POLITYKA OCHRONY DANYCH OSOBOWYCH

Z DNIA 25 maja 2018

Wersja 1

z dnia 25 maja 2018 r.

SZKOŁY JĘZYKOWE HELEN DORON

PROWADZONE W RAMACH SIECI FRANCZYZOWEJ

FIRMY

JOANNA CESARZ-KRZYSTANEK, CENTRUM JĘZYKA ANGIELSKIEGO

NAUKA DZIECI METODĄ HELEN DORON

Karta dokumentu:

	Imię i nazwisko	*data*
Przygotował:	Tomasz Ciupka Kancelaria Radcy Prawnego	2018-04-11
Zatwierdził:	Joanna Cesarz-Krzystanek	2018-05-25
Wdrożył:	Sylwia Strug	2018-05-25
Ostatni przegląd:		

Spis treści

1. Cel i zakres Polityki oraz osoby odpowiedzialne.

1.1 Niniejsza Polityka została wprowadzona w związku z realizacją obowiązków wynikających z RODO, które wiążą się z tym, iż Firma występuje w roli administratora oraz podmiotu przetwarzającego dla zbiorów danych zawierających dane osobowe, w tym także dane osobowe osób niepełnoletnich.

1.2 Niniejszy dokument stosowany jest przez wszystkie osoby, działające w imieniu lub na rzecz Firmy, w tym przez pracowników, zleceniobiorców, wykonawców oraz podwykonawców niezależnie od formy zatrudnienia.

1.3 Naruszenie zasad niniejszego dokumentu może zostać uznana za ciężkie naruszenie podstawowych obowiązków pracowniczych (w przypadku pracowników) albo za naruszenie podstawowych obowiązków kontraktowych i działanie na szkodę Firmy – w odniesieniu do osób, działających w imieniu Firmy na podstawie umów prawa cywilnego.

1.4 Polityka zawiera:

a) Opis zasad ochrony danych obowiązujących w Spółce;
b) Odwołania do załączników uszczegóławiających
c) Wzory dokumentów, stosowanych w procesach dotyczących ochrony danych;

2. Definicje i skróty:

2.1 **Firma** – Joanna Cesarz-Krzystanek, Centrum Języka Angielskiego Nauka Dzieci Metodą Helen Doron, w odniesieniu do obowiązków wynikających z niniejszej Polityki, określenie to oznacza również niezależnych przedsiębiorców, działających w ramach sieci franczyzowej Helen Doron podległej MF Tychy.

2.2 **Administrator** – Firma

2.3 **Helen Doron** – sieć franczyzowa prowadzona przez Helen Doron Ltd z siedzibą w Izraelu. Na potrzeby niniejszej Polityki oznacza część sieci, koordynowanej przez Firmę.

2.4 **Partner Helen Doron** – niezależni przedsiębiorcy prowadzący działalność gospodarczą w ramach sieci franczyzowej Helen Doron, zarządzanej przez Firmę.

2.5 **Strona trzecia** - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;

2.6 **Polityka** – niniejsza Polityka ochrony danych osobowych;

2.7 **PUODO** – Prezes Urzędu Ochrony Danych Osobowych;

2.8 **Procesor** - inaczej "podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

2.9 **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/697 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 96/46/WE

2.10 **Incydent bezpieczeństwa** – zdarzenie, w którego efekcie doszło do kradzieży lub utraty zbioru danych jak również do nieodwracalnej utraty integralności danych lub do udostępnienia zbioru danych osobom nieupoważnionym.

2.11 **Właściciel** – przedsiębiorca, prowadzący indywidualną działalność gospodarczą w ramach której działa szkoła objęta niniejszą Polityką. W przypadku spółek prawa handlowego, fundacji lub innych osób prawnych przez Właściciela należy rozumieć prezesa Zarządu.

