

Viskase Companies Inc.



Polityka Prywatności dla Pracowników w UE - Polska

Data publikacji: 25 maja 2018 roku

KARTA AKTUALIZACJI

Tytuł dokumentu	Viskase – Polityka Prywatności dla Pracowników w UE - Polska
Autor(zy)	Główny specjalista ds. zgodności (<i>Chief Compliance Officer</i>)
Numer wersji	1.0
Data dokonania zmiany	25 maja 2018 roku

Tabela 1 – identyfikacja dokumentu

Historia	Data	Status
Wersja 1.0	25/5/2018	Pierwsza publikacja - zatwierdzona

Tabela 2 – historia dokumentu

Spis treści

1. PRZEGLĄD POLITYKI	4
2. CEL.....	4
3. ZAKRES	5
4. OCHRONA DANYCH OSOBOWYCH.....	5
5. OGÓLNE KORZYSTANIE I PRAWO WŁASNOŚCI	7
6. DOZWOLONE KORZYSTANIE	7
7. NIEDOZWOLONE KORZYSTANIE	8
8. ZASADY UZYSKIWANIA DOSTĘPU DO INTERNETU	9
9. ZASADY KORZYSTANIA Z ADRESU E-MAIL	10
10. ZASADY KORZYSTANIA Z TELEFONÓW	12
11. ŚRODKI MONITOROWANIA STOSOWANE PRZEZ VISKASE	12
12. DANE UDOSTĘPNIANE PRZEZ VISKASE PODMIOTOM TRZECIM.....	13
13. NARUSZENIA OCHRONY DANYCH OSOBOWYCH.....	13
14. ZASADY ZACHOWYWANIA WIADOMOŚCI E-MAIL	13
15. ODEJŚCIE PRACOWNIKA	14
16. EGZEKWOWANIE POLITYKI	15
17. KONTAKT	15

VISKASE – POLITYKA PRYWATNOŚCI DLA PRACOWNIKÓW

1. PRZEGLĄD POLITYKI

Niniejszą politykę stosuje się do pracowników Viskase Companies, Inc. oraz jej spółek zależnych ("Viskase" lub "Spółka").

Niniejsza polityka ustala rodzaje danych osobowych pracowników, które są przetwarzane przez Viskase, jak również zasady korzystania z zapewnianych przez Spółkę systemów Internetu, Intranetu oraz Extranetu, w tym między innymi sprzętu komputerowego, urządzeń mobilnych, oprogramowania, systemów operacyjnych, nośników danych, kont w sieci umożliwiających korzystanie z usług e-mail, przeglądanie Internetu oraz FTP ("Systemy i Technologie Informatyczne Viskase"). Niniejszą politykę należy czytać w powiązaniu z Informacją Viskase o Ochronie Danych Osobowych, która wyjaśnia sposoby, w jakie Viskase zbiera i wykorzystuje dane osobowe pracowników oraz prawa przysługujące pracownikom w związku ze zbieraniem i wykorzystywaniem ich danych osobowych.

Zezwala się i zachęca pracowników Viskase do korzystania z usługi e-mail oraz Internetu jeżeli takie korzystanie wspiera osiągnięcie celów wynikających z działalności gospodarczej Spółki. Systemy i Technologie Informatyczne Viskase stanowią własność Viskase. Z systemów tych należy korzystać dla potrzeb biznesowych w celu zaspokojenia interesów Spółki.

Viskase dąży do ochrony swoich pracowników oraz Spółki przed zamierzonymi i niezamierzonymi bezprawnymi oraz szkodliwymi działaniami innych osób. Zapewnienie skutecznej ochrony stanowi wysiłek zespołu wspieranego przez każdego pracownika lub współpracownika Spółki, który ma do czynienia z danymi lub systemami informatycznymi. Viskase wdrożył polityki i procedury celem ochrony poufności, spójności i dostępności infrastruktury, sieci oraz zasobów teleinformatycznych. W ramach wspierania tych starań, Viskase zastrzega sobie prawo, w granicach dozwolonych właściwymi przepisami prawa, objęcia w posiadanie, uzyskania dostępu, przeglądania, monitorowania, przechwytywania oraz prowadzenia nadzoru wszelkich treści i materiałów znajdujących się w obiektach Viskase, sieci Viskase lub na urządzeniu wydany przez Viskase. Dla uniknięcia wątpliwości, taki dostęp, przeglądanie, monitoring oraz nadzór nie obejmą prywatnych wiadomości e-mail pracownika ani prywatnych dokumentów, do których dostęp uzyskuje się za pośrednictwem i które zapisywane są na sieci Viskase lub na urządzeniu wydany przez Viskase. Dalsze informacje na temat monitoringu można znaleźć w ustępach 8-11 poniżej.

Wszyscy użytkownicy Systemów i Technologii Informatycznych Viskase mają obowiązek zapoznać się z niniejszą polityką i stosować się do jej postanowień. Spółka zastrzega sobie prawo dokonywania zmian niniejszej polityki w dowolnym momencie. Informacje o zmianach polityki będą zamieszczane na portalu internetowym Spółki.

