



POLITYKA PRZETWARZANIA DANYCH OSOBOWYCH

ROZDZIAŁ 1 POSTANOWIENIA OGÓLNE

1. Polityka Przetwarzania Danych Osobowych (zwana dalej Polityką) w Walk15, UAB (zwane dalej Firmą) jest częścią publicznie udostępnionej Polityki Przetwarzania Danych, która reguluje cele przetwarzania danych osobowych osób fizycznych, których dane są przetwarzane przez Firmę, ustala procedury dochodzenia swoich praw, ustala organizacyjne i techniczne środki ochrony danych oraz reguluje powoływanie się na podmioty przetwarzające dane osobowe.
2. Niniejsza Polityka została przygotowana w oparciu o:
 - Ustawa w Sprawie Ochrony Danych Osobowych Republiki Litewskiej (zwana dalej LLPPD).
 - Ogólne Rozporządzenie o Ochronie Danych (zwane dalej RODO).
 - Zarządzenie Rządu Republiki Litewskiej nr 228 z dnia 28 lutego 2001 r. „W sprawie zatwierdzenia nakazu wynagradzania Podmiotu danych za przekazanie danych oraz wynagrodzenia za zbieranie danych od zarejestrowanych administratorów danych”.
 - Inne akty prawne związane z przetwarzaniem i ochroną danych osobowych.
3. Niniejsza Polityka dotyczy automatycznego przetwarzania danych osobowych osób fizycznych, jak również ręcznego przetwarzania systematycznych zbiorów danych osobowych. Niniejsza Polityka określa również prawa, obowiązki i odpowiedzialność pracowników Firmy w związku z przetwarzaniem danych osobowych.
4. Wymogi niniejszej Polityki obowiązują wszystkich pracowników Firmy (zwanym dalej Pracownikami) i muszą być również przestrzegane przez procesorów danych, którzy świadczą na rzecz Firmy usługi przetwarzania danych, powezmą informację i przetwarzają dane osobowe, przy czym nie jest to uregulowane odrębnymi umowami pomiędzy Firmą a procesorami danych.

ROZDZIAŁ 2

POJĘCIA OGÓLNE

5. Dane osobowe / Dane – oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej – bezpośrednio lub pośrednio, w szczególności przez odniesienie do identyfikatora takiego jak imię i nazwisko, osobisty kod, dane o lokalizacji, identyfikator internetowy lub do jednego lub więcej specyficznych czynników dla fizycznej, fizjologicznej, genetycznej, psychicznej, ekonomicznej, kulturowej lub społecznej tożsamości danej osoby fizycznej.
6. Przetwarzanie danych – oznacza każdą operację lub szereg operacji wykonywanych w sposób zautomatyzowany lub niezautomatyzowany na danych osobowych lub zbiorach danych osobowych, takie jak zbieranie, utrwalanie, sortowanie, systematyzowanie, przechowywanie, adaptowanie lub modyfikowanie, wyodrębnianie, zaznajomienie, używanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub udostępnianie do użytku w inny sposób, a także zestawianie lub łączenie z innymi danymi, ograniczanie, usuwanie lub niszczenie.
7. Administrator danych – Walk15, UAB, który określa sposoby i środki wykorzystania danych przy przetwarzaniu danych Podmiotów danych.
8. Podmiot danych – Pracownicy i inne osoby fizyczne, których dane są przetwarzane przez Walk15, UAB.
9. Procesor danych – podmioty przetwarzające dane osobowe kontrolowane przez Walk15, UAB na zlecenie Walk15, UAB na podstawie zawartych umów o świadczenie usług.
10. Podanie danych oznacza udostępnienie danych osobowych poprzez przekazanie lub ich udostępnienie w inny sposób (z wyłączeniem publikacji w mediach).
11. Aplikacja mobilna – administrowana przez Firmę aplikacja mobilna Walk15.
12. Administracja wewnętrzna – czynności zapewniające autonomiczne funkcjonowanie administratora danych (zarządzanie strukturą, zarządzanie personelem, zarządzanie i wykorzystanie dostępnych zasobów materialnych i finansowych, prowadzenie ewidencji).
13. Pozostałe pojęcia użyte w Polityce należy rozumieć zgodnie z rozumieniem aktu LLPPD i/lub RODO.

