowania	Brak szczególnego znaczenia	N/D
Art. 4	Definicje	Definiuje pojęcia: 'danych osobowych' i 'szczególnych kategorii' danych osobowych	*„Najczęściej zadawane pytania na temat usługi Reveal*", rozdział 3 i rozdział 4
Art. 5	Zasady i odpowiedzialność	Przetwarzanie Danych Osobowych Reveal musi być zgodne z zasadami ochrony danych, i administrator musi być w stanie wykazać zgodność	*„Wymogi w zakresie ochrony danych"* - ogólnie
Art. 6 i 7	Zgodność przetwarzania z prawem i warunki wyrażenia zgody	Konieczna jest podstawa prawna dla każdego celu przetwarzania Danych Osobowych Reveal	*„Wymogi w zakresie ochrony danych"*, rozdział E
Art. 8	Warunki wyrażenia zgody	Brak szczególnego	N/D

	przez dziecko w przypadku usług społeczeństwa informacyjnego	znaczenia	
Art. 9 i 10	Przetwarzanie szczególnych kategorii danych osobowych i informacji o czynach zabronionych	W przypadku każdego celu w odniesieniu do Danych Osobowych Reveal konieczna jest odpowiednia przesłanka uchylająca zakaz przetwarzania szczególnych kategorii danych lub danych dotyczących naruszeń prawa	*„Najczęściej zadawane pytania na temat usługi Reveal*", rozdział 4, i *„Wymogi w zakresie ochrony danych”* , rozdział E
Art. 11	Przetwarzanie niewymagające identyfikacji	Brak szczególnego znaczenia	N/D
Art. 12	Przejrzyste informowanie, komunikacja oraz tryb wykonywania praw przez osobę, której prawa dotyczą	Informacje podane do wiadomości osób, których Dane Osobowe Reveal są przetwarzane muszą być zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne oraz formułowane jasnym i prostym językiem.	*„Wymogi w zakresie ochrony danych”* rozdział B i rozdział J
Art. 13 i 14	Informacje podawane osobie, której dane dotyczą	Osobom, których dane Osobowe Reveal są przetwarzane należy przekazać zawiadomienie o ochronie danych	*„Wymogi w zakresie ochrony danych”,* rozdział B
Art. 15	Prawo dostępu	Na żądanie należy osobom umożliwić dostęp do Danych Osobowych Reveal (z zastrzeżeniem wyjątków)	*„Wymogi w zakresie ochrony danych”,* rozdział J
Art. 16	Prawo do sprostowania	Na żądanie osób Dane Osobowe Reveal muszą zostać sprostowane	*„Wymogi w zakresie ochrony danych”,* rozdział J
Art. 17	Prawo do usunięcia	Na żądanie osób Dane Osobowe Reveal muszą zostać usunięte, o ile to prawo przysługuje	*„Wymogi w zakresie ochrony danych”*, rozdział J
Art. 18	Prawo do ograniczenia	Na żądanie osób przetwarzanie Danych Osobowych Reveal musi zostać ograniczone, o ile to prawo przysługuje	*„Wymogi w zakresie ochrony danych”*, rozdział J
Art. 19	Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania	W przypadku otrzymania wniosku o sprostowanie, usunięcie albo ograniczenie w odniesieniu do Danych Osobowych Reveal, o takim wniosku należy	*„Wymogi w zakresie ochrony danych”,* rozdział J

		poinformować osoby trzecie, którym dane ujawniono	
Art. 20	Prawo do przenoszenia danych	Dane Osobowe Reveal muszą zostać przeniesione do osób, których te dane dotyczą (lub wskazanych osób trzecich) na żądanie osób, o ile to prawo przysługuje	*„Wymogi w zakresie ochrony danych”*, rozdział J
Art. 21	Prawo sprzeciwu	Na żądanie osoby Dane Osobowe Reveal nie mogą być dalej przetwarzane, o ile to prawo przysługuje	*„Wymogi w zakresie ochrony danych”*, rozdział J
Art. 22	Zautomatyzowane podejmowanie decyzji w indywidulanych przypadkach, w tym profilowanie	Całkowicie zautomatyzowane decyzje o osobach, które prowadzą do prawnych lub podobnie istotnych skutków mogą być podejmowane zgodnie z art. 22	*„Wymogi w zakresie ochrony danych”*, rozdział L
Art. 23	Ograniczenia	Brak szczególnego znaczenia	N/D
Art. 24	Obowiązki administratora	Należy wdrożyć środki techniczne i organizacyjne w celu zapewnienia (i wykazania), że przetwarzanie jest zgodne z RODO	*„Wymogi w zakresie ochrony danych ”* - ogólnie
Art. 25	Ochrona danych w fazie projektowania oraz domyślna ochrona danych	Należy się odnieść do kwestii ochrony danych na początku i w trakcie przetwarzania Danych Osobowych Reveal, i przetwarzaniu powinno podlegać minimum danych osobowych niezbędne do osiągniecia celu	*„Wymogi w zakresie ochrony danych”,* rozdział F i rozdział N
Art. 26	Współadministratorzy	Brak szczególnego znaczenia	N/D
Art. 27	Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii	Brak szczególnego znaczenia	N/D
Art. 28	Podmiot przetwarzający	Do przetwarzania Danych Osobowych Reveal zaangażowane mogą być wyłącznie podmioty	*„Wymogi w zakresie ochrony danych”,* rozdział I