2. CEL

Celem niniejszej polityki jest zapewnienie przejrzystości procesu przetwarzania danych osobowych pracowników oraz właściwego wykorzystania technologii, działania zgodnie z odpowiednimi przepisami prawa oraz ochrony pracowników i Viskase. Nieodpowiednie korzystanie stwarza ryzyka dla Spółki, takie jak ataki wirusów, pogorszenie wydajności systemów sieciowych i usług oraz inne utrudnienia.

3. ZAKRES

Niniejszą politykę stosuje się do pracowników, funkcjonariuszy, doradców, personelu tymczasowego oraz innych osób pracujących dla Viskase i jej spółek zależnych, jak również do wszystkich członków personelu współpracujących z podmiotami trzecimi, które wykorzystują Systemy i Technologie Informatyczne Viskase, oraz podmiotów przetwarzających dane osobowe pracowników Viskase. Niniejszą politykę stosuje się do wszelkich urzędzeń, których Viskase jest właścicielem lub najemcą, jak również do urzędzeń, których właścicielami lub najemcami są osoby objęte niniejszą polityką w zakresie, w jakim urzędzenia są wykorzystywane w sprawach Spółki. Viskase udostępni niniejszą politykę wszystkim nowym pracownikom.

4. OCHRONA DANYCH OSOBOWYCH

W celu uzyskania dalszych informacji na temat danych osobowych przetwarzanych przez Viskase, które dotyczą pracowników, jak również praw przysługujących pracownikom z tytułu takiego przetwarzania, prosimy o zapoznanie się z Informacją Viskase o Ochronie Danych Osobowych.

Viskase przetwarza dane osobowe, które dotyczą pracowników, rozumiane jako wszelkie dane bezpośrednio lub pośrednio identyfikujące pracownika. Viskase przetwarza następujące kategorie danych osobowych dotyczących pracowników:

- Dane identyfikujące osobę oraz jej adres;
- Środki komunikowania się i dane kontaktowe;
- Dane dotyczące wykształcenia i doświadczenia;
- Dane związane z zatrudnieniem;
- Dane związane z rodziną, stylem życia i sytuacją społeczną;
- Dane finansowe, ekonomiczne i ubezpieczeniowe;
- Dane techniczne istotne z uwagi na zarządzanie technologiami informatycznymi.

Viskase przetwarza dane dotyczące stanu zdrowia pracowników, którzy nie wykonują pracy z uwagi na chorobę lub kontuzję. Viskase przetwarza również dane dotyczące członkostwa pracowników w związkach zawodowych i radach pracowniczych. Dane osobowe należące do powyższych kategorii zalicza się do wrażliwych danych osobowych.

Viskase dąży do przetwarzania danych jedynie w oznaczonych celach związanych z przetwarzaniem, o czym informuje zainteresowanych pracowników z chwilą zebrania ich danych osobowych. Viskase prowadzi pisemny rejestr przetwarzania danych, który zawiera wykaz kategorii przetwarzanych danych.

Viskase przetwarza dane pracowników na następujących podstawach:

- Przetwarzanie jest niezbędne do spełnienia przez Viskase obowiązków wynikających z przepisów prawa;
- Przetwarzanie jest niezbędne w celu zaspokojenia uzasadnionych interesów Spółki; oraz
- Przetwarzanie jest niezbędne w celu spełnienia obowiązków wynikających z umowy.

Wrażliwe dane osobowe pracowników są przetwarzane przez Viskase na następujących podstawach:

- Przetwarzanie jest niezbędne do spełnienia przez Viskase ciężących na niej prawnych obowiązków lub wykonywania praw wynikających z przepisów prawa pracy;
- Przetwarzanie jest niezbędne z uwagi na istotny interes publiczny;
- Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń;
- Przetwarzanie jest niezbędne dla potrzeb programów medycyny prewencyjnej lub medycyny pracy, oceny zdolności pracowników do pracy, dokonywania diagnoz medycznych, świadczenia pomocy społecznej lub leczniczej lub zarządzania systemami opieki zdrowotnej lub społecznej oraz usługami w oparciu o prawo Unii Europejskiej, prawo kraju członkowskiego UE lub umowę z pracownikiem ochrony zdrowia
- Udzielili Państwo wyraźnej zgody na przetwarzanie odpowiednich Wrażliwych Danych Osobowych przez Viskase.

Pracownicy mogą żądać uzyskania dostępu, sprostowania lub usunięcia ich danych osobowych. Pracownicy mogą również żądać przeniesienia danych jeżeli dane są przetwarzane na podstawie umowy pomiędzy podmiotem danych i Viskase, podmiot danych przekazał dane Viskase oraz dane są przetwarzane automatycznie. Pracownicy mogą korzystać ze swoich praw poprzez złożenie wniosku do swojego przełożonego na piśmie. Wnioski te zostaną przekazane do głównego specjalisty ds. zgodności Viskase (*Chief Compliance Officer*). Spółka rozpatrzy wniosek pracownika w ciągu dwóch miesięcy.