2.12 **NDA** – (non-disclosure agreement) – umowa o zachowaniu poufności

2.13 **IOD** – Inspektor Ochrony Danych

2.14 **LCF** - - Lerning Center Franchisee (Właściciel Centrum Helen Doron)

2.15 **LSF** – Lerning Studio Franchisee (Właściciel Studia Helen Doron)

2.16 **IT** – Independent Teacher (nauczyciel niezależny)

3. Klasyfikacja informacji zawierających dane osobowe;

3.1 W związku z prowadzoną działalnością w zakresie usług edukacyjnych, Firma przetwarza jako administrator (we własnych placówkach) lub podmiot przetwarzający (w odniesieniu do danych, przetwarzanych w placówkach Partnerów Helen Doron) dane osobowe uczniów oraz ich opiekunów prawnych, a w szczególności:

a) Imiona i nazwiska uczniów;
b) Imiona i nazwiska opiekunów prawnych
c) Numery PESEL opiekunów prawnych
d) Adres zamieszkania opiekuna/opiekunów;
e) Numer telefonu do opiekuna/opiekunów;
f) Adres e-mail opiekuna/opiekunów
g) Numery rachunków bankowych klientów (w przypadku, gdy zapłata za usługi dokonywana jest w formie przelewu).
h) Wizerunek (nagrania, zdjęcia, nagrania z monitoringu) uczniów, opiekunów oraz nauczycieli i członków personelu Firmy.

3.2 Firma może przetwarzać dane o szczególnym charakterze (tzw. „dane wrażliwe”), a w szczególności dane o stanie zdrowia dziecka (np. alergie pokarmowe, ograniczenia i dysfunkcje mogące wpłynąć na proces nauczania). Podanie tych informacji przez opiekunów jest dobrowolne i wymaga odebrania odrębnej zgody.

3.3 W Firmie przetwarzane są informacje związane z zatrudnieniem, zawierające dane osobowe pracowników oraz usługobiorców – zgodnie z obowiązującymi wymaganiami prawnymi;

3.4 W Firmie przetwarzane są dane osobowe nauczycieli – osób fizycznych lub osób fizycznych prowadzących indywidualna działalność gospodarczą w celu realizacji zobowiązań wynikających z umów zawartych z tymi osobami.

3.5 W Firmie przetwarzane są informacje związane z prowadzoną działalnością gospodarczą, zawierające dane osobowe partnerów handlowych (sprzedaż i zakupy), zleceniobiorców i zleceniodawców, kontrahentów oraz osób, które złożyły zapytania ofertowe oraz wnioski o nawiązanie współpracy;

3.6 Firma przetwarza informacje związane z koniecznością realizacji obowiązków prawno-finansowych, w tym faktury, umowy, aneksy, porozumienia i podobne.

3.7 Firma przetwarza informacje w postaci korespondencji elektronicznej (e-maile), które mogą potencjalnie zawierać dane osobowe.

3.8 Firma pozyskuje dane w drodze:

a) dobrowolnych zgód poprzez formularze kontaktowe (www.helendoron.pl),

b) poprzez uzyskanie zgody w treści formularza zgłoszeniowego;
c) poprzez informacje uzyskane od kandydatów na partnerów w wiadomościach e-mail;
d) wynikające z treści zawartych umów lub faktur.

3.9 Dane przetwarzane są poprzez dedykowaną aplikację, zarządzaną przez Helen Doron LTD. (dalej: Aplikacja Helen Doron) lub w plikach z danymi (np. xls) – w postaci zbiorczej lub rozproszonej lub w postaci wykazów papierowych.

3.10 Dane mogą być przetwarzane w środowisku lokalnym (komputery, dyski, pen-drive) oraz w środowisku chmurowym. W przypadku wyboru środowiska chmurowego, akceptowani są jedynie rekomendowani dostawcy usług o utrwalonej pozycji rynkowej i zapewniający wysoki poziom bezpieczeństwa danych (np. Microsoft, Google).

4. Zarządzanie ryzykiem;

4.1 Na dzień opublikowania pierwszej wersji niniejszej Polityki Firma przeprowadziła analizę ryzyk dla wszystkich procesów związanych z przetwarzaniem danych osobowych, funkcjonujących w Firmie i nie stwierdziła występowania istotnego ryzyka dla praw i wolności osób, których dane są przetwarzane.

4.2 Dla każdego nowego procesu wdrażanego w Firmie przeprowadzana jest weryfikacja, czy proces ten wiąże się lub potencjalnie może wiązać się z przetwarzaniem danych osobowych. Za wykonanie analizy ryzyka odpowiedzialna jest osoba zarządzająca przygotowaniem nowego procesu (zasada *„privacy by design”*).

