POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Katowice, 25 maja 2018r.

I. Postanowienia ogólne

1. Źródła prawa:

Niniejsza polityka bezpieczeństwa danych osobowych została opracowana w oparciu o powszechnie obowiązujące przepisy prawa z zakresu ochrony danych osobowych i jej treść odpowiada wymaganiom stawianym w szczególności przez przepisy w brzmieniu na dzień sporządzenia niniejszej polityki:

- rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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 95/46/WE, zwanego dalej RODO;
- ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwanej dalej UODO.

2. Cel polityki

Niniejsza polityka określa zasady, procedury oraz środki techniczne i organizacyjne niezbędne w celu zapewnienia ochrony danych osobowych przetwarzanych w spółce GYM FOR YOU sp. z o.o. z siedzibą w Katowicach przed wszelkiego rodzaju zagrożeniami.

Stosowanie zasad oraz wdrożenie procedur, określonych w niniejszej polityce ma na celu zapewnienie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe oraz utrzymania bezpieczeństwa ich przetwarzania.

Przez bezpieczeństwo przetwarzania danych należy rozumieć spełnienie zasad wynikających z art. 5 RODO:

- **zasada zgodności z prawem** –dane osobowe winny być przetwarzane w zgodzie ze wszystkimi normami, w oparciu o przesłankę, która legalizować będzie ten proces,
- **zasada rzetelności i przejrzystości -** przetwarzanie danych winno odbywać się rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
- **zasada ograniczenia celu -** dane osobowe mogą być zbierane jedynie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami,
- **zasada minimalizacji danych -** przetwarzane dane osobowe winny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których odbywa się przetwarzanie,
- **zasada prawidłowości** - przetwarzane dane osobowe winny być prawidłowe i w razie potrzeby uaktualniane; oznacza to konieczność podjęcia wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,
- **zasada ograniczenia przechowywania** - dane osobowe winny być przechowywane w formie, która uniemożliwi identyfikację osoby, której dane dotyczą i wyłącznie przez okres niezbędny do celów przetwarzania,
- **zasada integralności i poufności** - dane osobowe winny być przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed

niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

- **zasada rozliczalności** - co rodzi po stronie administratora danych osobowych obowiązek utrzymywania zdolności do wykazania przestrzegania zasad dotyczących przetwarzania danych osobowych.

3. Definicje

Użyte w treści niniejszej polityki bezpieczeństwa informacji określenia oznaczają:

- **administrator danych osobowych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – w tym wypadku administratorem danych osobowych jest spółka GYM FOR YOU sp. z o.o. z siedzibą w Katowicach (zwana dalej: **„administratorem danych osobowych”**);
- **inspektor ochrony danych (IOD)** – osoba wyznaczona przez administratora danych osobowych, odpowiedzialna w szczególności za zapewnienie przestrzegania przepisów o ochronie danych osobowych;
- **administrator systemu informatycznego (ASI)** – osoba wyznaczona przez administratora danych osobowych, odpowiedzialna w szczególności za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych;
- **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4 pkt 1 RODO);
- **zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- **przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie
- **osoba upoważniona** – osoba posiadająca upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych lub inny podmiot do tego umocowany, w tym upoważniona na podstawie umowy powierzenia danych osobowych;
- **system informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych w celu przetwarzania danych;
- **sieć LAN/WAN** – sieć lokalna/rozległa umożliwiająca połączenie systemów informatycznych przy wykorzystaniu specjalistycznych dedykowanych urządzeń i sieci telekomunikacyjnych;

- **urządzenie przenośne** – urządzenie elektroniczne, pozwalające na przetwarzanie, odbieranie i wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią (m.in. notebook, smartfon);
- **nośnik danych** - przedmiot, na którym możliwe jest zapisanie oraz późniejsze odczytanie informacji, nośnik danych może być odczytany na dowolnym urządzeniu wyposażonym w odpowiedni napęd lub slot;
- **użytkownik** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym;
- **incydent** – każde zdarzenie, które zagraża lub może zagrozić bezpieczeństwu danych osobowych, w tym ich poufności, dostępności lub integralności.

4. Zakres stosowania

Niniejszą politykę stosuje się do wszelkich operacji przetwarzania danych osobowych, w tym do przetwarzania danych w systemach informatycznych oraz zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji.

Dopuszcza się możliwość przyjęcia i stosowania obok niniejszej polityki regulacji szczególnych.

5. Obszar czynności przetwarzania

Wyznacza się niniejszym obszar czynności przetwarzania danych osobowych, zgodnie z Załącznikiem nr 1 do niniejszej polityki.