Viskase zatrzyma dane osobowe pracownika przez okres pięciu lat po odejściu pracownika z pracy lub przez dłuższy okres, jeżeli będzie to wymagane przepisami lokalnymi (np. dla potrzeb podatkowych lub rachunkowych), oraz jedynie na okres niezbędny, na który dane osobowe zostały zebrane. Viskase dokona zniszczenia danych osobowych, jak również wszystkich kopii znajdujących się w systemach informatycznych, po upływie okresu zatrzymania danych.

Dane osobowe pracowników mogą być przechowywane i przetwarzane poza granicami Europejskiego Obszaru Gospodarczego (EOG) lub w Stanach Zjednoczonych. W takich przypadkach dane zostaną przekazane na podstawie Wewnętrzgrupowego Porozumienia o Transferze Danych lub standardowych klauzul umownych. Mogą Państwo otrzymać egzemplarz odpowiedniego dokumentu kontaktując się z Panem Douglas Ochab, Chief Compliance Officer, pod numerem telefonu: +1-630-874-0767 lub wysyłając wiadomość na adres e-mail: Compliance.Officer@viskase.com.

5. OGÓLNE KORZYSTANIE I PRAWO WŁASNOŚCI

1. Stanowisko pracy pracownika, jego komputer, adres e-mail, urządzenie mobilne oraz system dostępu do Internetu stanowią własność Spółki. Użytkownicy powinni być świadomi faktu, że dane, które tworzą na systemach firmowych, pozostają własnością Viskase.
2. Sporadyczne korzystanie w celach osobistych jest dopuszczalne, jednakże pracownicy ponoszą odpowiedzialność za dokonywanie prawidłowych osądów w zakresie zasadności takiego korzystania. W razie wątpliwości, pracownicy powinni zasięgnąć porady swoich przełożonych lub kadry zarządzającej.
3. W celu zapewnienia bezpieczeństwa i utrzymania sieci, osoby upoważnione przez Viskase mogą w dowolnym momencie monitorować korzystanie z urządzeń, systemów i sieci. Czynności monitorujące, o których mowa powyżej, nie obejmą prywatnych danych pracownika (w tym między innymi prywatnych wiadomości e-mail i dokumentów), które są przechowywane lub do których dostęp uzyskiwany jest za pośrednictwem urządzeń i systemów należących do Viskase. Więcej informacji na temat czynności monitorujących znajduje się w ustępach 8-11 poniżej.
4. Dostęp do Systemów i Technologii Informatycznych Viskase kończy się w ostatnim dniu zatrudnienia, chyba że dalszy dostęp zostanie zatwierdzony przez przełożonego pracownika w niezbędnych celach biznesowych, zaś informacja o udzieleniu takiego dostępu zostanie przekazana działowi Human Resources.
5. Jeżeli współpracownik (w tym doradcy, personel tymczasowy, stażyści oraz usługodawcy będący podmiotami trzecimi) zrezygnuje ze świadczenia usług, umowa łącząca go z Viskase ulegnie rozwiązaniu lub współpracownik zakończy wykonywanie zadań tymczasowych, przełożony będący pracownikiem Spółki musi wyznaczyć ostatni dzień ich dostępu do Systemów i Technologii Informatycznych Viskase, w tym adresu e-mail. Zaleca się, by ostatnim dniem dostępu był ostatni dzień świadczenia pracy. Przełożony ma obowiązek poinformowania działów informatycznego i Human Resources o wszelkich zmianach.

6. DOZWOLONE KORZYSTANIE

Korzystanie z Systemów i Technologii Informatycznych Viskase oraz podłączanie urządzeń do sieci wymaga autoryzacji. Autoryzacje są powiązane z kontami chronionymi hasłem. Dane te mają charakter wysoce poufny i nie mogą być, z wyjątkiem grupy korzystającej ze wspólnej stacji roboczej, przekazywane osobom trzecim, choćby tymczasowo. Jeżeli niezbędne jest wsparcie informatyków, użytkownik może przekazać swoje hasło działowi informatycznemu. Autoryzacje takie mogą zostać w każdej chwili wycofane. Każda autoryzacja wygasa w momencie zakończenia wykonywania czynności służbowych.

Powyższe ustawienia są zastrzeżone dla każdego użytkownika i muszą być zachowane w poufności.

Pracownicy muszą przestrzegać poniższych zasad bezpieczeństwa. Poniższy wykaz nie jest wyczerpujący.

1. Powiadom dział informatyczny Viskase o każdym rzeczywistym lub domniemanym naruszeniu lub próbie naruszenia konta w sieci oraz, ogólnie, o każdym przypadku nieprawidłowego działania.