4.3 Dla procesów, które wiążą lub mogą wiązać się z przetwarzaniem danych osobowych każdorazowo przeprowadza się analizę ryzyka według następujących zasad:

a. Określony zostaje zakres danych osobowych, których może dotyczyć przetwarzanie;
b. Określona zostaje skala przetwarzania;
c. Wskazani zostają potencjalni odbiorcy danych a także inne podmioty lub osoby, które mogą przetwarzać dane;
d. Wskazane zostają potencjalne ryzyka dla praw i wolności osób, których dane będą lub mogą być przetwarzane – przy użyciu skali pięciostopniowej;
e. Wskazane zostają środki zabezpieczenia danych osobowych;
f. Określone zostaje prawdopodobieństwo naruszenia zasad ochrony danych osobowych – przy użyciu skali pięciostopniowej;
g. Określony zostaje poziom ryzyka dla procesu, stanowiący wypadkową poziomu ryzyka dla praw i wolności oraz prawdopodobieństwo naruszenia zasad ochrony danych osobowych ustandaryzowanej metodologii zarządzania ryzykiem;

4.4 Dla każdego procesu związanego z przetwarzaniem danych osobowych, w przypadku gdy analiza ryzyka wykaże wysoki poziom zagrożenia dla praw i wolności osób, których dane są przetwarzane, Firma przeprowadza analizę skutków dla ochrony danych, zgodnie z wytycznymi opisanymi w art. 35 RODO. Analiza przeprowadzana jest przez IOD lub inną osobę lub firmę wyznaczoną przez Firmę (analiza DPIA).

4.5 W przypadku ustalenia w ramach analizy DPIA, iż poziom ryzyka związany z potencjalnym naruszeniem praw i wolności osób, których dane są przetwarzane jest wysoki lub bardzo wysoki, Firma przeprowadza konsultacje z prezesem UODO zgodnie z art. 36 RODO przed rozpoczęciem przetwarzania.

5. Prowadzenie Rejestru Czynności Przetwarzania Danych;

5.1 W przypadku procesu, w ramach którego w Firmie dojdzie do przetwarzania danych o charakterze informacji wrażliwych, bądź przetwarzanie będzie miało charakter inny niż sporadyczny albo przetwarzanie będzie wiązało się z ryzykiem naruszenia praw i wolności osób, których dane będą przetwarzane, Spółka utworzy dla takiego procesu Rejestr Czynności Przetwarzania Danych (RCP), zgodnie z zasadą rozliczalności, wynikającą z art. 5 ust. 2 RODO.

5.2 RCP prowadzony i aktualizowany jest przez Właściciela lub osobę przez niego wyznaczoną przy użyciu wzoru, stanowiącego **załącznik nr 1** do Polityki.

5.3 W przypadku, gdy Firma w wyniku powierzenia przetwarza dane objęte obowiązkiem sporządzenia Rejestru Kategorii Czynności Przetwarzania (np. dane szczególnych kategorii), Właściciel lub osoba przez niego wyznaczona utworzy Rejestr przy użyciu wzoru stanowiącego **załącznik nr 2** do Polityki.

5.4 RCP zawierać będzie co najmniej:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO

6. Zasady dostępu do danych osobowych;

6.1 Zbiory danych, zawierające dane osobowe udostępniane są jedynie osobom uprawnionym.

6.2 Upoważnienie do przetwarzania danych osobowych może mieć formę odrębnego dokumentu, wystawionego przez osobę uprawnioną do reprezentacji Firmy lub wyznaczonego pracownika. Uprawnienie może również wynikać z odpowiedniej klauzuli w umowie, stanowiącej podstawę współpracy między osobą uprawnioną a Firmą.

6.3 Firma może w każdym czasie wycofać lub czasowo zawiesić uprawnienie do dostępu do wszystkich lub poszczególnych zbiorów zawierających dane osobowe. Taki sam skutek wiąże się z zakończeniem współpracy z osobą upoważnioną.

6.4 W przypadku zawieszenia lub wycofania upoważnienia, administrator najpóźniej w ciągu 2 dni roboczych odbiera osobie, której odebrano, dostępy do przestrzeni dyskowych, aplikacji, pomieszczeń lub innych miejsc, gdzie przechowywane są zbiory danych osobowych.

6.5 Przetwarzanie danych osobowych w Firmie odbywa się na podstawie polecenia administratora. Polecenie przetwarzania danych musi zostać udokumentowane. Dopuszcza się wydanie polecenia w formie e-mailowej.