II. Podmioty zaangażowane w wykonywanie polityki

1. Obowiązki administratora danych osobowych

Administrator danych osobowych obowiązany jest do zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym lub zabraniem przez te osoby oraz przetwarzaniem z naruszeniem prawa, a w tym przed ich nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

Administrator danych osobowych, we współdziałaniu z IOD, jeżeli ten został powołany:

- zapewnia legalność procesów przetwarzania danych osobowych,
- sprawuje nadzór nad zabezpieczeniem danych osobowych,
- na bieżąco identyfikuje i analizuje zagrożenia oraz ryzyko związane z bezpieczeństwem przetwarzanych danych osobowych,
- kontroluje i monitoruje funkcjonowanie zabezpieczeń, wdrożonych w celu ochrony danych osobowych w systemach informatycznych oraz przetwarzanych poza systemami informatycznymi;
- podejmuje działania służące zapobieganiu naruszeń procedur z zakresu ochrony danych osobowych oraz usunięciu skutków tych naruszeń.
- prowadzenie rejestru czynności przetwarzania, zgodnie z wzorem stanowiącym załącznik nr 2 do niniejszej polityki.

2. Inspektor ochrony danych osobowych

Powołuje się IOD. W przypadku niepowołania IOD, wszelkie jego zadania przewidziane niniejszą polityką wykonuje administrator danych osobowych.

Do podstawowych zadań IOD należy:

- sprawdzanie zgodności przetwarzania danych osobowych z przepisami prawa w drodze przeprowadzania okresowych audytów sprawdzających, w tym identyfikacja zagrożeń;
- opracowywanie sprawozdań dla administratora danych osobowych w zakresie zgodności przetwarzania danych osobowych z przepisami prawa;
- nadzorowanie opracowania i aktualizowania wymaganej przepisami prawa dokumentacji przestrzegania zasad przetwarzania danych osobowych;
- zapewnianie zapoznania osób upoważnionych z przepisami o ochronie danych osobowych;

Możliwe jest powierzenie IOD przez administratora danych osobowych innych obowiązków, jeśli nie naruszy to prawidłowego wykonywania podstawowych zadań IOD.

3. Administrator Systemów Informatycznych

Powołuje się ASI. W przypadku niepowołania ASI, wszelkie jego zadania przewidziane niniejszą polityką wykonuje administrator danych osobowych.

Do podstawowych zadań ASI należy:

- wdrażanie w porozumieniu z administratorem danych osobowych nowych rozwiązań technologicznych mających na celu polepszenie standardu ochrony danych osobowych;
- masowe integrowanie oraz migracje danych,
- dbałość o sprawność urządzeń, konserwacja urządzeń i wprowadzanie technicznych zabezpieczeń systemu informatycznego;
- monitorowanie oraz zapewnianie ciągłości działania systemów informatycznych,
- utrzymywanie, konfigurowanie i monitorowanie wydajności systemów informatycznych,
- instalacja i konfiguracja sprzętu i aplikacji,
- administracja oprogramowania systemowego w celu zachowania bezpieczeństwa i integralności systemów informatycznych oraz zabezpieczenia danych a w szczególności danych osobowych przed bezprawnym dostępem osób trzecich,
- konserwacja oprogramowania i systemów informatycznych,
- współpraca z licencjodawcami i innymi dostawcami oprogramowania,
- zarządzanie kopiami zapasowymi, w tym danych osobowych,
- tworzenie oraz usuwanie kont użytkowników,
- nadawanie oraz odbieranie uprawnień użytkownikom,
- monitorowanie częstotliwości zmian hasla użytkowników.

Możliwe jest powierzenie ASI przez administratora danych osobowych innych obowiązków, jeśli nie naruszy to prawidłowego wykonywania podstawowych zadań ASI.

III. Ewidencjonowanie procesów przetwarzania danych osobowych

1. Rejestr czynności przetwarzania danych osobowych

Prowadzi się rejestr czynności przetwarzania danych osobowych. Za prowadzenie rejestru, o którym mowa w zdaniu poprzednim odpowiada administrator danych osobowych.

Rejestr czynności przetwarzania prowadzi się w formie elektronicznej i zamieszcza się w nim:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- 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 RODO, dokumentacja odpowiednich zabezpieczeń;
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Wzór rejestru czynności przetwarzania stanowi załącznik nr 2 do niniejszej polityki.

2. Aktualizacja rejestru

Dokonuje się, co najmniej raz na 12 miesięcy, okresowych przeglądów rejestru przetwarzania danych osobowych pod kątem jego zgodności ze stanem faktycznym.