2. Nigdy nie udostępniaj swojej nazwy użytkownika ani hasła.
3. Nigdy nie pytaj współpracownika o jego nazwę użytkownika lub hasło.
4. Nie przechowuj swojej nazwy użytkownika ani hasła w systemie, podawaj je w całości jedynie z chwilą uzyskiwania dostępu do systemu.
5. Nie używaj nazwy użytkownika ani hasła należących do innego użytkownika.
6. Nie ukrywaj swojej prawdziwej tożsamości.
7. Nie posługuj się tożsamością innej osoby.
8. Nie zmieniaj ustawień stacji roboczej.
9. Nie pobieraj oprogramowania bez autoryzacji.
10. Nie sporządzaj kopii, nie zmieniaj ani nie niszczyć oprogramowania będącego własnością Viskase.
11. Z chwilą opuszczania stacji roboczej, wyloguj się lub zablokuj komputer
12. Nie uzyskuj dostępu, nie próbuj uzyskać dostępu ani nie usuwaj lub zmieniaj danych, które Ciebie nie dotyczą.

7. NIEDOZWOLONE KORZYSTANIE

Działania wymienione poniżej są co do zasady zakazane. Istnieje możliwość wyłączenia pracownika spod poniższych ograniczeń z uwagi na uzasadnione obowiązki służbowe (np. personel zarządzający systemami może wstrzymać dostęp do sieci komputera głównego jeżeli powoduje on zakłócenia w dostarczaniu usług).

Pracownik Viskase Companies Inc. nie może w żadnym wypadku podejmować jakichkolwiek działań sprzecznych z przepisami obowiązującego prawa z wykorzystaniem zasobów będących własnością lub pozostających pod zarządem Viskase.

Poniższy wykaz nie jest wyczerpujący, ale zawiera ogólne wskazania co do działań stanowiących przejawy niedozwolonego korzystania.

Poniższe działania są bezwzględnie zakazane:

1. Pobieranie oraz instalacja oprogramowania, plików typu *shareware*, jak również innych programów bez uprzedniej zgody działu informatycznego. Zakaz obejmuje między innymi wygaszacze ekranu, komunikatory internetowe oraz inne programy, które nie są niezbędne do prowadzenia działalności gospodarczej przez Spółkę.
2. Naruszenie praw jakiejkolwiek osoby lub spółki, które podlegają ochronie z tytułu praw autorskich, tajemnicy przedsiębiorstwa, patentu, prawa własności intelektualnej, oraz podobnych przepisów lub regulacji, w tym między innymi instalacja lub dystrybucja "pirackiego" oprogramowania bądź innego oprogramowania, co do którego Viskase nie posiada odpowiedniej licencji na użytkowanie.
3. Sporządzanie nieautoryzowanych kopii materiału chronionego prawem autorskim, w szczególności digitalizacja i dystrybucja fotografii pochodzących z czasopism, książek i innych publikacji objętych prawem autorskim, muzyki chronionej prawem autorskim, jak

również instalacja oprogramowania objętego prawem autorskim, co do którego Viskase lub użytkownik końcowy nie posiada odpowiedniej licencji na użytkowanie.

4. Eksport oprogramowania, danych technicznych, oprogramowania szyfrującego lub technologii w sposób naruszający przepisy prawa eksportowego. Przed dokonaniem eksportu takich materiałów należy skonsultować się z członkami kadry zarządzającej Spółki.
5. Wprowadzanie szkodliwych programów do sieci lub na serwer (np. wirusów, robaków, koni trojańskich, bomb pocztowych (*e-mail bomb*), etc.).
6. Korzystanie z systemów lub urządzeń należących do Viskase w celu uzyskiwania lub przekazywania materiałów, które naruszają postanowienia firmowych polityk i przepisów prawa chroniących przed molestowaniem seksualnym i wrogością w miejscu pracy.
7. Składanie nieuczciwych ofert produktów, artykułów lub usług.
8. Dopuszczanie się naruszeń zasad bezpieczeństwa lub zakłócanie komunikacji sieciowej. Naruszenia bezpieczeństwa obejmują między innymi uzyskiwanie dostępu do danych nieprzeznaczonych dla pracownika lub logowanie się na serwer lub konto bez wyraźnej autoryzacji, chyba że czynności te należą do zakresu normalnych obowiązków służbowych pracownika. W rozumieniu niniejszego ustępu, "zakłócenie" obejmuje między innymi przeszukiwanie sieci (*network sniffing*), zalewanie wiadomościami ping (*pinged floods*), podszywanie się (*packet spoofing*), ataki typu "odmowa dostępu" (*denial of service*) oraz fałszywe trasowanie danych (*forged routing information*) w złych celach.
9. Skanowanie portów lub skanowanie systemu bezpieczeństwa bez uprzedniego zezwolenia działu informatycznego.
10. Prowadzenie czynności monitorujących sieć w jakikolwiek sposób, w celu przechwycenia danych nieprzeznaczonych dla komputera głównego pracownika, chyba że działania takie należą do normalnych obowiązków służbowych pracownika.
11. Obchodzenie systemu uwierzytelniającego użytkownika lub system bezpieczeństwa jakiegokolwiek komputera głównego, systemu lub konta.
12. Zakłócanie lub uniemożliwianie korzystania z usług przez jakiegokolwiek pracownika (na przykład przeprowadzenie ataku typu "odmowa dostępu" (*denial of service*)).
13. Korzystanie z programu//skryptu/polecenia lub wysyłanie wiadomości jakiegokolwiek rodzaju w celu zakłócenia lub zakończenia sesji terminalowej użytkownika, w jakikolwiek sposób, lokalnie lub za pomocą systemów Internet/Intranet/Extranet.
14. Przekazywanie informacji na temat pracowników Viskase lub ich wykazów osobom i podmiotom spoza Viskase.