ROZDZIAŁ 3

ZASADY I CELE PRZETWARZANIA DANYCH OSOBOWYCH

14. Przy wykonywaniu swoich obowiązków i przetwarzaniu danych osobowych pracownicy są zobowiązani do:
 - Przetwarzania danych osobowych w sposób uczciwy, przejrzysty i zgodny z prawem.
 - Zbierania danych w określonych, jawnych i prawnie uzasadnionych celach i nieprzetwarzania ich dalej w sposób niezgodny z tymi celami.



- Przestrzegania zasad celowości, proporcjonalności i minimalizacji ilości danych przy gromadzeniu i przetwarzaniu danych osobowych, nie wymagania podawania danych, które nie są potrzebne i nie są przechowywane oraz powstrzymywania się od przetwarzania danych w nadmiarze.
 - Zapewnienia dokładności danych osobowych oraz, jeśli jest to konieczne do celów przetwarzania danych osobowych, ich aktualizacji; poprawienia, uzupełnienia, usunięcia lub wstrzymania przetwarzania niedokładnych lub niekompletnych danych.
 - Przechowywania danych osobowych w postaci umożliwiającej identyfikację Podmiotu danych, nie dłużej niż jest to niezbędne do celów, dla których dane zostały zebrane i przetwarzane.
 - Przetwarzania danych osobowych w taki sposób, aby zapewnić odpowiednie bezpieczeństwo danych osobowych poprzez zastosowanie odpowiednich środków technicznych lub organizacyjnych, w tym ochronę przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem oraz przed nieumyślną utratą, zniszczeniem lub uszkodzeniem danych (zasada integralności i poufności).
15. Osobą odpowiedzialną za aktualizację danych Podmiotów danych Firmy jest dyrektor ds. rozwoju regionalnego Justina Verbickaitė.
16. Informacje o Podmiotach danych muszą być podane, jeżeli wymagają tego przepisy prawa.

ROZDZIAŁ 5

PRZETWARZANIE DANYCH KANDYDATÓW DO ZATRUDNIENIA

- Firma przetwarza następujące dane osób, które chcą wziąć udział w procesie rekrutacji Firmy: imię, nazwisko, data urodzenia, adres, telefon, adres e-mail, wykształcenie, inne dane określone w dokumentach przekazanych przez kandydatów do pracy w Firmie, w tym CV. W przypadku, gdy ustawodawca Republiki Litewskiej przewiduje dodatkowe ograniczenia dotyczące rodzaju przetwarzanych informacji o kandydatach do pracy, Administrator danych zapewnia, że przetwarzane są wyłącznie dane osobowe kandydatów, które mogą być przetwarzane. Dane wrażliwe nie są przetwarzane, chyba że kandydat zdecyduje się podać takie dane.
17. Podstawą przetwarzania danych jest zgoda kandydata do pracy. Kandydaci na wolne stanowiska wyrażają zgodę (w drodze aktu rozstrzygającego) na przetwarzanie ich danych wyłącznie do czasu zakończenia naboru. Dane kandydatów, którzy nie zostali wybrani na konkretne stanowisko (wakat), są usuwane po zakończeniu postępowania kwalifikacyjnego, chyba że na zakończenie procedury selekcyjnej wyrażą wyraźną zgodę na przetwarzanie danych.
18. Celem przetwarzania danych jest administracja wewnętrzna. W przypadku uzyskania zgody kandydata na przetwarzanie jego danych po zakończeniu postępowania kwalifikacyjnego w celu zaferowania przyszłej pracy, dane będą przetwarzane na podstawie udzielonej zgody.
19. Kandydaci podają swoje dane osobowe podczas aplikowania do pracy w Firmie. W niektórych przypadkach, gdy zbieranie dokumentów jest przeprowadzane przez podmioty trzecie (podmioty przetwarzające dane Firmy), dane są najpierw przekazywane tym podmiotom trzecim, a dopiero później Firmie. We wszystkich przypadkach administratorem danych jest Firma.



