|  |  |
| --- | --- |
|  | **⚫SUPLEMENT CHMUROWY** |
| Data ostatniej aktualizacji: . |
|  |
|  |
| **Przeznaczenie Suplementu** |

**§ 1. INFORMACJE OGÓLNE**

1. Niniejszy Suplement (definicja: **Suplement**) do Regulaminu znajduje zastosowanie jako uzupełnienie postanowień Regulaminu **w przypadku Klientów, wobec których Vercom świadcząc określone Usługi, pełni rolę dostawcy usług chmury obliczeniowej** w rozumieniu Komunikatu Urzędu Komisji Nadzoru Finansowego dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z dnia 23 stycznia 2020 roku, wraz ze wszelkimi zmianami (definicja: **Komunikat**).
2. W przypadku, gdy znajduje on zastosowanie stosownie do postanowień ust. 1 powyżej, niniejszy Suplement stanowi integralną część Regulaminu.
3. Niniejszy Suplement znajduje zastososwanie odpowiednio do Usługi Redlink oraz Ussługi EMAILLABS, w zależności od tego, z której Usługi Klient korzysta.
4. Klient w ramach korzystania z Usług(i) przetwarza w chmurze obliczeniowej informacje prawnie chronione w rozumieniu Komunikatu, w szczególności dane osobowe klientów Klienta, które stanowią tajemnicę prawnie chronioną i w związku z tym w zakresie tych informacji Vercom akceptuje, że Klient jest zobowiązany spełnić wymogi Komunikatu oraz zawiadomić Komisję Nadzoru Finansowego („KNF”) o outssourcingu chmury obliczeniowej.
5. W zakresie niezbędnym i uzasadnionym treścią Komunikatu, Vercom zobowiązuje się stosować do wszelkich uzasadnionych wytycznych Klienta mających na celu spełnienie wymogów Komunikatu. W przypadku, gdy realizacja powyższych zaleceń Klienta wiązać się będzie z potrzebą poniesienia przez Vercom dodatkowych kosztów, koszty te obciążać będą Klienta.
6. Vercom oświadcza, że centrum przetwarzania danych (CPD) zlokalizowane jest w Polsce (Poznań) oraz w Niemczech (Berlin), natomiast centrum zapasowe znajduje się w na terenie EOG (Niemcy Frankfurt).
7. Vercom gwarantuje, że w ramach świadczenia usług wsparcia w zakresie odnoszącym się do chmury obliczeniowej informacje przetwarzane w chmurze będą przetwarzane wyłącznie na terenie EOG.
8. Vercom jest obowiązany powiadamiać Klienta, w terminach wynikających z Dokumentów Umownych, o planowanych do wprowadzenia zmianach lub aktualizacjach w usłudze chmury obliczeniowej obejmujących zmiany w interfejsie użytkownika, API, integracji, aktualizacji, strukturze danych lub fizycznej lokalizacji, jeśli powyższe zmiany w istotny sposób zmieniają funkcjonalność usług Vercom, wymagają wdrożenia po stronie Klienta lub wpływają na sposób lub bezpieczeństwo przetwarzania informacji w chmurze obliczeniowej.
9. Vercom zobowiązuje się do zapewnienia Klientowi możliwości migracji (pobrania) danych, w dowolnym terminie,
ze wszystkich usług chmury obliczeniowej do środowiska Klienta lub innego dostawcy usług chmury obliczeniowej. Vercom zobowiązuje się zapewnić, że format migrowanych danych z chmury obliczeniowej będzie pozwalał na ich zaimportowanie.
10. Vercom przechowuje dane nieobejmujące treści wiadomości email, a jedynie informacje o: adresie, temacie, statusie i dacie wysyłki, w formie kopii zapasowych (backup) przez okres dwóch lat od zakończenia świadczenia usługi, po tym okresie Vercom zobowiązuje się do usunięcia danych z całej infrastruktury. Dane opisane w zdaniu poprzednim szyfrowane są za pomocą standardu AES256.

**§ 2. EMAILLABS – ŚRODKI ZWIĘKSZAJĄCE BEZPIECZEŃSTWO: PANEL**

Platforma EMAILLABS zawiera następujące ustawienia zwiększające bezpieczeństwo korzystania z Usług świadczonych za jej pośrednictwem:

1. Logowanie do Panelu EMAILLABS możliwe jest wyłącznie ze zautoryzowanych adresów IP Klienta i ograniczone wyłącznie do tych adresów,
2. Realizacja wysyłek zleconych kampanii w ramach Usługi EMAILLABS poprzez API ograniczona jest wyłącznie do konkretnych, zautoryzowanych adresów IP;

**§ 3. EMAILLABS – ŚRODKI ZWIĘKSZAJĄCE BEZPIECZEŃSTWO WYSYŁEK: OPCJE DOSTĘPNE W PANELU**

1. Ograniczenie listy adresów, do których mogą prowadzić linki trackingowe w ramach danego Konta EMAILLABS – możliwość ustawienia tzw. autoryzowanych domen trackingowych,
2. Funkcja Link Tracking uwzględnia protokół SSL,
3. Funkcja Open Tracking uwzględnia protokół SSL,
4. Usługa EMAILLABS realizowana jest w oparciu o technologie oraz autoryzacje bazujące na SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) oraz DMARC (Domain-Based Message Authentication, Reporting & Conformance),
5. Usługa EMAILLABS może uwzględniać szyfrowanie wiadomości przy użyciu zabezpieczeń S/MIME

**§ 4. EMAILLABS – KLIENT: KONFIGURACJA ZWIĘKSZAJĄCA BEZPIECZEŃSTWO POŁĄCZENIA Z PLATFORMĄ**

W celu zwiększenia bezpieczeństwa połączenia pomiędzy środowiskiem Klienta a Platformą EMAILLABS zaleca się:

1. **W przypadku wysyłki przez SMTP:** używanie połączenia szyfrowanego TLS, co zwiększa bezpieczeństwo przesyłanych treści uniemożliwiając osobom postronnym (w szczególności hakerom) dostęp do przesyłanych informacji; w zależności od oprogramowania użytego do wysyłki, opcja ta może być domyślnie włączona lub może wymagać włączenia,
2. **W przypadku wysyłki przez API:** system wymusza korzystanie z protokołu HTTPS.

W obu przypadkach EMAILLABS umożliwia korzystanie z tunelu VPN.