8. ZASADY UZYSKIWANIA DOSTĘPU DO INTERNETU

Internet, w tym również media i serwisy społecznościowe, stanowi istotne narzędzie biznesowe udostępniane pracownikom w celu usprawnienia procesu wyszukiwania i gromadzenia informacji. Możliwość uzyskania dostępu do Internetu za pośrednictwem sieci komputerowej należącej do Spółki ma w zamierzeniu być wykorzystywana w celach biznesowych, nie osobistych. Wysyłanie, wyświetlanie, pobieranie lub drukowanie obraźliwych wiadomości, zdjęć pornograficznych lub o wyraźnie seksualnym charakterze, oraz materiałów uwłaczających na tle religijnym lub rasowym stanowią niedopuszczalne korzystanie z Internetu.

Pracownicy muszą zdawać sobie sprawę, że w przypadku elektronicznych "odwiedzin" strony internetowej z lub za pośrednictwem sieci komputerowej Spółki, firma Spółki widnieje jako inicjator danej wiadomości lub "wizyty". Korzystanie z zasobów Spółki w celu odwiedzania stron mogących wpłynąć negatywnie na firmę i reputację Spółki w otoczeniu jest zakazane.

Ze względów bezpieczeństwa i etyki, dostęp do określonych stron może być ograniczony lub zablokowany przez dział informatyczny, który wykorzystuje konfiguracje ustawień przeglądarki oraz instaluje mechanizmy filtrujące celem ograniczenia dostępu do takich stron.

Spółka rejestruje aktywność swoich pracowników w Internecie. Rejestrowane dane mogą być wykorzystywane dla celów statystycznych, nadzorczych i weryfikacyjnych w granicach obowiązującego prawa. Więcej informacji na temat monitorowania znajduje się w ustępie 11 poniżej.

9. ZASADY KORZYSTANIA Z ADRESU E-MAIL

W niniejszym ustępie opisane zostały zasady uzyskiwania dostępu oraz ujawniania wiadomości e-mail wysyłanych lub odbieranych przez pracowników, doradców, personel tymczasowy oraz inne osoby pracujące dla Viskase oraz jej spółki zależne oraz wszystkich współpracowników podmiotów trzecich, które wykorzystują systemy należące do Spółki lub jej usługi. Opisane zostały tutaj także zasady odpowiedniego korzystania z systemu poczty elektronicznej e-mail, który Spółka zapewnia w celach biznesowych. Poniższe zasady stosuje się do wiadomości wysyłanych z wykorzystaniem tego systemu oraz wiadomości wysyłanych lub odbieranych zdalnie z wykorzystaniem tego systemu jako punktu źródłowego, punktu odbioru lub punktu pośredniego. Wszelkie pytania dotyczące niniejszych zasad należy kierować do głównego specjalisty ds. zgodności (*Chief Compliance Officer*). Spółka zastrzega sobie prawo dokonywania zmian niniejszych zasad w dowolnym momencie.

1. Spółka zdaje sobie sprawę, że pracownicy mogą mieć potrzebę załatwiania spraw osobistych w godzinach pracy oraz, że w dobie komunikacji elektronicznej korzystanie z poczty elektronicznej e-mail dla prowadzenia komunikacji osobistej może okazać się konieczne. W związku z powyższym, sporadyczne korzystanie z systemu e-mail Spółki w sprawach osobistych jest dopuszczalne. Dopuszczeniem nie są objęte przypadki korzystania wymagające znaczących nakładów czasu, korzystanie w celach zarobkowych ani korzystanie naruszające politykę Spółki. Wiadomości e-mail muszą być ściśle zgodne z ograniczeniami wynikającymi ze wszystkich postanowień niniejszej polityki. W możliwie najszerszym zakresie, pracownicy powinni dążyć do korzystania z własnych prywatnych kont e-mail w celach osobistych, nie zaś z systemu e-mail należącego do Spółki.
2. Wiadomości e-mail nie powinny zawierać treści, które mogą być szkodliwe, zawstydzające lub sprzeczne z którąkolwiek z polityk lub zasad Spółki. W szczególności, Spółka bezwzględnie zakazuje rozpowszechniania wiadomości e-mail, które są nieodpowiednie lub obraźliwe, w tym zwłaszcza wiadomości o charakterze seksualnym, rasowym, pornograficznym lub nękającym. Ponadto, nie należy wykorzystywać wiadomości e-mail w celu prowadzenia agitacji politycznej, kampanii ani w innych celach politycznych. Wysyłanie obraźliwych wiadomości stanowi podstawę do zwolnienia ze skutkiem natychmiastowym. Jeżeli otrzymają Państwo nieodpowiednią wiadomość, prosimy o kontakt z działem kadr (Human Resources).