20. Dane kandydata nie będą ujawniane innym podmiotom trzecim, chyba że kandydat o to zawnioskuje i istnieją uzasadnione podstawy do takiego przekazania.

21. Dane kandydata są na bieżąco przetwarzane w bazach danych Firmy, do których dostęp mają dostawcy usług IT Firmy. CV lub listy motywacyjne kandydatów mogą być również przechowywane w formie papierowej.

22. Kandydat zostaje poinformowany o przetwarzaniu danych i przysługujących mu prawach, w tym o prawie do wystąpienia do Firmy o usunięcie danych. Informacje te zostają zawarte w Polityce publicznie dostępnej na stronach internetowych Firmy.

ROZDZIAŁ 6

DANE OSÓB FIZYCZNYCH PRZETWARZANE W CELU ŚWIADCZENIA USŁUG

23. Firma może przetwarzać następujące dane osób korzystających z usług Firmy w aplikacji mobilnej: imię, nazwisko, płeć, wzrost, waga, długość kroku, język, e-mail, adres, lokalizacja, dane otrzymywane od dostawców usług płatniczych (tj. Google Pay), a także inne dane podane bezpośrednio przez Podmiot danych.

24. Użytkownicy Serwisu wyrażają zgodę na warunki korzystania z zarządzanej przez Firmę aplikacji mobilnej przed skorzystaniem z niej. Podstawą przetwarzania danych jest zawarcie i wykonanie umowy.

25. Celem przetwarzania danych jest prawidłowe świadczenie usług.

26. Podmiot danych sam podaje swoje dane osobowe lub umożliwia aplikacji mobilnej synchronizację danych z Samsung Health, Apple Health Kit lub innymi aplikacjami mobilnymi. W szczególnych przypadkach dane mogą być pozyskiwane od osób trzecich, m.in. gdy podmiot danych dokonuje zakupów, dane pochodzą od firm świadczących usługi płatnicze lub, gdy loguje się za pomocą konta Google lub Facebook, dane pochodzą bezpośrednio od tych firm.

27. Dane są przechowywane w bazach danych Firmy, do których dostęp mają firmy świadczące na rzecz Firmy usługi informatyczne. Dane nie będą ujawniane innym stronom trzecim, chyba że zostanie zgłoszony taki wniosek i gdy istnieją uzasadnione podstawy do takiego przekazania.

Gdy Podmiot danych korzysta z niektórych funkcji aplikacji mobilnej (np. udział w wyzwaniu), jego dane mogą być publicznie dostępne w aplikacji mobilnej, ale we wszystkich przypadkach może wyłączyć tę funkcję i uczestniczyć anonimowo.

Dane mogą być również przekazywane podmiotom trzecim, którzy we współpracy z Firmą publikują swoje oferty w aplikacji mobilnej („Step Wallet”). Takie dane są dostarczane, gdy użytkownik aplikacji mobilnej zdecyduje się korzystać z funkcji Step Wallet.

28. Podmiot danych jest informowany o przetwarzaniu swoich danych i przysługujących mu prawach. Powiadomienia dokonuje się w Polityce publicznie dostępnej na stronie internetowej Firmy oraz w aplikacji mobilnej, a także w warunkach korzystania, udostępnionych w aplikacji mobilnej.

