Warszawa, 01.04.2025 r.

Signal, Whatsapp i inne komunikatory internetowe a RODO

Świat niedawno obiegła historia grupy na komunikatorze Signal, w której dziennikarz „The Atlantic" uzyskał dostęp do informacji o planowanych przez rząd USA nalotach na rebeliantów Huti w Jemenie[i]. Historia ta zyskała sporo uwagi w mediach i jej popularność jest dobrym przyczynkiem do tego, by porozmawiać o korzystaniu z tego typu aplikacji w świetle ogólnego bezpieczeństwa informacji w organizacji oraz przepisów o ochronie danych osobowych.
Celem niniejszej publikacji jest przybliżenie prawnych i organizacyjnych kwestii związanych z wykorzystaniem komunikatorów internetowych w świetle przepisów o ochronie danych osobowych, omówienie podstawowych kwestii bezpieczeństwa oraz sposobów na wykazanie zgodności z przepisami w razie kontroli organu regulacyjnego.

Czy w ogóle można?

W pewnym uproszczeniu, pracownicy firmy będą korzystali z komunikatorów internetowych na dwa sposoby:

- do prywatnego kontaktu między sobą (umówienie wspólnego spotkania po pracy, przesyłanie memów z kotkami, zastępstwa urlopowe, itp.);
- do wszelkich wymagających kontaktu spraw służbowych (przekazywanie materiałów, ustalenia terminów i agend spotkań, współdzielenie dokumentów itp.).

Truizmem będzie powiedzieć, że pracodawca ani nie ma narzędzi prawnych, ani interesu w kontrolowaniu kontaktów z tej pierwszej grupy. Jest to całkowicie prywatna sfera życia pracowników, do której RODO – z mocy jego art. 2 ust. 2 lit. c) – nie ma zastosowania. To z jakich narzędzi pracownicy korzystają w życiu prywatnym i jakie dane w nich udostępniają pozostaje ich sprawą. Ważne jest jednak, by przy tych prywatnych kontaktach pracownicy nie przesyłali danych osobowych administrowanych przez firmę, czy innych informacji, które firma ma obowiązek chronić (jak informacji np. objętych tajemnicą handlową).

Jeżeli chodzi o kontakt w sprawach służbowych, tu RODO jak najbardziej będzie miało zastosowanie. Pracodawca – jako administrator danych osobowych – określa cele i metody przetwarzania danych. Nie tylko może, ale i powinien określić z jakich narzędzi należy korzystać w trakcie świadczenia pracy. Jasne określenie z jakich narzędzi informatycznych wolno korzystać i jakie dane mogą być do nich wprowadzane. Takie klarowne zasady pozwolą przeprowadzić sensowną analizę ryzyka dla tego typu działań, faktycznie zarządzać retencją takich komunikatów oraz uniknąć sytuacji, która spotkała niedawno amerykańskich urzędników najwyższego szczebla.

Czy Signal jest bezpieczny, czyli jak wybrać komunikator?

Autor niniejszego tekstu nie posiada wiedzy i umiejętności pozwalających ocenić techniczne zabezpieczenia aplikacji. Ale dostępne publikacje osób, które taką wiedzą dysponują pozwalają na szybko odpowiedzieć że:

- Signal jest open sourceowym rozwiązaniem, które oferuje pełne szyfrowanie danych end to end i ma generalnie dobrą opinię w środowisku bezpieczeństwa informacji[ii]. Z uwagi na fakt, właścicielem Signal Messenger LLC jest fundacja non profit Signal Technology Foundation[iii] ryzyko że treść rozmów na aplikacji zostanie wykorzystana w innym celu (np. do szkolenia AI

bądź do opracowania celowanego ataku phishingowego) należy ocenić niższa niż u konkurencji.

