# Polityka prywatności

1. Cel Polityki

Określenie zasad przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w przedsiębiorstwie prowadzonym w ramach Bring spółka z ograniczoną odpowiedzialnością w Warszawie (zwaną dalej Bring) przez pracowników i współpracowników, którzy przetwarzają dane osobowe, dla zapewnienia prawidłowej ochrony (bezpieczeństwa przetwarzania) danych osobowych przetwarzanych przez Bring przed ich udostępnieniem osobom nieuprawnionym, zmianą przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

2. Podstawa prawna

Polityka bezpieczeństwa przetwarzania danych osobowych w Bring (dalej: Polityka) zostaje wprowadzona na podstawie: 1. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135 z późn. zm.; dalej: Ustawa); 2. rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100/2004, poz. 1024, dalej: Rozporządzenie).

3. Zakres stosowania

Politykę stosuje się do danych osobowych przetwarzanych w systemie informatycznym, danych osobowych zapisanych na zewnętrznych nośnikach informacji oraz informacji dotyczących bezpieczeństwa przetwarzania danych osobowych, w szczególności dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych. Polityka obowiązuje wszystkich pracowników i współpracowników Bring oraz inne osoby mające dostęp do danych osobowych, w tym osoby świadczące usługi na rzecz Bring na podstawie umów zlecenia lub współpracujące na podstawie umów o dzieło.

4. Wymogi w zakresie bezpieczeństwa przetwarzania danych osobowych

Zapewnienie prawidłowej ochrony (bezpieczeństwa przetwarzania) danych osobowych wymaga spełnienia warunków:

• poufności —zapewnienia, że dane osobowe nie są udostępniane podmiotom nieuprawnionym;

• integralności — zapewnienia, że dane osobowe nie zostaną zmienione lub zniszczone w sposób niekontrolowany;

• rozliczalności — zapewnienia, że działania poszczególnych osób przetwarzających dane osobowe mogą być przypisane w sposób jednoznaczny tym osobom.

5. Poziom bezpieczeństwa przetwarzania danych osobowych

Z uwagi na połączenie urządzeń systemu służącego do przetwarzania danych osobowych z siecią publiczną przy przetwarzaniu danych osobowych należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia.

6. Administrator danych osobowych

Administratorem danych osobowych jest Bring spółka z ograniczoną odpowiedzialnością w Warszawie, z siedzibą przy ul. Mokotowskiej 57/6 (00-542 Warszawa) wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000678537, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, posiadającą NIP: 7010691914 oraz REGON: 3673296557, jest Alfred Chłapowski-Myjak, Prezes Zarządu uprawniony do samodzielnej reprezentacji spółki.

7. Dane osobowe

Przez dane osobowe rozumie się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

8. Osoby uprawnione do przetwarzania danych osobowych

Do przetwarzania danych osobowych uprawnieni są wyłącznie: Administrator danych osobowych, osoby posiadające upoważnienie wydane przez Administratora danych osobowych, osoby uprawnione na podstawie obowiązujących przepisów prawa.

9. Przetwarzanie danych osobowych

Przetwarzaniem danych osobowych są wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

10. Obowiązki Administratora danych osobowych

Do obowiązków Administratora danych osobowych należy:

• zrozumienie oraz zapewnienie świadomości bezpieczeństwa przetwarzania danych osobowych, jego problematyki oraz wymagań;

• nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie elektronicznej i papierowej;

Do obowiązków Administratora danych osobowych należy w szczególności:

• podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych, w tym określenie wymagań bezpieczeństwa przetwarzania danych osobowych;

• podział zadań i obowiązków związanych z organizacją ochrony danych osobowych;

• nadzór nad wdrożeniem środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych;

• doprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych;

• poddawanie przeglądom skuteczności polityki bezpieczeństwa przetwarzania danych osobowych;

• zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;

• zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym dla nich celu;

• zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych.

• prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych;

• w przypadku naruszenia zasad ochrony danych osobowych – analiza sytuacji, okoliczności i przyczyn, które doprowadziły do takiego naruszenia oraz przygotowanie wdrożenie zaleceń i rekomendacji dotyczących eliminacji przyczyn ich wystąpienia.

11. Obowiązki osób upoważnionych do przetwarzania danych osobowych

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa i przyjętymi regulacjami. Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy w szczególności: postępowanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych; zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia; ochrona danych osobowych oraz

środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem; informowanie o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe do Administratora danych osobowych; uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej.

12. Zarządzanie ochroną danych osobowych

12.1. Podstawowe zasady

1) Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych.

2) Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

3) Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.

4) Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.

5) Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.

6) Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

12.2. Upoważnienie do przetwarzania danych osobowych

1) Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 37 Ustawy.

2) Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora danych osobowych.

3) W celu upoważnienia do przetwarzania danych osobowych należy dostarczyć do Administratora danych osobowych podpisane oświadczenie, którego wzór stanowi załącznik nr 1 do Polityki.

4) Na podstawie otrzymanego oświadczenia Administrator danych osobowych udziela upoważnienia do przetwarzania danych osobowych i wydaje upoważnienie sporządzane wg wzoru stanowiącego załącznik nr 2 do Polityki.

5) Upoważnienia, o których mowa powyżej, przechowywane są w aktach osobowych pracownika i obowiązują do czasu ustania stosunku pracy lub obowiązków związanych z przetwarzaniem danych osobowych.

12.3. Ewidencja osób upoważnionych

Administrator danych osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Ewidencja zawiera w szczególności: - imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych; - zakres upoważnienia do przetwarzania danych osobowych; - identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych; - datę nadania i odebrania uprawnień.

12.4. Zachowanie danych osobowych w tajemnicy

Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

12.5. Znajomości regulacji wewnętrznych

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznać się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w Bring, w szczególności Polityką bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

12.6. Zgodność Polityki z obowiązującym prawem oraz strukturą organizacyjną Bring

Polityka powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Bring, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne. Okresowy przegląd Polityki powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Bring oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

13. Zarządzanie usługami zewnętrznymi

13.1. Bezpieczeństwo usług zewnętrznych

Należy zapewnić, aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych obowiązującymi w Bring, wymaganiami umowy oraz wymaganiami prawa. Wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić w umowie świadczenia usług. Należy zapewnić, aby użytkownicy nie będący pracownikami Bring stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych, co użytkownicy będący pracownikami.

13.2. Powierzanie przetwarzania danych osobowych

Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy. Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 31 i nast. Ustawy. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36-39a Ustawy. W umowach stanowiących podstawę powierzenia przetwarzania danych albo eksploatacji systemu informatycznego lub części infrastruktury, jeśli kontrahent będzie miał dostęp do danych osobowych w postaci umożliwiającej ich przetwarzanie, należy umieścić zobowiązanie podmiotu zewnętrznego do przestrzegania Polityki oraz zastosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności Bring za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa Bring do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa.

13.3. Udostępnianie danych osobowych

Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub udzielonej zgody oraz osobom, których dotyczą. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora danych osobowych. Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o udostępnieniu bezpośrednio w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

13.4. Monitorowanie i przegląd usług strony trzeciej

Monitorowanie usług strony trzeciej powinno być udokumentowane i powinno zawierać informacje o: poziomie wykonania usługi, incydentach bezpieczeństwa teleinformatycznego oraz ochrony danych osobowych, śladach audytowych, problemach operacyjnych, awariach, błędach i zakłóceniach.

14. Bezpieczeństwo fizyczne obszarów przetwarzania

Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Bring prowadzi działalność. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane

podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostępu do nich osobom nieuprawnionym.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku drzwi. Wydruki i nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.

Niepotrzebne wydruki lub inne dokumenty należy niszczyć za pomocą niszczarek.

Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.

Urządzenia służące do przetwarzania danych osobowych należy przechowywać w bezpieczny i nadzorowany sposób.

Klucze dostępowe, karty, hasła itd. służące do uzyskania dostępu do systemów informatycznych służących do przetwarzania danych osobowych należy zabezpieczać.

Kończąc pracę, należy zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację, wydruki, elektroniczne nośniki informacji i umieścić je w zamykanych szafkach.

W przypadku korzystania z usług zewnętrznych podmiotów oferujących zbieranie i niszczenie papierów, urządzeń lub nośników zwierających dane osobowe, należy wybrać wykonawcę z odpowiednimi zabezpieczeniami i doświadczeniem.

15. Ocena ryzyka i przeglądy

15.1. Ocena ryzyka

Systemy informatyczne i aplikacje powinny być poddawane ocenie ryzyka pod kątem identyfikacji zagrożeń dla bezpieczeństwa przetwarzania danych osobowych co najmniej raz na dwa lata. Ocena ryzyka powinna być również przeprowadzana przy dużych zmianach procesów biznesowych, systemów informatycznych i aplikacji. Narzędzia informatyczne służące do oceny ryzyka bezpieczeństwa przetwarzania danych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

15.2. Przeglądy bezpieczeństwa

Przeglądy bezpieczeństwa przetwarzania danych osobowych powinny być przeprowadzane okresowo, co najmniej raz na 2 lata, w celu określenia wymaganego poziomu zabezpieczeń pozwalającego na ograniczenie ryzyka do poziomu akceptowalnego. Przeglądy zgodności z zasadami bezpieczeństwa przetwarzania danych osobowych urządzeń informatycznych oraz sieci

teleinformatycznych należy przeprowadzać okresowo, co najmniej raz na rok. Narzędzia informatyczne służące do przeprowadzania przeglądów bezpieczeństwa przetwarzania danych osobowych powinny być chronione przed nieautoryzowanym lub nieuprawnionym dostępem a ich użycie odpowiednio kontrolowane.