6.6 Wzór upoważnienia do przetwarzania danych osobowych stanowi **załącznik nr 3.**

6.7 Wzór polecenia przetwarzania danych osobowych stanowi **załącznik nr 4**.

6.8 Użycie upoważnienia lub wzoru polecenia odbiegającego od wzoru załączonego do niniejszej Polityki wymagają zgody IOD lub Radcy Prawnego świadczącego pomoc prawną dla Spółki.

7. Powierzanie danych osobowych;

7.1 W związku z pracą w ramach sieci Helen Doron, Firma, po uzyskaniu zgody osób uprawnionych wprowadza ich dane osobowe do Aplikacji Helen Doron, powierzając w ten sposób dane osobowe HELEN DORON LTD. Warunkiem wprowadzenia danych do aplikacji jest wyraźna zgoda osób uprawnionych wyrażona na formularzu zgłoszeniowym. W przypadku braku takiej zgody, do Aplikacji Helen Doron należy wprowadzić dane w postaci zanonimizowanej – tj. uniemożliwiającej identyfikację danych konkretnej osoby (np. poprzez wprowadzenie samych inicjałów lub numeru porządkowego).

7.2 Powierzenie danych osobowych dopuszczalne jest w sytuacjach uzasadnionych potrzebami Firmy.

7.3 Przed pierwszym powierzeniem przetwarzania danych osobowych, Firma weryfikuje, czy podmiot, któremu dane zostaną powierzone, gwarantuje realizacje obowiązków wynikających z przepisów prawa oraz posiada warunki i środki zapewniające bezpieczeństwo powierzanych zbiorów danych. W razie wątpliwości, Firma pozyskuje odpowiednie oświadczenie podmiotu przetwarzającego w formie pisemnej lub e-mailowej.

7.4 Potwierdzeniem informacji, o których mowa w pkt 6.3 powyżej może być okazanie przez podmiot przetwarzający wyniku audytu potwierdzającego zgodność procesów przetwarzania z RODO, certyfikacja udzielona przez akredytowany podmiot, udział w kodeksach dobrych praktyk lub oświadczenie osoby uprawnionej do reprezentacji.

7.5 Podstawą do powierzenia danych może być zawarcie umowy powierzenia lub zastosowanie odpowiednich klauzul w umowie o współpracy z podmiotem, który będzie przetwarzał dane w imieniu i na polecenie Firmy.

7.6 Podmiot przetwarzający zobowiązany jest do niezwłocznego informowania Firmy jako administratora o wszelkich zdarzeniach, stanowiących Incydenty Bezpieczeństwa, o wszelkich wystąpieniach osób uprawnionych względem podmiotu przetwarzającego, a w szczególności o żądaniach dotyczących częściowego lub całościowego przetwarzania danych osobowych tych osób jak również o wszelkich innych zdarzeniach, związanych z przetwarzaniem danych, względem których Firma występuje w roli administratora.

7.7 Firma prowadzi rejestr podmiotów, którym powierzono dane osobowe zgodnie z wzorem stanowiącym **załącznik nr 5** do Polityki.

7.8 Wzór umowy powierzenia danych osobowych stanowi **załącznik nr 6** do Polityki. Odstępstwa od wzoru, zmiany we wzorze lub zastosowanie wzoru dostarczonego przez inny podmiot możliwe jest po akceptacji Właściciela lub osoby przez niego wyznaczonej.

8. Udostępnienie danych stronie trzeciej;

8.1 Dopuszcza się, aby Firma w przypadku zaistnienia takiej potrzeby, przekazała dostępy do zbiorów danych lub systemów (aplikacji) IT zawierających dane osobowe podmiotowi, który nie jest odbiorcą tych danych ani nie występuje w roli podmiotu przetwarzającego (Strona Trzecia).

8.2 Warunkiem udostępnienia danych Stronie Trzeciej jest podpisanie uprzednio umowy zawierającej odpowiednie klauzule związane z bezpieczeństwem danych albo umowy NDA oraz upoważnienie Strony Trzeciej do dostępu do danych osobowych;

8.3 Firma weryfikuje prawidłowość korzystania z dostępu do danych oraz podejmuje środki, zapewniające bezpieczeństwo zbiorów danych, do których dostęp otrzymała Strona Trzecia.
8.4 Przykładowy wzór umowy NDA stanowi **załącznik nr 7**