ROZDZIAŁ 7

PRZETWARZANIE DANYCH W CELACH MARKETINGU BEZPOŚREDNIEGO

29. Na potrzeby marketingu bezpośredniego Firma przetwarza następujące dane osobowe: imię, nazwisko, adres e-mail. Mogą być również przetwarzane inne dane kontaktowe.
30. Przetwarzanie danych odbywa się na podstawie udzielenia zgody.
31. Podmiot danych sam przekazuje Firmie swoje dane osobowe.
32. Dane są przechowywane w bazach danych Firmy, do których dostęp mają inne firmy świadczące usługi informatyczne na rzecz Firmy. Dane nie będą ujawniane innym stronom trzecim, chyba że zostanie zgłoszony taki wniosek przez Podmiot danych i gdy istnieją uzasadnione podstawy do takiego przekazania.
33. Firma nie przetwarza w tym celu danych małoletnich ani wrażliwych danych osobowych. Niemniej jednak, zbierając dane do celów marketingu bezpośredniego, Firma nie weryfikuje wieku Podmiotu danych, ponieważ byłoby to traktowane jako gromadzenie danych w nadmiarze.
34. Podmiot danych jest informowany o przetwarzaniu danych i przysługujących mu prawach, w tym o prawie do wystąpienia do Firmy o usunięcie danych. Powiadomienie powinno zostać dokonane w Polityce, udostępnionej publicznie na stronie internetowej Firmy oraz w aplikacji mobilnej. Podmiot danych po pobraniu i użyciu aplikacji mobilnej ma prawo wyrazić zgodę na przesyłanie newsletterów marketingu bezpośredniego do Podmiotu danych za pośrednictwem poczty elektronicznej lub w inny sposób podany przez Podmiot danych. Podmiot danych ma prawo w każdej chwili zrezygnować z subskrypcji lub anulować tę opcję.

ROZDZIAŁ 8

PRZETWARZANIE DANYCH W CELU REALIZACJI ZGŁOSZENIA, WNIOSKU LUB SKARGI, OCENY I BADANIA

35. Firma może przetwarzać w określonym celu następujące dane kontaktujących się osób fizycznych: imię i nazwisko, język, adres e-mail, adres zamieszkania. Firma może również przetwarzać inne dane uzyskane bezpośrednio od Podmiotu danych, a które są niezbędne do rozpatrzenia, administrowania lub oceny wniosku, zgłoszenia lub skargi.
36. Podstawą przetwarzania danych jest zawarcie i wykonanie umowy.
37. Podmiot danych sam podaje swoje dane osobowe.
38. Dane są przechowywane w bazach danych Firmy, do których dostęp mają inne firmy świadczące usługi informatyczne na rzecz Firmy. Dane nie będą ujawniane innym stronom trzecim, chyba że zostanie zgłoszony taki wniosek przez Podmiot danych i gdy istnieją uzasadnione podstawy do takiego przekazania.
39. Podmiot danych jest informowany o przetwarzaniu jego danych i przysługujących mu prawach. Powiadomienie zostanie dokonane w Polityce, udostępnionej publicznie na stronie internetowej Firmy oraz w aplikacji mobilnej.

ROZDZIAŁ 9

PLIKI COOKIE

40. Firma używa plików cookie w celu usprawnienia nawigacji i usług świadczonych przez stronę Walk15.com. Strona internetowa Firmy może wykorzystywać analityczne pliki cookie stron trzecich – „Google Analytics”.

41. Następujące pliki cookie są lub mogą być używane na stronie internetowej Firmy.

Nazwa pliku cookie	Opis	Moment stworzenia	Czas wygaś	Wykorzystane dane
_ga	Unikalny identyfikator jest rejestrowany i używany do generowania statystyk dotyczących sposobu korzystania z witryny przez użytkownika.	Klikając przycisk „Wyrażam zgodę”	2 lata	Unikalny identyfikator
_gid	Ten plik cookie służy do rozróżniania użytkowników.	Klikając przycisk „Wyrażam zgodę”	24 godz.	Unikalny identyfikator
_gat*	Te pliki cookie służą do ograniczenia liczby żądań.	Podczas wchodzenia na stronę	10 min.	Unikalny identyfikator
cookieconsent_status	Wykorzystywane do zapisywania zgody użytkownika na używanie plików cookie.	Klikając przycisk „Wyrażam zgodę”	1 rok	Unikalny identyfikator
pll_language	Ten plik cookie służy do zapisywania preferowanego języka osoby odwiedzającej.	Podczas wchodzenia na stronę	1 rok	Język