16. Zarządzanie incydentami

16.1. Monitorowanie incydentów

Incydenty związane z bezpieczeństwem przetwarzania danych osobowych powinny być wykrywane, rejestrowane i monitorowane w celu ich zidentyfikowania i zapobiegania ich wystąpieniu w przyszłości. Zdarzenia systemowe powinny być przechowywane jako materiał dowodowy zaistniałych incydentów związanych z bezpieczeństwem przetwarzania danych osobowych. Użytkownicy systemów powinni znać i przestrzegać zasad zgłaszania incydentów związanych z bezpieczeństwem przetwarzania danych osobowych.

16.2. Zgłaszanie incydentów

Zaistniałe zdarzenia związane z naruszeniem lub podejrzeniem naruszenia bezpieczeństwa przetwarzania danych osobowych takie jak np. utrata integralności, niedostępność, awarie, uszkodzenia, ostrzeżenia i alarmy bezpieczeństwa systemów informatycznych, urządzeń teleinformatycznych oraz danych powinny być niezwłocznie zgłaszane do Administratora danych osobowych.

17. Postanowienia końcowe

Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy Ustawy oraz przepisy wykonawcze do niej.

Pracownicy Bring zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce, w wypadku odrębnych od zawartych w Polityce uregulowań występujących w innych procedurach obowiązujących w Bring, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

## Cookies

W celu podkreślenia znaczenia, jakie przypisujemy ochronie prywatności Użytkowników i poufności zamieszczanych przez nich danych oraz w związku z obowiązkiem udzielenia informacji dotyczącej wykorzystywania plików cookies, niniejszym przedstawiamy Państwu zasady przetwarzania danych osobowych udostępnianych w ramach korzystania z Serwisu Bring.

Informujemy, że administratorem danych osobowych gromadzonych w Serwisie Bring spółka z ograniczoną odpowiedzialnością w Warszawie, z siedzibą przy ul. Mokotowskiej 57/6 (00-542 Warszawa) wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000678537, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, posiadającą NIP: 7010691914 oraz REGON: 3673296557, jest Alfred Chłapowski-Myjak, Prezes Zarządu uprawniony do samodzielnej reprezentacji spółki.

Podanie przez Użytkownika dokonującego Rejestracji danych osobowych wskazanych w formularzu zgłoszeniowym jest dobrowolne, lecz niezbędne do dokonania rejestracji w Serwisie.

Dane osobowe Użytkowników przetwarzane są zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. Nr 101/2002, poz. 926 z późn. zm.) oraz ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144/2001, poz. 1204 z późn. zm.), w tym z poszanowaniem określonych w przepisach zasad zabezpieczenia danych osobowych przed nieuprawnionym wglądem osób trzecich. Wszelkie dane osobowe udostępniane w trakcie rejestracji podlegają włączeniu do zbioru danych osobowych zgłoszonego do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO) zgodnie z obowiązującymi przepisami prawa.

Administrator przetwarza dane osobowe Użytkowników wyłącznie w celu i w zakresie niezbędnym do:

1. nawiązania, ukształtowania, wykonania, zmiany lub rozwiązania Umowy świadczenia usług drogą elektroniczną łączącej Użytkownika z Administratorem,

2. zawierania i wykonania Umów, świadczenia Usług oraz zawierania i wykonania Umów dodatkowych, a także prawidłowego wykonania obowiązków wynikających z przepisów prawa związanych z tymi umowami,

3. w przypadku uzyskania wiadomości o korzystaniu przez Użytkownika z Serwisu w sposób niezgodny z prawem lub Regulaminem – w celu i w zakresie potrzebnym do ustalenia odpowiedzialności Użytkownika.

Użytkownik wyraża niniejszym zgodę na gromadzenie i przetwarzanie przez Administratora jego danych osobowych, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, w zakresie i celu wskazanym powyżej.

Użytkownik w każdym czasie na prawo do wglądu i modyfikacji swych danych osobowych oraz ich usunięcia, za pośrednictwem Serwisu, z zastrzeżeniem, że w przypadku usunięcia danych niezbędnych dla prawidłowego świadczenia usług na rzecz Użytkownika lub cofnięcia zgody na ich przetwarzanie, Administrator będzie uprawniony do rozwiązania umowy z Użytkownikiem ze skutkiem natychmiastowym. Wglądu w swoje dane osobowe, ich modyfikowania i usuwania dokonuje się drogą e-mailową pod adresem office@bring.ai. Dopuszczalne jest również dokonywanie zgłoszeń dotyczących konieczności wprowadzenia tego rodzaju zmian pisemnie na adres Administratora.