9. Zabezpieczanie zbiorów danych

9.1 Firma stosuje metody organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa zbiorów danych.
9.2 Dostęp do zbiorów danych, zawartych w plikach lub aplikacjach zabezpieczony jest poprzez nadawanie osobom upoważnionym indywidualnych haseł do tych plików lub aplikacji.
9.3 Hasło może być ustalone lub zmienione indywidualnie przez użytkownika aplikacji. Ustalone hasło musi spełniać co najmniej następujące kryteria
a) 8 znaków;
b) W haśle występuje co najmniej jedna wielka litera, jedna cyfra i jeden znak specjalny (np. #,!,@,$,&);
c) Hasło zmieniane jest co najmniej raz na 6 miesięcy.
9.4 Dostęp do zbiorów danych przechowywanych w formie papierowej zabezpieczony jest poprzez zastosowanie zamka lub zamka cyfrowego oraz ograniczony jest do osób upoważnionych, których wykaz prowadzi osoba zarządzająca lub pracownik przez nią wyznaczony.
9.5 W przypadku korzystania z usług podmiotów przetwarzających, Firma pozyskuje co najmniej oświadczenie, że podmiot przetwarzający stosuje środki techniczne i infrastrukturalne w celu zapewnienia bezpieczeństwa powierzonym zbiorom danych. Oświadczenie to może stanowić element umowy stanowiącej podstawę współpracy Firmy z podmiotem przetwarzającym.
9.6 W przypadku przekazywania danych w celach weryfikacji poprawności wykonania zleceń jak również w celach analitycznych i statystycznych do Klientów Firmy, którzy nie są podmiotami przetwarzającymi dane, przekazywane zbiory podlegają pseudonimizacji lub anonimizacji, w taki sposób, iż ustalenie przez tą osobę trzecią tożsamości osób fizycznych, których dane znajdują się z zbiorach nie będzie możliwe.

10. Postępowanie na wypadek naruszeń;

10.1 Przez incydent bezpieczeństwa rozumie się:
a) Naruszenie integralności zbiorów danych;
b) Nieuprawnione usunięcie danych ze zbiorów lub utratę zbiorów danych
c) Uzyskanie dostępu do danych przez osoby nieuprawnione;
d) Kradzież zbiorów danych lub ich części;
10.2 Każda osoba, która powzięła uzasadnione podejrzenie, iż doszło do incydentu bezpieczeństwa, zobowiązana jest do poinformowania o tym Właściciela lub osobę przez niego wyznaczoną.;
10.3 Właściciel lub osoba przez niego wyznaczona weryfikuje, czy do naruszenia doszło oraz czy miało ono charakter istotny;
10.4 Naruszenia o niskiej istotności rejestrowane są wyłącznie w wewnętrznym rejestrze naruszeń, którego wzór stanowi **załącznik nr 8** do Polityki.
10.5 W przypadku naruszeń o istotnym charakterze, Właściciel lub osoba przez niego wyznaczona przeprowadza wewnętrzne postępowanie celem potwierdzenia informacji o naruszeniu, z wyłączeniem sytuacji, gdy naruszenie to ma charakter oczywisty. Oprócz wzmianki w rejestrze naruszeń, w sytuacji naruszenia istotnego Właściciel lub osoba przez

niego wyznaczona sporządza raport dotyczący incydentu bezpieczeństwa, którego wzór stanowi **załącznik nr 9** do Polityki.

10.6 W przypadku potwierdzenia wystąpienia naruszenia, Właściciel informuje o zdarzeniu Prezesa UODO, a jeżeli jest naruszenie może zagrażać prawom i wolnościom osób, których danych incydent dotyczy – w miarę możliwości informowane są również te osoby.

10.7 W przypadku uznania, iż w związku z incydentem konieczne jest poinformowanie Prezesa UODO, informacja ta przekazywana jest w ciągu 72 godzin od momentu potwierdzenia naruszenia w sposób zgodny z wytycznymi opublikowanymi przez UODO.