3. Spółka ma prawo uzyskania dostępu lub ujawnienia wiadomości elektronicznych lub plików pracownika (nieoznaczonych wyraźnie jako prywatne), w tym wszelkich plików na dysku twardym, w następujących celach: zapewnienie bezpieczeństwa systemu, wypełnianie obowiązków ciążących na Spółce, wykrywanie wykroczeń pracowników, stosowanie się do procedur prawnych oraz ochrona praw i własności Spółki. Spółka zastrzega sobie prawo ujawniania wszelkich wiadomości elektronicznych lub plików (nieoznaczonych wyraźnie jako prywatne) organom stosującym prawo oraz innym podmiotom trzecim mającym interes w takim ujawnieniu, bez obowiązku uprzedniego powiadomienia o tym fakcie pracownika i innych zainteresowanych stron. Spółka doloży najwyższych starań, by ujawnieniem nie zostały objęte dane osobowe pracownika, chyba że ujawnienie danych osobowych jest dozwolone lub wymagane właściwymi przepisami prawa.
4. Spółka zastrzega sobie prawo monitorowania wiadomości e-mail oraz innych plików elektronicznych tworzonych w dowolnym momencie przez pracowników. Dla uniknięcia wątpliwości, czynności monitorujące nie obejmą prywatnych wiadomości e-mail oraz plików elektronicznych, do których dostęp uzyskiwany jest lub które są przechowywane na, urządzeniach i systemach należących do Viskase. Więcej informacji na temat czynności monitorujących znajduje się w ustępie 11 poniżej.
5. Prowadzenie elektronicznych działań "szpiegujących" przez jakiegokolwiek pracownika stanowi naruszenie polityki Spółki i może być podstawą zwolnienia. Niezależnie od przysługującego Spółce prawa uzyskiwania dostępu do wiadomości, powinny być one utrzymywane w poufności przez pracowników i jedynie zamierzeni odbiorcy powinni mieć do nich dostęp. Pracownicy nie powinni odbierać ani zapoznawać się z wiadomościami poczty elektronicznej, które nie są wysyłane do nich bezpośrednio, chyba że zamierzony odbiorca udzielił uprzedniej zgody innej osobie lub innym osobom na uzyskanie dostępu do jego/jej poczty.
6. Pracownicy powinni zdawać sobie sprawę, że nawet w razie usunięcia wiadomości, w dalszym ciągu możliwe jest jej odzyskanie i odczytanie. Systemy obsługujące wiadomości, które są wyposażone w bramy do systemów zewnętrznych, są wysoce ryzykowne pomimo dążeń Spółki nakierowanych na zapewnienie bezpieczeństwa systemu.
7. Nie należy korzystać z systemu e-mail w celu prowadzenia działalności lobbingsowej popierającej konkretne rozwiązania legislacyjne, zabiegania o przedsięwzięcia komercyjne ani agitowania w celach religijnych lub politycznych.
8. Użytkownicy muszą przestrzegać wszystkich umów licencyjnych na oprogramowanie.
9. Systemu poczty elektronicznej e-mail nie należy wykorzystywać w celu naruszania praw autorskich lub innych praw własności intelektualnej przysługujących osobom trzecim, dystrybucji obraźliwych, fałszywych lub nękających wiadomości, ani w celu podejmowania innych bezprawnych lub szkodliwych działań.
10. W ramach ochrony systemów Spółki przed wirusami i robakami, system e-mail Spółki nie przyjmuje następujących formatów plików: .exe, .com, .bat, .vbs, .wsh, .pif, .lnk, .scr. Lista może być zmieniana w zależności od potrzeby.
11. Tworzenie lub przesyłanie "łańcuszków internetowych", wiadomości na temat schematów "Ponzi" lub innych "piramid" finansowych jakiegokolwiek rodzaju jest ściśle zakazane.

10. ZASADY KORZYSTANIA Z TELEFONÓW

Viskase może wyposażać pracowników w komputer stacjonarny lub przenośny oraz telefon komórkowy, smartfon lub tablet do wykorzystania w toku wykonywania obowiązków służbowych. Urządzenia należące do Spółki mają w zamierzeniu być wykorzystywane w celach biznesowych, nie osobistych. Powyższe zasady stosuje się do korzystania z telefonów komórkowych oferujących dostęp do Internetu i poczty e-mail. Wiadomości tekstowych należy używać wyłącznie w celu prowadzenia korespondencji służbowej.

Viskase rejestruje częstotliwość połączeń telefonicznych (z wyłączeniem treści połączeń) wykonywanych za pośrednictwem telefonów stacjonarnych i komórkowych będących własnością Viskase. Rejestrowane dane są wykorzystywane dla celów statystycznych, nadzorczych i weryfikacyjnych, w granicach przepisów obowiązującego prawa. Viskase uzyska dostęp do numerów telefonów wybieranych przez pracowników, dokona jednak ich identyfikacji wyłącznie w przypadku wdania się w prawny spór z pracownikiem.