Pomimo usunięcia przez Użytkownika jego danych osobowych lub cofnięcia zgody na ich przetwarzanie, Administrator jest uprawniony do ich przetwarzania w zakresie niezbędnym do wykonania wcześniej zawartych umów lub dochodzenia roszczeń.

Administrator jest uprawniony do powierzania przetwarzania danych osobowych Użytkowników osobom trzecim, w tym przekazywania danych osobowych osobom spoza Europejskiego Obszaru Gospodarczego. W takim przypadku Administrator bierze odpowiedzialność za przestrzeganie przez taką osobę zasad przetwarzania danych osobowych określonych w przepisach prawa.

Administrator, bez odrębnej zgody Użytkowników nie będzie przetwarzać danych osobowych w celach innych niż wskazane powyżej, w szczególności w celach promocyjnych i marketingowych, z zastrzeżeniem, że na adres poczty elektronicznej podany w Profilu Administrator może wysyłać informacje dotyczące Serwisu lub inne wskazane w treści Regulaminu.

W przypadku wyrażenia przez Użytkownika zgody Administrator może wysyłać na adres wskazany w Koncie informacje handlowe dotyczące oferowanych usług (newsletter). W takim przypadku Użytkownik w każdym czasie może zrezygnować z otrzymywania informacji kierując odpowiednie oświadczenie w trybie wskazanym w otrzymanej wiadomości. W takim przypadku Administrator niezwłocznie zaprzestanie wysyłania informacji Użytkownikowi.

Administrator jest uprawniony do przetwarzania następujących danych charakteryzujących sposób korzystania przez Użytkownika z Serwisu:

a) oznaczenia identyfikujące Użytkownika,

b) oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał Użytkownik, w tym numer IP,

c) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z Serwisu,

d) informacje o skorzystaniu przez Użytkownika z Serwisu. Serwis wykorzystuje pliki cookies, czyli pliki tekstowe przechowywane w urządzeniu, którym posługuje się osoba korzystająca z Serwisu.

Pliki cookies wykorzystywane są w celu:

a) analizy preferencji osób korzystających z Serwisu odnośnie prezentowanych w nim treści,

b) dostosowania treści prezentowanych w Serwisie do preferencji osób korzystających z Serwisu,

c) analizy sposobu korzystania z Serwisu,

d) umożliwienia Użytkownikom korzystania z Serwisu bez konieczności logowania się na każdej odwiedzanej podstronie Serwisu.

Pliki cookies przechowywane są w urządzeniu, którym posługuje się osoba korzystająca z Serwisu, w zależności od ich przeznaczenia, do chwili wylogowania się Użytkownika lub do chwili usunięcia plików cookies z pamięci urządzenia. Przechowywane pliki cookies pochodzą zarówno bezpośrednio od Administratora, jak i od osób trzecich, jeśli jest to wskazane dla osiągnięcia celów korzystania z plików cookies.

Część plików cookies wykorzystywanych przez Serwis jest niezbędna dla jego prawidłowego działania. Wiele przeglądarek domyślnie dopuszcza automatyczne zapisywanie i przechowywanie plików cookies w urządzeniu. Ustawienia i zmiany zasad przechowywania plików cookies dokonuje się w ustawieniach przeglądarki internetowej.

Dokonując Rejestracji w Serwisie, a następnie logując się do Serwisu, Użytkownik wyraża zgodę na posługiwanie się plikami cookies niezbędnymi dla prawidłowego działania Serwisu. W pozostałym zakresie odmowa zgody na przechowywanie plików cookies, w tym dokonana za pomocą ustawień przeglądarki internetowej, nie wyłącza możliwości korzystania z Serwisu, choć może wpływać na sposób jego działania.

Niniejsze zasady mogą ulec zmianie w przypadku zmiany zasad działania Serwisu, zmian w przepisach prawa regulujących kwestie ochrony prywatności oraz w przypadku dalszego rozwoju Serwisu. Jeśli tak się stanie, zostaniecie Państwo poinformowani o zakresie wprowadzanych zmian na zasadach analogicznych do zmiany Regulaminu Serwisu. W kwestiach nieuregulowanych w niniejszej Polityce Prywatności zastosowanie znajdą odpowiednie postanowienia Regulaminu Serwisu oraz powszechnie obowiązujące przepisy prawa polskiego.

W każdej chwili możecie Państwo zgłaszać do Administratora pytania i wnioski dotyczące przetwarzania danych osobowych. Należy je kierować za pośrednictwem poczty elektronicznej na adres office@bring.ai.