- Whatsapp należy obecnie do korporacji Meta, jest programem, który cieszy się ogólnie dobrą opinią jeżeli chodzi o oferowany poziom bezpieczeństwa[iv]. Czy Meta wykorzystuje do własnych celów wiedzę zebraną z analizy rozmów? Autorowi raz zdarzyło się wspomnieć nazwę pewnego produktu w rozmowie na Whatsapp przed południem, by po południu zobaczyć jego reklamę na Facebooku. Zbieg okoliczności[v]?
- Microsoft Teams jest elementem płatnego pakietu Office 365 oferowanego przez Microsoft. Ma tę zaletę, że dostęp do aplikacji może być zarządzany przez firmę, która go wykupiła – co oznacza że z chwilą zakończenia współpracy z danym pracownikiem utraci on cały dostęp do historii rozmów i przekazanych tamtędy danych.
- Google Chat można pozyskać wykupując pakiet biznesowy Google Workspace, ma te same zalety co produkt Microsoftu – tylko integruje się z pakietem Mountain View, a nie firmy z Redmond.
- Telegram jest popularnym komunikatorem opracowanym przez obywatela Federacji Rosyjskiej[vi]. Szeroko informowano, że technologia szyfrowania zastosowana w tym oprogramowaniu ma wady, a w szczególności nie używa szyfrowania typu End-to-End dla całej komunikacji[vii]. Z doniesień prasowych wynika również, że dostęp do tego oprogramowania mogły uzyskać rosyjskie agencje wywiadowcze[viii].

Który program jest najlepszy? Autor niniejszego tekstu skłania się ku rozwiązaniom Microsoft Teams oraz Google Chat – głównie dlatego, że są to usługi płatne, dające dużą kontrolę nad kontami użytkowników. Pozwalają również na taką konfigurację, by dane osobowe nie opuszczały Europejskiego Obszaru Gospodarczego, co jest dodatkowym plusem z perspektywy compliance. Dodatkowo trzymanie wszystkich danych w obrębie jednego ekosystemu odrobinę zmniejsza ogólny poziom ryzyka dla ochrony danych.
Ale trzeba przyznać, że Mocie Marlinspike (pseudonim Matthew Rosenfeld`a – twórcy Signala), również ma mocne argumenty za swoim produktem:

Udokumentowanie zgodności

Zacznę od małego truizmu: w mikroprzedsiębiorstwach nie ma sensu tworzyć dodatkowych papierów do regulowania kwestii korzystania z komunikatora internetowego. Ale na pewno w przedsiębiorstwach średnich i dużych takie wytyczne będą bardzo pomocne. W wewnętrznej dokumentacji warto odnotować co najmniej:

- jakie komunikatory są dopuszczalne do celów służbowych (tu warto skonsultować kwestie techniczne z działem IT);

- że przesyłanie danych osobowych związanych z świadczoną pracą innymi kanałami jest zakazane;
- jeżeli firma nie korzysta z centralnie zarządzanego narzędzia jak Microsoft Teams czy Google Chat – jakie są zasady usuwania użytkowników z grupowych czatów po zakończeniu współpracy;
- zasady retencji danych osobowych przetwarzanych z użyciem komunikatorów;
- zasady autoryzacji przy logowaniu (najlepiej z użyciem logowania dwuskładnikowego);
- jakie dane można przesyłać komunikatorem, a jakich nie (bardzo dobrym, bezpiecznym rozwiązaniem jest wprowadzenie zasady udostępniania odnośników do plików na zasobie sieciowym zamiast samych plików – wówczas ewentualnie omyłkowo dodany dziennika… użytkownik nie będzie mógł otworzyć zalinkowanego pliku z powodu braku uprawnień na chmurze);
- zasady kontaktu z klientami za pomocą wybranych kanałów komunikacji.

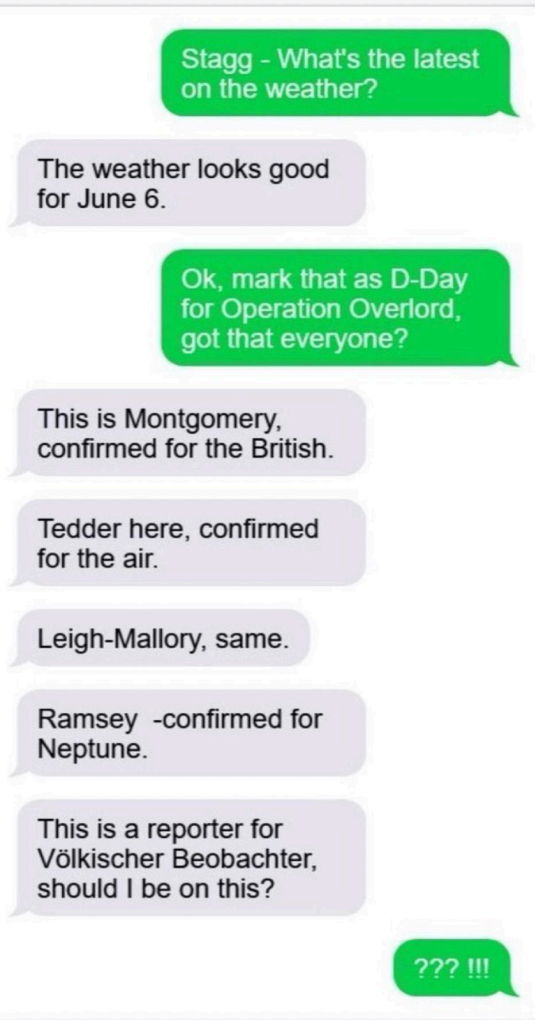
Kwestie te najlepiej zawrzeć w osobnym dokumencie i udostępniać go pracownikom w taki sposób, by w razie kontroli dysponować dowodem, że pracownicy się z nim zapoznali.