11. Realizacja dyspozycji osób uprawnionych;

11.1 Osoby uprawnione mogą złożyć następujące dyspozycje w zakresie przetwarzania ich danych osobowych:

a) Udzieleniu informacji w zakresie przetwarzania danych osobowych;
b) Przeniesienia danych osobowych;
c) Ograniczenia zakresu przetwarzania, np. poprzez wyłączenie niektórych celów przetwarzania;
d) Żądanie zaprzestania profilowania danych osobowych;
e) Żądanie zaprzestania podejmowania zautomatyzowanych decyzji opartych na profilowaniu
f) Żądanie zaprzestania przetwarzania danych osobowych (realizacja „prawa do bycia zapomnianym”);

11.2 W przypadku złożenia zapytania o potwierdzenie przetwarzania danych osobowych (np. imienia, nazwiska, numeru telefonu, adresu e-mail) przez jakąkolwiek osobę fizyczną, osoba upoważniona przez Firmę udziela informacji, czy dane są przetwarzane, a w przypadku odpowiedzi pozytywnej, odpowiedź jest uzupełniona o następujące informacje:

a) Od kiedy dane są przetwarzane;
b) Do jakich kategorii zalicza się dane osobowe
c) Jaka jest podstawa przetwarzania (np. zgoda lub realizacja obowiązku prawnego) ewentualnie informacje o źródle danych – jeżeli dane nie zostały zebrane od osoby, której one dotyczą;
d) W jakich celach dane są przetwarzane;
e) W jakiej roli występuje Firma (administrator, podmiot przetwarzający czy odbiorca);
f) Do kiedy dane będą przetwarzane;
g) Czy dane podlegają profilowaniu a jeżeli tak – to w jakich celach;
h) Czy dane zostały udostępnione do odbiorców znajdujących się w państwach trzecich lub organizacjach międzynarodowych
i) Odnośnik do odpowiedniego dokumentu z informacjami o przetwarzaniu lub załączenie tego dokumentu do odpowiedzi;
j) Informację o prawie wniesienia skargi do organu nadzoru

11.3 W razie wątpliwości, osoba wyznaczona przez Firmę ma prawo uzależnić udzielenie informacji od przekazania informacji, które w sposób jednoznaczny potwierdzą, że pytający jest rzeczywiście osobą, której dane są przetwarzane (np. poprzez przesłanie kopii umowy lub weryfikację dodatkowych informacji);

11.4 W przypadku, gdy zapytania od tej samej osoby lub osób reprezentujących tą samą grupę (np. przedstawicieli jednej firmy) powtarzają się w sposób uporczywy, Firma ma możliwość udzielenia kolejnej informacji od złożenia opłaty, odpowiadającej kosztom udzielenia informacji – a w szczególności kosztom pracy osoby, delegowanej do udzielenia informacji.

11.5 W przypadku żądania przeniesienia danych osobowych, Firma realizuje tą dyspozycję, o ile posiada środki techniczne i przeniesienie danych jest możliwe, zaś wskazany odbiorca

danych potwierdzi gotowość do przyjęcia danych oraz wskaże sposób migracji (platformę informatyczną do przekazania danych). Postanowienia ust. 11.3 oraz 11.4 powyżej stosuje się odpowiednio.

11.6 W przypadku otrzymania dyspozycji ograniczenia przetwarzania danych, zaprzestania profilowania danych osobowych lub zaprzestania podejmowania zautomatyzowanych decyzji opartych o profilowanie, Firma realizuje tą dyspozycję nie później niż w ciągu 5 dni roboczych od dnia jej otrzymania. Ust. 11.3 stosuje się odpowiednio.

11.7 W przypadku otrzymania żądania zaprzestania przetwarzania danych osobowych, Firma wykreśla dane osobowe ze wszystkich zbiorów danych, pozostawiając jedynie informacje niezbędne do ochrony przed roszczeniami – tj. dane o sposobie i dacie pozyskania danych osobowych, zakresie przetwarzania, podstawie przetwarzania i dacie otrzymania oraz realizacji dyspozycji usunięcia danych jak również kopie umów. Dane takie przechowywane są przez okres do 11 lat po dacie otrzymania dyspozycji usunięcia danych w celach ewentualnej ochrony interesów prawnych Firmy.

11.8 Wzór rejestru realizacji czynności Osób uprawnionych stanowi **Załącznik nr 10** do Polityki.

11.9 W ramach realizacji prawa do bycia zapomnianym, Firma informuje wszystkich przetwarzających, odbiorców oraz strony trzecie o konieczności usunięcia danych osobowych ze zbiorów, które te dane zawierają;

11.10 Realizacja prawa do bycia zapomnianym następuje w terminie 10 dni roboczych od momentu złożenia takiej dyspozycji przez osobę uprawnioną. Ust. 11.3 stosuje się odpowiednio.