Osoby odpowiedzialne za procesy biznesowe (kierownicy komórek organizacyjnych), zarządzające zbiorami danych osobowych obowiązane są zgłaszać do administratora danych osobowych wszelkich planowanych zmian struktur zarządzanych przez siebie zbiorów danych osobowych oraz utworzenia nowego zbioru danych.

3. Ocena skutków przetwarzania

Na moment sporządzenia niniejszej polityki nie stwierdza się, aby administrator danych osobowych był zobowiązany do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych – za wyjątkiem monitoringu terenu przy ul. Pławskiej 1b w Brzezince oraz pomieszczeń w budynku, gdzie wydaje się, że ocena skutków przetwarzania jest konieczna (art. 35 ust. 3 lit. c RODO). Ocena skutków przetwarzania w tym zakresie stanowi Załącznik 7 do niniejszej polityki.

Dokonuje się, co najmniej raz na 12 miesięcy, okresowego badania mającego na celu stwierdzenie, czy nie pojawiły się okoliczność wymagające przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

IV. Zarządzanie dostępem do danych osobowych

1. Upoważnienie do przetwarzania danych osobowych oraz ewidencja osób upoważnionych

Do przetwarzania danych osobowych dopuszcza się wyłącznie osoby upoważnione, wpisane do ewidencji osób upoważnionych. Osoby upoważnione zobowiązane są do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.

Upoważnienie dotyczy pracowników Administratora.

Upoważnienia do przetwarzania danych osobowych wydawane są przez administratora danych osobowych lub pośrednio, przez upoważnione przez niego osoby, na wniosek bezpośredniego przełożonego.

Powyższą procedurę stosuje się odpowiednio w sprawach modyfikacji zakresu wydanych już upoważnień.

Zakres upoważnienia związany jest z zajmowanym stanowiskiem lub pełnioną funkcją oraz zakresem obowiązków służbowych ciążących na osobie upoważnionej. Upoważnienia do przetwarzania danych osobowych udzielane są na czas trwania umowy o pracę/umowy cywilnoprawnej, na podstawie której upoważniony jest zatrudniony u administratora danych osobowych.

Ewidencja osób upoważnionych prowadzona jest w formie elektronicznej i zawiera:

- imię i nazwisko osoby upoważnionej;
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
- identyfikator/y w systemie/ach informatycznym/ch, jeżeli upoważnienie obejmuje przetwarzanie danych w systemie informatycznym.

Ewidencję osób upoważnionych prowadzi administrator danych osobowych lub upoważnione przez niego osoby.

Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej polityki.

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszej polityki.

2. Umowy powierzenia przetwarzania danych osobowych.

Ilekroć osoba, której Administrator zamierza powierzyć dane osobowe, nie jest pracownikiem Administratora, ale osobą zatrudnioną przez Administratora na podstawie umowy cywilnoprawnej, nie udziela się takiej osobie upoważnienia, o którym mowa w ust.1, ale podpisuje się z nią umowę powierzenia przetwarzania danych osobowych, która stanowi Załącznik nr 7 do niniejszej polityki.

W umowie powierzenia znajdują się zobowiązania podmiotu przetwarzającego do:

a) przetwarzania danych wyłącznie na udokumentowane polecenie administratora,

b) zapewniania, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

c) podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomagania administratorowi wywiązać się z tych obowiązków,

d) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego – tzw. podpowierzenie przetwarzania danych jest dopuszczalne wyłącznie za zgodą administratora danych,

e) pomagania administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,

f) usunięcia danych lub do zwrotu danych administratorowi danych po zakończeniu przetwarzania, zgodnie z decyzją administratora,

g) udostępnia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów.

Umowa powierzenia może zostać zawarta w formie pisemnej oraz w formie elektronicznej, pod warunkiem zapewnienia integralności i autentyczności dokumentu w postaci elektronicznej.

3. Identyfikator użytkownika w systemie informatycznym

Wszystkim użytkownikom nadaje się w systemach informatycznych odpowiednie identyfikatory. Identyfikator użytkownika w systemie informatycznym nadawany jest przez ASI, na wniosek bezpośredniego przełożonego użytkownika.

Identyfikator użytkownika w systemie informatycznym tworzony jest zgodnie z formatem:

<pierwsza litera imienia i nazwisko>*

bez znaków diakrytycznych

Dopuszcza się odstępstwo od powyższej zasady w uzasadnionych przypadkach, w tym w odniesieniu do systemów informatycznych, dla których przewidziano odmienne zasady tworzenia identyfikatorów.