11. ŚRODKI MONITOROWANIA STOSOWANE PRZEZ VISKASE

Viskase wdrożył, zgodnie z przepisami obowiązującego prawa, szereg polityk i procedur celem ochrony poufności, spójności i dostępności infrastruktury, sieci oraz zasobów teleinformatycznych Viskase. W ramach wspierania tych starań, Viskase zastrzega sobie prawo, w granicach dozwolonych właściwymi przepisami prawa, objęcia w posiadanie, uzyskania dostępu, przeglądania, monitorowania, przechwytywania oraz prowadzenia nadzoru wszelkich treści lub danych znajdujących się w obiektach Viskase, jakimkolwiek systemie Viskase, lub przesyłanych za pośrednictwem sieci Viskase. Na przykład, monitorowanie, o którym mowa powyżej, obejmuje korzystanie przez pracownika z Internetu, konta e-mail oraz telefonu zgodnie z postanowieniami ustępów 8-10 powyżej. Dla uniknięcia wątpliwości, uzyskiwanie dostępu, przeglądanie, monitoring oraz nadzór, o których mowa powyżej, nie obejmą prywatnych wiadomości e-mail pracownika ani prywatnych dokumentów, do których dostęp uzyskuje się za pośrednictwem i które zapisywane są na sieci Viskase lub na urządzeniu wydanym przez Viskase.

Czynności monitorujące mogą być prowadzone z różnych przyczyn, w tym między innymi w celu zapewnienia zgodności z polityką i procedurami Viskase, dochodzenia przestępstw oraz utrzymania i ochrony Systemów i Technologii Informatycznych Viskase. Czynności monitorujące będą prowadzone zawsze zgodnie z obowiązującymi lokalnie przepisami ustaw i rozporządzeń. Dział informatyczny Viskase prowadzi dochodzenia niezbędne do rozwiązywania wszelkich problemów wynikłych w systemie informatycznym lub którymkolwiek z jego komponentów, które mogłyby negatywnie wpłynąć na jego funkcjonowanie lub spójność. Dane są wykorzystywane jedynie w tym celu, jak również podlegają usunięciu po upływie 12 miesięcy.

Dział informatyczny wykorzystuje w powyższym celu pliki dziennika systemowego, które zawierają wykaz wszystkich połączeń i prób połączeń z systemem informatycznym. Pliki te zawierające następujące dane: daty, stacje robocze oraz przedmiot zdarzenia.

Dział informatyczny Viskase ma możliwość uzyskania zdalnego dostępu do wszystkich stacji roboczych. Dział informatyczny uzyska dostęp do stacji roboczej wyłącznie za wyraźną zgodą użytkownika. W kontekście dokonywania aktualizacji i modernizacji systemu informatycznego, oraz kiedy żaden użytkownik nie jest podłączony do stacji roboczej, dział informatyczny może

ingerować w otoczenie techniczne stacji roboczych, ale nie może uzyskiwać dostępu do zawartości takich stacji roboczych.

Mogą zaistnieć okoliczności, w których upoważniony pracownik Viskase uzyska dostęp lub będzie monitorował stację roboczą - włącznie z danymi tam przechowywanymi oraz dotyczącymi korzystania z Państwa komputera, systemów lub urządzeń należących do Viskase - w celu zapewnienia ochrony pozostałym użytkownikom lub w innych przypadkach, kiedy będzie to, w ocenie kadry zarządzającej, odpowiednie i proporcjonalne, w sposób zgodny z właściwymi przepisami ustaw i rozporządzeń, na przykład celem zapobiegania naruszeniom bezpieczeństwa cybernetycznego oraz w celu utrzymania i ochrony Systemów i Technologii Informatycznych Viskase. Monitoring nie obejmie danych prywatnych (w tym między innymi prywatnej korespondencji e-mail oraz dokumentów) przechowywanych na komputerze pracownika, systemach lub urządzeniach należących do Viskase.

Dla celów bezpieczeństwa, wejścia do naszych obiektów są monitorowane przez kamery telewizji przemysłowej CCTV.

12. DANE UDOSTĘPNIANE PRZEZ VISKASE PODMIOTOM TRZECIM

Zgodnie z właściwymi przepisami prawa, Viskase może powierzać dane pozyskane w toku prowadzenia czynności monitorujących podmiotom trzecim, w tym regulatorom i organom stosującym prawo.

Możemy również udostępniać Państwa dane usługodawcom będącym podmiotami trzecimi, którzy świadczą usługi i oferują funkcjonalności w celu usprawnienia naszej działalności i zgodnie z postanowieniami niniejszej polityki, w tym między innymi usługi kadrowe (*human resources*) i kadrowo-płacowe (*payroll*), czynności monitorujące, zbieranie danych, sprawozdawczość oraz usługi analityczne. Dane osobowe pracowników mogą być również udostępniane doradcom prawnym Viskase celem uzyskania porady prawnej i ochrony praw Viskase.

13. NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Naruszenie ochrony danych osobowych stanowi naruszenie bezpieczeństwa prowadzące do przypadkowego bądź bezprawnego zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia, uzyskania dostępu do przesyłanych, przechowywanych lub przetwarzanych danych osobowych. Pracownicy powinni informować swoich przełożonych z chwilą powzięcia wiadomości o potencjalnym lub faktycznym naruszeniu danych osobowych.