42. Firma może gromadzić dane dotyczące działań osób odwiedzających i ich nawyków przeglądania na stronie internetowej.

43. Więcej informacji można znaleźć na stronie: <http://www.google.com/analytics>.

44. Aby dowiedzieć się, jak wyłączyć śledzenie na stronach internetowych za pomocą plików cookie Google Analytics, możesz wejść na stronę: <http://tools.google.com/dlpage/gaoptout>.

45. Dane przekazywane są dostawcom usług IT oraz Google. Dane nie będą ujawniane innym stronom trzecim, chyba że zostanie zgłoszony taki wniosek i gdy istnieją uzasadnione podstawy do takiego przekazania.

46. Strona internetowa umożliwia rezygnację z używania plików cookie.

ROZDZIAŁ 10

WARUNKI PRZECHOWYWANIA DANYCH

47. Administrator danych stosuje następujące okresy przechowywania danych osobowych:

Nr	Cel przetwarzania danych osobowych	Okres przechowywania
1.	Przetwarzanie danych pracowników na potrzeby administracji wewnętrznej.	Do 50 lat po zakończeniu umowy o pracę, zgodnie z Indekssem okresów przechowywania w Dokumentacji ogólnej.
2.	Przetwarzanie danych osobowych kandydatów do pracy.	Do końca procesu selekcyjnego.
3.	Przetwarzanie danych osobowych kandydatów do pracy po zakończeniu naboru następuje po uzyskaniu zgody na przetwarzanie danych.	Dwa lata od daty otrzymania C.V.
4.	Świadczenie usług.	Dane będą przetwarzane przez okres nie dłuższy niż 10 lat, zgodnie z przepisami prawa.
5.	Administracja, ocena i badanie wniosków, zgłoszeń lub skarg.	6 miesięcy od daty otrzymania wniosku.
6.	Do celów marketingu bezpośredniego.	3 lata od uzyskania zgody.
7.	Pliki cookie poprawiające jakość korzystania z witryny.	Czas, przez jaki plik cookie pozostaje na Twoim komputerze, zależy od rodzaju pliku cookie.

48. Mogą zostać określone wyjątki od powyższych okresów przechowywania, o ile takie wyjątki nie naruszają praw Podmiotu danych, spełniają wymogi prawne i są odpowiednio udokumentowane.

ROZDZIAŁ 11

PRAWA PODMIOTÓW DANYCH I PROCEDURY ICH WDRAŻANIA

Zapewnienie praw i świadomości Podmiotu danych

49. Podmiot danych ma prawo do:

- Informacji (poinformowania) o przetwarzaniu ich danych osobowych.
- Przesyłając Firmie dokument tożsamości lub za pośrednictwem drogi elektronicznej, która pozwala na prawidłową identyfikację osoby – dostępu do swoich danych osobowych i ich przetwarzania, uzyskania informacji o źródłach oraz o tym, jakie konkretnie dane osobowe są gromadzone, w jakim celu dane są przetwarzane, informacji o odbiorcach danych w okresie co najmniej ostatniego 1 roku, dodatkowo – do otrzymania kopii dokumentów zawierających swoje dane osobowe.