		przetwarzające zapewniające odpowiednie gwarancje i takie podmioty przetwarzające muszą podlegać obowiązkom na mocy umowy	
Art. 29	Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego	Brak szczególnego znaczenia	N/D
Art. 30	Rejestrowanie czynności przetwarzania	Przetwarzanie Danych Osobowych Reveal musi być odzwierciedlone w rejestrze czynności przetwarzania	„Wymogi w zakresie ochrony danych”, rozdział C
Art. 31	Współpraca z organem nadzorczym	Brak szczególnego znaczenia	N/D
Art. 32	Bezpieczeństwo przetwarzania	Konieczne jest wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić bezpieczeństwo Danych Osobowych Reveal	*„Wymogi w zakresie ochrony danych”,* rozdział I
Art. 33 i 34	Zgłaszanie naruszenia ochrony danych osobowych (organowi nadzorczemu i osobom)	W przypadku naruszenia ochrony Danych Osobowych Reveal, jeżeli przekroczone zostały odpowiednie progi, należy zawiadomić o tym organ nadzorczy oraz osoby, dotknięte naruszeniem	*„Wymogi w zakresie ochrony danych”* , rozdział I
Art. 35 i 36	Ocena skutków dla ochrony danych i uprzednie konsultacje	Należy przeprowadzić ocenę skutków dla ochrony danych w przypadku przetwarzania Danych Osobowych Reveal oraz, jeżeli zachodzi potrzeba, przeprowadzić konsultacje z organem nadzorczym, jeżeli przetwarzanie powoduje wysokie realne ryzyko dla osób	*„Wymogi w zakresie ochrony danych”* , rozdział A
Art. 37, 38 i 39	Inspektor ochrony danych	Właściwy inspektor danych osobowych musi zostać powołany, jeżeli główna działalność administratora polega na 'regularnym i systematycznym' monitorowaniu osób,	*„Wymogi w zakresie ochrony danych”* , rozdział Q

		których dane dotyczą na dużą skalę lub na przetwarzaniu na dużą skalę szczególnych kategorii danych/danych dotyczących naruszeń prawa	
Art. 40, 41, 42 i 43	Kodeksy postępowania, certyfikacja i akredytacja	Brak szczególnego znaczenia	N/D
Art. 44 - 50	Przekazywanie	Przekazywanie Danych Osobowych Reveal poza EOG do państw, które nie zapewniają odpowiedniej ochrony (np. innym dostawcom platform lub grupom spółek) jest dopuszczalne jedynie przy jednoczesnym zastosowaniu mechanizmu przekazywania lub w przypadku zaistnienia wyjątku	*„Najczęściej zadawane pytania na temat usługi Reveal*", *rozdział* 6, i „Wymogi w zakresie ochrony danych" , rozdział K
Art. 51 - 59	Organ nadzorczy i właściwość, zadania, uprawnienia i sprawozdania	Brak szczególnego znaczenia	N/D
Art. 60 - 67	Współpraca i spójność	Brak szczególnego znaczenia	N/D
Art. 68 - 76	Europejska Rada Ochrony Danych	Brak szczególnego znaczenia	N/D
Art. 77	Prawo do wniesienia skargi do organu nadzorczego	Brak szczególnego znaczenia	N/D
Art. 78	Prawo do środka ochrony prawnej przeciwko organowi nadzorczemu	Brak szczególnego znaczenia	N/D
Art. 79 - 82	Prawo do skutecznego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu i odszkodowanie	Brak szczególnego znaczenia	N/D
Art. 83 - 84	Sankcje i kary administracyjne	Brak szczególnego znaczenia	N/D
Art. 85 - 91	Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem	Brak szczególnego znaczenia	N/D
Art. 92 - 93	Akty delegowane i akty wykonawcze	Brak szczególnego znaczenia	N/D
Art. 94 - 99	Przepisy końcowe	Brak szczególnego	N/D

		znaczenia	