11.11 O wszelkich zmianach w zakresie danych osobowych (w tym o wykreśleniu, skorygowaniu, ograniczeniu celu przetwarzania, zaprzestaniu profilowania) osoba, której zmiana ta dotyczy informowana jest poprzez kontakt mailowy lub telefoniczny – jeżeli Firma nie dysponuje jej adresem mailowym.

12. Współpraca z PUODO

12.1 Za współpracę z PUODO odpowiada Właściciel, lub osoba przez niego uprawniona.

12.2 Na początku kontroli osoba dedykowana do współpracy z PUODO zobowiązana jest do weryfikacji dokumentów potwierdzających fakt reprezentowania PUODO (legitymacja służbowa, upoważnienie do kontroli) oraz określić zakres i termin kontroli. W razie wątpliwości osoba odpowiedzialna weryfikuje uzyskane informacje poprzez kontakt z PUODO.

12.3 Na żądanie PUODO lub przedstawiciela PUODO, Firma udostępnia wszelkie dokumenty oraz informacje związane z przetwarzaniem danych osobowych;

12.4 Pracownicy oraz współpracownicy Firmy zobowiązani są do podjęcia wszelkich działań w celu kompleksowego wyjaśnienia wszelkich okoliczności objętych kontrolą oraz udzielenie kontrolerowi PUODO wsparcia w realizacji zadań objętych zakresem Kontroli.

13. Monitorowanie zgodności;

13.1 Właściciel lub osoba przez niego wyznaczona sprawuje nadzór nad przestrzeganiem Polityki, w tym przechowuje dokumenty i informacje potwierdzające realizację obowiązków z niej wynikających.

13.2 Przynajmniej raz w roku dokonywany jest przegląd procesów pod kątem ich aktualności oraz zgodności z Polityką.

13.3 Przynajmniej raz w roku Firma dokonuje poprzez osobę wyznaczoną weryfikacji zbiorów danych pod kątem danych, których czas przetwarzania upłynął, które straciły podstawę przetwarzania lub nie są już potrzebne dla realizacji celów przetwarzania oraz usuwa takie dane ze zbiorów. Realizacja tego obowiązku potwierdzona zostaje poprzez sporządzenie protokołu lub wysłanie maila do kierownictwa Firmy z informacją o realizacji obowiązku.

a) dane ze zbioru danych pracowników usuwane są po upływie okresu ich przechowywania, wymaganego przepisami prawa;
b) dane finansowo-księgowe (np. faktury, rozliczenia, uzgodnienia sald itp…) usuwane są po upływie okresu ich przechowywania, wymaganego przepisami prawa;
c) dane uczniów i ich opiekunów usuwane są nie później niż po upływie 2 lat od roku, w którym uczeń ukończy 19 rok życia, co wiąże się z możliwością kontynuacji przez ucznia nauki a także umożliwieniu odtworzenia i udostępnienia na jego życzenie dokumentacji związanej z nauką;
d) dane nauczycieli, partnerów franchisingowych, kontrahentów, w tym umowy, korespondencja i załączniki usuwane są nie później niż 15 lat po ustaniu współpracy. Wiąże się to z umożliwieniem ochrony przed roszczeniami wynikającymi z podjętej współpracy w związku ze standardowym, 10-letnim okresem przedawnienia z uwzględnieniem przedawnienia roszczeń dotyczących obowiązku zachowania poufności przez partnera przez 5 lat po zakończeniu współpracy z Firmą.

13.4 Przynajmniej raz w roku dokonywany jest przegląd zgodności dokumentacji dotyczącej przetwarzania – w tym niniejszej Polityki z przepisami prawa, a w szczególności z RODO oraz innymi przepisami dotyczącymi ochrony danych osobowych.

13.5 Właściciel lub osoba przez niego wyznaczona uczestniczy w projektach związanych z projektowaniem lub zmianą procesów, dokonując oceny wpływu procesów na przetwarzanie danych osobowych oraz prawa i wolności osób fizycznych, których dane będą przetwarzane.

13.6 Właściciel lub osoba przez niego wyznaczona może w każdej chwili dokonywać wyrywkowych (ad-hoc) kontroli zgodności działań podejmowanych w imieniu Firmy oraz dokumentów z Polityką oraz przepisami RODO a także innymi przepisami dotyczącymi ochrony danych osobowych.