- Żądania sprostowania, usunięcia lub ograniczenia danych osobowych, z wyjątkiem przechowywania, gdy przetwarzanie narusza wymogi prawne.
- Wniesienia sprzeciwu wobec przetwarzania danych osobowych.
- Żądania przeniesienia danych do innego administratora danych lub przekazania ich bezpośrednio Podmiotowi danych, w dogodnej dla niej formie (takie dane przekazane Firmie przez sam Podmiot danych).
- Złożenia skargi do organu nadzorczego.
- Cofnięcia wyrażonej zgody (jeżeli dane osobowe są przetwarzane na podstawie wyrażenia zgody).

50. We wszystkich przypadkach Firma musi przekazać Podmiotowi danych, informacje (chyba że Podmiot danych posiada już takie informacje) o:

- Nazwie, kodzie podmiotu prawnego i siedzibie.
- Danych kontaktowych inspektora ochrony danych, jeśli taki istnieje.
- W jakich celach i na jakiej podstawie prawnej przetwarzane są dane osobowe Podmiotu danych.
- Odbiorcach danych i ich kategoriach.
- Okresie przechowywania danych lub kryteriach stosowanych do określenia tego okresu.
- Innych dodatkowych informacjach (jakie Dane osobowe musi podać podmiot danych oraz konsekwencjach niepodania danych, o prawie dostępu do danych osobowych Podmiotu danych oraz jego prawie do poprawiania nieprawidłowych, niekompletnych, niedokładnych danych osobowych) w ilości niezbędnej do zapewnienia prawidłowego przetwarzania danych osobowych bez naruszania praw Podmiotu danych.
- Przekazaniu danych osobowych stronom trzecim najpóźniej w momencie, gdy dane są przekazywane po raz pierwszy, a podmiot danych nie wiedział, że dane zostaną przekazane innemu podmiotowi.

Zarządzenie realizacji praw Podmiotu danych

51. Firma jest zobowiązana do:

- Umożliwienia Podmiotowi danych skorzystania z określonych praw Podmiotu danych, z wyjątkiem przypadków przewidzianych przez prawo, gdy jest to niezbędne do zapewnienia bezpieczeństwa lub obronności państwa, porządku publicznego, zapobiegania przestępczości, prowadzenia dochodzeń, wykrywania przestępstwa lub przeprowadzenia postępowania karnego, zapewnienia ochrony ważnych interesów gospodarczych i finansowych państwa, zapobiegania łamaniu etyki zawodowej lub usługowej, dochodzeniu i wykrywaniu, ochrony praw i wolności Podmiotu danych lub innych osób.
- W celu skorzystania ze swoich praw Podmiot danych musi skontaktować się z oddziałem Firmy pod następującym adresem: info@walk15.lt.



- Firma musi zapewnić, że wszystkie niezbędne informacje są przekazywane Podmiotowi danych w jasny i zrozumiały sposób.

- Podmiot danych musi odpowiedzieć nie później niż w ciągu 20 (dwudziestu) dni roboczych od daty otrzymania prośby. Jeżeli Podmiotowi danych odmówiono dostępu do danych, otrzymuje uzasadnioną i umotywowaną odpowiedź dotyczącą niewykonania jego prośby.

52. Firma niezwłocznie poinformuje odbiorców danych osobowych, które zostały sprostowane lub zniszczone na żądanie Podmiotu danych o wstrzymaniu przetwarzania danych osobowych, chyba że podanie takich informacji byłoby niemożliwe lub nadmiernie utrudnione (z uwagi na dużą liczbę Podmiotów danych; okres, w którym dane są przetwarzane; nieuzasadnione wysokie koszty). W takim przypadku należy niezwłocznie powiadomić Państwową Inspekcję Ochrony Danych.

53. Firma udostępnia dane Podmiotowi danych nieodpłatnie. W niektórych przypadkach (gdy Podmiot danych wyraźnie nadużywa swoich praw, składa bezzasadnie powtarzające się prośby o informacje, wyciągi, dokumenty), takie przekazanie informacji i danych Podmiotowi danych, może wymagać wynagrodzenia zgodnie z wymogami prawnymi i stawkami określonymi przez Firmę.