Korzystanie z wybranego komunikatora internetowego należy też oczywiście odnotować w Rejestrze Czynności Przetwarzania Danych Osobowych i uwzględniać przy szacowania ryzyka dla procesów przetwarzania danych osobowych.

Podsumowując

Szczególnie po okresie pandemicznej pracy z domu trudno wyobrazić sobie pracę biurową bez użycia komunikatorów internetowych. Wiosną 2020 roku prawie wszyscy uczyliśmy się pracy z domu przy akompaniamencie przejeżdżających pod domami radiowozów nadających przez megafon komunikat o wywołanym pandemią obowiązku pozostania w domu. Wtedy można było spodziewać się łagodnej reakcji organów państwa na potknięcia przy korzystaniu z tych nierzadko nowych w organizacji narzędzi. Te czasy jednak bezpowrotnie minęły i w razie incydentu związanego z korzystaniem z komunikatora internetowego nie można już liczyć na wyrozumiałość organów. Zapewnienie bezpieczeństwa przekazywanych informacji to nie tylko prawny obowiązek, ale też i przewaga konkurencyjna firmy.
Zarządzający przedsiębiorstwami powinni pamiętać, że ewentualne kary za naruszenie RODO nie powinny osiągnąć skali która doprowadzi firmę do bankructwa. Tego samego nie można jednak powiedzieć o wycieku tajemnic przedsiębiorstwa – tu nie ma limitu strat do poniesienia.

Dziękując za pozostanie z nami do końca artykułu i mamy primaaprilis, podzielę się ulubionym memem związanym z Signalgate. Co prawda nazwisko adm. Ramsay`a jest z literówką, ale żart uważam przedni.



Daniel Taberski - radca prawny, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.

Przypisy

[i] https://www.wirtualnemedia.pl/artykul/signalgate-w-usa-redakcja-the-atlantic-publikuje-plan-uderzenia-na-jemen-z-czatu-urzednikow [dostęp 01.04.2025 r.].
[ii] https://www.computerworld.pl/article/2501719/signal-czy-ten-komunikator-jest-bezpieczny.html [dostęp 01.04.2025 r.], https://sekurak.pl/czym-jest-komunikator-signal-jakie-bezpieczenstwo-zapewnia-jak-z-niego-korzystac/ [dostęp 01.04.2025 r.],
[iii] https://signalfoundation.org/ [dostęp 01.04.2025 r.].
[iv] https://zaufanatrzeciastrona.pl/post/podstawy-bezpieczenstwa-whatsapp-jak-zadbac-o-bezpieczenstwo-i-prywatnosc/ [dostęp 01.04.2025 r.].
[v] To oczywiście dowód anegdotyczny i zbyt mała próbka by wyciągać jakieś szersze wnioski, a to naprawdę mógł być zbieg okoliczności.
[vi] https://telegram.org/press?setln=pl [dostęp 01.04.2025 r.].
[vii] https://www.avast.com/c-is-telegram-safe [dostęp 01.04.2025 r.]. https://www.forbes.com/sites/zakdoffman/2024/02/02/apple-iphone-google-pixel-and-samsung-galaxy-telegram-app-warning/ [dostęp 01.04.2025 r.], https://polskieradio24.pl/artykul/3417917,kreml-ma-dostep-do-prywatnych-tresci-na-telegramie-eksperci-o-aplikacji [dostęp 01.04.2025 r.], https://oko.press/komunikator-telegram-bezpieczenstwo [dostęp 01.04.2025 r.], https://www.pcmag.com/reviews/telegram [dostęp 01.04.2025 r.].
[viii] https://techcrunch.com/2019/09/18/russia-sorm-nokia-surveillance/ [dostęp 01.04.2025 r.].