13.7 Właściciel lub osoba przez niego wyznaczona na wniosek najwyższego kierownictwa jak również z własnej inicjatywy i za zgodą najwyższego kierownictwa może przeprowadzić w każdym czasie audyt zgodności procesów oraz działań Firmy z RODO i innymi przepisami dotyczącymi ochrony danych osobowych.

13.8 Właściciel lub inna osoba przez niego wyznaczona prowadzi szkolenia z ochrony danych osobowych – zarówno dla nowych pracowników lub usługobiorców jak i okresowe szkolenia przypominające. Pracownik lub usługobiorca potwierdza fakt odbycia szkolenia poprzez podpisanie formularza zgodnego z Załącznikiem nr 11 (karta szkolenia). Upoważnienie do dostępu do zbioru zawierającego dane osobowe może być udzielone jedynie pracownikowi/usługobiorcy, który odbył szkolenie.

14. Zastosowanie polityki w sieci franchisingowej MFa.

14.1 Partnerzy franchisingowi (LSF, LCF, IT) zobowiązani są do odpowiedniego stosowania zapisów niniejszej polityki.

14.2 Przez odpowiednie stosowanie rozumiane jest w szczególności:

a) Wprowadzenie techniczno-organizacyjnych metod zabezpieczenia przetwarzanych lub powierzonych zbiorów danych, na poziomie nie niższym, niż opisany w ust. 8 Polityki;
b) Realizacja wobec osób uprawnionych obowiązku informacyjnego;
c) Realizacja żądań osób uprawnionych, zgodnie z treścią Polityki (ust. 10)
d) Realizacja wymogów Polityki w zakresie powierzenia danych oraz nadawania i odbierania dostępów do zbiorów (ust. 5,6,7);
e) Prowadzenie dokumentacji dotyczącej przetwarzania danych osobowych – zgodnie z niniejszą polityką i RODO.

14.3 Partner franchisingowy zobowiązywany jest niezwłoczne (nie później niż w ciągu 24 godzin od momentu powzięcia w tym zakresie informacji) informowanie MF o incydentach bezpieczeństwa dotyczących przetwarzanych zbiorów danych, o wszczęciu kontroli przez PUODO, UOKiK lub inny uprawniony organ publiczny, o wniesieniu powództwa cywilnoprawnego w związku z przetwarzaniem danych a także o wszelkich skargach dotyczących przetwarzania danych osobowych.

14.4 Partner franchisingowy zobowiązany jest do pełnego wsparcia i udzielenia wszelkich informacji w zakresie działań kontrolnych lub postępowań administracyjnych lub cywilnych, w których stroną jest inny partner franchisingowy lub MF, a które dotyczą danych, które są lub były przetwarzane u tego partnera.

14.5 Partner franchisingowy zobowiązany jest do zapoznania swoich pracowników lub osób świadczących na jego rzecz usługi na podstawie umów cywilnoprawnych z niniejszą Polityką oraz przechowywania dowodu realizacji tego obowiązku.

15. Informacje dodatkowe

15.1 Polityka wchodzi w życie z dniem 25 maja 2018 r.

15.2 Do przestrzegania Polityki zobowiązani są wszyscy pracownicy Firmy oraz osoby i podmioty, wykonujące w imieniu i na rzecz dla Firmy zadania na podstawie umów cywiloprawnych;

15.3 Polityka jest poufnym dokumentem wewnętrznym przeznaczonym dla pracowników oraz innych osób upoważnionych przez Firmę.

15.4 W przypadku niezgodności Polityki z RODO lub innymi powszechnie obowiązującymi przepisami, zastosowanie mają przepisy RODO lub innych aktów prawnych, które wchodzą w miejsce postanowień nieważnych. W pozostałej części Politykę stosuje się odpowiednio.

16. Załączniki

16.1 Rejestr czynności przetwarzania
16.2 Rejestr rodzajów czynności przetwarzania
16.3 Wzór upoważnienia do przetwarzania danych osobowych.
16.4 Wzór polecenia przetwarzania danych osobowych.
16.5 Wzór wykazu podmiotów, którym powierzono dane osobowe
16.6 Wzór umowy powierzenia danych osobowych.

16.7 Wzór umowy NDA.
16.8 Wzór rejestru naruszeń bezpieczeństwa danych osobowych.
16.9 Wzór raportu – incydent bezpieczeństwa danych.
16.10 Wzór rejestru zgłoszeń od osób uprawnionych.
16.11 Wzór karty szkoleń w zakresie ochrony danych osobowych