Udostępnianie danych do odbiorców danych

54. Firma udostępnia Dane Podmiotu danych zgodnie z wymogami aktów prawnych oraz z zachowaniem ich poufności.

55. W przypadku jednorazowego udostępnienia danych Firma w pierwszej kolejności przekazuje informacje drogą elektroniczną.

56. Udostępnienie danych osobowych instytucjom i organom państwowym i samorządowym, gdy te instytucje i organy otrzymują dane osobowe w celu wykonywania ustawowych funkcji kontrolnych, nie jest uważane za przekazanie danych odbiorcom.

ROZDZIAŁ 12

ŚRODKI ORGANIZACYJNE I TECHNICZNE DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH

57. Firma dokłada wszelkich starań, aby stosowane w Firmie zabezpieczenia organizacyjne i techniczne danych były zgodne z wymogami RODO. W celu ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, zmianą, ujawnieniem lub innym niezgodnym z prawem przetwarzaniem, podejmuje się następujące środki infrastrukturalne, administracyjne i telekomunikacyjne (elektroniczne):

- Właściwy układ i konserwacja sprzętu, konserwacja systemów informatycznych, zarządzanie siecią, zapewnienie bezpieczeństwa korzystania z Internetu i innych środków technologii informacyjnej.

- Dostęp do Danych oraz prawo do wykonywania operacji przetwarzania Danych przysługuje wyłącznie Pracownikom, którzy potrzebują dostępu do danych osobowych w związku z wykonywanymi obowiązkami i wykonywanymi funkcjami w pracy.

- Zapewnienie bezpieczeństwa pomieszczeń, w których przechowywane są dane osobowe (dostęp do pomieszczeń mają tylko osoby upoważnione).



- Po przypisaniu komputera lub elektronicznego urządzenia komunikacyjnego do konkretnego Pracownika, taki komputer / elektroniczne urządzenie komunikacyjne musi być chronione hasłem. Hasła muszą być zmieniane okresowo, a także w przypadku wystąpienia pewnych okoliczności (zmiany pracownika, zagrożenia włamaniami hakerskimi, podejrzenia, że hasło stało się znane osobom trzecim, itp.).
- Zapewnienie ochrony danych osobowych przed nieuprawnionym dostępem do wewnętrznej sieci komputerowej za pomocą środków komunikacji elektronicznej.
- Zapewnienie stosowania bezpiecznych protokołów do przesyłania danych osobowych przez zewnętrzne sieci teleinformatyczne.
- Ścisłe przestrzeganie norm bezpieczeństwa wydanych przez służby ochrony;
- Właściwa organizacja pracy i innych środków administracyjnych;
- Wdrożenie niezbędnych środków bezpieczeństwa danych z uwzględnieniem wyników oceny ryzyka;
- Tworzenie kopii zapasowych i odzyskiwanie danych;
- Zapewnienie przywrócenia danych z najnowszych dostępnych kopii zapasowych w przypadku utraty danych z powodu awarii sprzętu, błędu oprogramowania lub innego naruszenia integralności danych;
- inne środki.

58. Za wdrożenie, kontrolę i egzekwowanie takich organizacyjnych i technicznych środków bezpieczeństwa danych odpowiedzialny jest kierownik ds. rozwoju regionalnego Firmy, Justina Verbickaitė.

59. Pracownicy przetwarzający dane osobowe muszą przestrzegać zasady poufności i zachować poufność wszelkich istotnych informacji, do których uzyskali dostęp w trakcie wykonywania swoich obowiązków. Obowiązek ten będzie nadal obowiązywał po przeniesieniu na inne stanowisko w Firmie lub po rozwiązaniu stosunku pracy lub stosunku wiążącego taką osobę umową z Firmą.