14. ZASADY ZACHOWYWANIA WIADOMOŚCI E-MAIL

Dział informatyczny wdrożył politykę zachowywania wiadomości e-mail, by przechowywać wiadomości e-mail bez nadmiernego obciążania firmowego serwera. Zasady te mogą być zmieniane bez konieczności przekazywania uprzedniej informacji o tym fakcie pracownikom Spółki.

By zachować rozsądny rozmiar aktywnych skrzynek poczty elektronicznej, wobec obecnych pracowników stosuje się następujące zasady zachowywania wiadomości e-mail:

Folder	Okres zachowania	Kiedy
Wszystkie pozycje w skrzynce odbiorczej	10 lat	Automatycznie (z chwilą przetrzymywania wiadomości przez okres 10 lat)
Pozycje usunięte	30 dni	Automatycznie (po 30 dniach od usunięcia pozycji)
Kalendarz	Nie podlega usunięciu	Nie dotyczy
Kontakty	Nie podlega usunięciu	Nie dotyczy

1. Serwer poczty elektronicznej Exchange jest wspierany wyłącznie w zakresie odzyskiwania danych w przypadku awarii; nie jest możliwe odzyskanie poszczególnych skrzynek poczty elektronicznej ani wiadomości e-mail w razie ich usunięcia.
2. Spółka nie prowadzi archiwizacji wiadomości e-mail poza serwerem poczty elektronicznej Exchange; z tego powodu wszelkie pliki PST oraz archiwa wiadomości e-mail są usuwane z serwerów, komputerów stacjonarnych i przenośnych, które należą do Spółki.
3. Spółka wyraźnie zakazuje pobierania wiadomości e-mail na komputery osobiste, napędy flash oraz inne nośniki wymienne.
4. Spółka zachowuje prawo zawieszenia obowiązywania zasad zachowywania wiadomości e-mail w celu zatrzymania informacji, które Spółka jest zobowiązana zachować w związku z prowadzonym dochodem lub postępowaniem sądowym.

15. ODEJŚCIE PRACOWNIKA

W przypadku rozwiązania stosunku zatrudnienia z pracownikiem Viskase, dział kadr (Human Resources) poinformuje dział informatyczny o dniu odejścia pracownika. Wyboru dnia zamknięcia konta pracownika dokona, na wniosek działu Human Resources, przełożony odchodzącego pracownika, który przekaze swoją decyzję działowi informatycznemu. Zamknięcie konta użytkownika nie może przypaść przed dniem rozwiązania stosunku zatrudnienia ze Spółką.

Z chwilą odejścia ze Spółki, pracownik zostanie poinformowany o zbliżającym się zamknięciu jego konta użytkownika. Jeżeli pracownik jest w posiadaniu urządzeń należących do Viskase, a które zostały pracownikowi udostępnione wyłącznie do użytku na potrzeby wykonywania czynności służbowych, w tym między innymi komputera przenośnego lub telefonu komórkowego, pracownik powinien zwrócić wszystkie takie urządzenia w dniu faktycznego odejścia. Pracownik dokona usunięcia dokumentów osobistych i danych prywatnych. Konta oraz dane osobowe pracownika zostaną usunięte w ciągu roku od dnia jego odejścia. Zatrzymanie przez pracownika kopii jakichkolwiek dokumentów służbowych wymaga zgody kierownika działu.

Jeżeli stosunek zatrudnienia pracownika zostaje rozwiązany przez Viskase ze skutkiem natychmiastowym i pracownik ma obowiązek niezwłocznego opuszczenia obiektu Viskase, dział Human Resources poinformuje o tym dział informatyczny. Dział informatyczny dokona natychmiastowej zmiany hasła do konta pracownika i ograniczy do niego dostęp, utrzymując go jedynie dla przełożonego zwalnianego pracownika. Dla nadawców wiadomości e-mail skierowanych do pracownika zostanie ustawiona automatyczna odpowiedź informująca o tym,

że odbiorca nie jest już pracownikiem Viskase. Konto pracownika pozostanie aktywne tak długo, jak długo jest to konieczne dla zapewnienia ciągłości działania oraz ochrony sytuacji prawnej Viskase w razie wniesienia przez pracownika lub podmiot trzeci roszczenia przeciwko Viskase. W tym okresie przełożony pracownika uzyska dostęp do plików znajdujących się na koncie pracownika jedynie w celach opisanych powyżej, lub w odpowiedzi na skorzystanie przez pracownika z jego praw jako podmiotu danych. Po zakończeniu tego okresu, konto użytkownika należące do zwolnionego pracownika oraz jego dane osobowe zostaną usunięte.

16. EGZEKWOWANIE POLITYKI

Wobec osób naruszających postanowienia niniejszej polityki stosowane będą środki dyscyplinarne, włącznie z rozwiązaniem stosunku zatrudnienia lub innej podstawy współpracy ze Spółką.

17. KONTAKT

Pracownicy powinni zgłaszać pytania związane z niniejszą polityką do głównego specjalisty ds. zgodności Viskase (*Viskase Chief Compliance Officer*) (Compliance.Officer@viskase.com).