60. Pracownicy mogą przetwarzać dane osobowe w sposób zautomatyzowany dopiero po uzyskaniu dostępu do odpowiedniego systemu informatycznego. Dostęp do danych osobowych może mieć wyłącznie osoba, która potrzebuje danych osobowych do wykonywania swoich zadań. Z chwilą rozwiązania stosunku pracy prawa Pracownika do dostępu do rejestrów i innych programów zostaną cofnięte.

61. Pracownicy mogą przekazywać dokumenty zawierające dane osobowe wyłącznie Pracownikom, którzy są uprawnieni do pracy z danymi osobowymi w ramach obowiązków służbowych lub odrębnych zadań.

62. Pracownicy wykonujący zadania związane z przetwarzaniem Danych Podmiotu danych zapobiegają przypadkowemu lub nieuprawnionemu przetwarzaniu oraz prowadzą ewidencję we właściwy i bezpieczny sposób (unikając niepotrzebnego przechowywania danych Podmiotu danych, itp.). Kopie dokumentów zawierających dane Podmiotu danych zostaną zniszczone w taki sposób, aby nie można było odtworzyć treści tych dokumentów i zidentyfikować ich treści.



63. Pracownicy, których komputery przechowują Dane lub których komputery mają dostęp do systemów informatycznych Firmy, w których przechowywane są Dane, muszą używać haseł na swoich komputerach; Konta użytkowników typu „Gość” w takich systemach, m.in konta bez hasła są zabronione. Te komputery muszą również używać wygaszacza ekranu z odblokowaniem przy użyciu hasła.

64. O ile nie jest to konieczne, pliki z Danymi nie muszą być duplikowane cyfrowo, tj. kopiowane na lokalne dyski komputerowe, nośniki wymienne, zdalnie przechowywane, itp.

65. Kontrolę bezpieczeństwa i usuwanie danych osobowych zawartych na zewnętrznych nośnikach danych i poczcie elektronicznej po ich wykorzystaniu zapewnia się poprzez przeniesienie ich do baz danych.

66. Kierownik ds. rozwoju regionalnego Justina Verbickaitė musi zapewnić:

- kontrolę nieuprawnionego dostępu do pomieszczeń serwerowych;
- ochronę wewnętrznej sieci komputerowej Firmy.

67. Pracownicy muszą organizować swoją pracę w taki sposób, aby w jak największym stopniu ograniczyć dostęp innych osób do przetwarzanych danych osobowych. Przepis ten stosuje się, aby:

- Powstrzymać się od pozostawiania dokumentów z przetworzonymi danymi osobowymi lub komputera, na którym można bez nadzoru otwierać pliki zawierające dane osobowe, tak aby informacje w nich zawarte mogły być odczytane przez Pracowników nieuprawnionych do pracy z określonymi danymi osobowymi, studentów lub inne osoby;
- Przechowując dokumenty nie były one (lub ich fragmenty) odczytane przez przypadkowe osoby;
- Jeżeli dokumenty zawierające dane osobowe są przekazywane innym Pracownikom, jednostkom, oddziałom, urzędom za pośrednictwem osób nieuprawnionych do przetwarzania danych osobowych lub za pośrednictwem poczty lub z wykorzystaniem usług kurierskich, należy je przekazać w zamkniętej nieprzezroczystej kopercie. Niniejszy ustęp nie ma zastosowania w przypadku, gdy takie wiadomości są przekazywane osobiście i w sposób poufny.

68. Za zarządzanie naruszeniami danych osobowych i reagowanie na nie odpowiedzialny jest kierownik ds. rozwoju regionalnego, Justina Verbickaitė.

ROZDZIAŁ 13

POSTANOWIENIA KOŃCOWE

69. Firma ma prawo w dowolnym momencie zmienić Politykę Prywatności. Wprowadzone zmiany obowiązują od momentu aktualizacji Polityki Prywatności na stronie <https://walk15.lt/en/privacy-policy/>. Podmiotom danych zaleca się zapoznanie się ze zaktualizowaną Polityką Prywatności.