Nadawane identyfikatory są unikalne. Identyfikator użytkownika, który utracił uprawnienia nie może zostać przydzielony innej osobie, w tym nowemu użytkownikowi.

Identyfikator użytkownika w systemie informatycznym odnotowuje się w prowadzonym rejestrze upoważnień do przetwarzania danych osobowych.

4. Nadawanie uprawnień do przetwarzania danych osobowych w systemie informatycznym

Uprawnienia do przetwarzania danych osobowych w systemie Informatycznym oraz dostępu do jego zasobów nadawane są przez ASI, na wniosek bezpośredniego przełożonego użytkownika, na podstawie wydanego uprzednio upoważnienia do przetwarzania danych osobowych.

Zakres uprawnień nadawanych użytkownikom jest związany z zakresem upoważnienia do przetwarzania danych osobowych przypisanego dla danej kategorii użytkowników, co skorelowane jest z zaszeregowaniem użytkownika w ramach określonej kategorii uprawnień oraz zajmowanym stanowiskiem lub pełnioną funkcją oraz zakresem obowiązków służbowych ciążących na użytkowniku. W uzasadnionych przypadkach ASI może odmówić nadania uprawnień i zwrócić się o podjęcie decyzji w tej sprawie do IOD.

W uzasadnionych przypadkach, w tym w szczególności z uwagi na delegowanie użytkownika do wykonywania określonych zadań, możliwa jest czasowa zmiana zakresu uprawnień użytkownika. Zmiana, o której mowa w zdaniu poprzednim dokonywana jest na wniosek bezpośredniego przełożonego użytkownika po uzyskaniu zgody administratora danych osobowych.

Powyższą procedurę stosuje się odpowiednio w sprawach modyfikacji i cofnięcia nadanych już uprawnień.

O fakcie nadania, modyfikacji lub cofnięciu uprawnień użytkownika ASI informuję drogą elektroniczną bezpośredniego przełożonego użytkownika, których zmiana w zakresie nadanych uprawnień dotyczy oraz IOD.

Uprawnienia użytkowników w zakresie administrowania systemami informatycznymi, w tym uprawnienia ASI nadawane, modyfikowane i wycofywane są za zgodą administratora danych osobowych, wyłącznie przez osobę wyznaczoną przez administratora danych osobowych.

Uprawnienia nadawane są na czas trwania stosunku zatrudnienia u administratora danych osobowych lub innego stosunku prawnego stanowiącego podstawę przyznania uprawnień. W uzasadnionych przypadkach administrator danych osobowych może zdecydować o pozostawieniu aktywnych uprawnień po ustaniu zatrudnienia lub innego stosunku prawnego stanowiącego podstawę przyznania uprawnień.

Prowadzi się matrycę uprawnień nadanych użytkownikom w systemie informatycznym. Matrycę uprawnień, o której mowa w zdaniu poprzednim prowadzi ASI w formie papierowej lub elektronicznej.

5. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

Uwierzytelnianie użytkowników w systemie informatycznym następuje za pomocą indywidualnych, przypisanych do identyfikatorów użytkowników, haseł dostępu, karty RFID lub danych biometrycznych. Stosuje się jednostopniowe uwierzytelnienie, tj. na poziomie dostępu do systemu informatycznego.

Pierwotne hasło dostępu przydzielane jest użytkownikowi przez ASI na etapie przyznawania uprawnień do przetwarzania danych osobowych w systemie informatycznym oraz dostępu do jego zasobów i sieci LAN/WAN oraz do serwera Administratora. Hasło pierwszego logowania przekazywane jest użytkownikowi bezpośrednio, lub identyfikator do systemu poprzez pocztę elektroniczną – natomiast hasło poprzez wiadomość tekstową SMS. Zabronione jest przekazywanie identyfikatora i hasła tym samym źródłem elektronicznym.

Po otrzymaniu pierwotnego hasła dostępu, użytkownik jest obowiązany do jego zmiany, niezwłocznie po zalogowaniu się do systemu informatycznego. Pierwsza i kolejne zmiany hasła dokonywane są przez użytkownika. Zmiana hasła następuje co 30 dni. Użytkownik zobowiązany jest do zmiany hasła co 30 dni również w odniesieniu do systemów informatycznych, które nie wymuszają tego rodzaju zmiany.

Hasło winno składać się co najmniej z 8 znaków i zawierać małe oraz wielkie litery, a także cyfry i znaki specjalne.

Login i hasło użytkownika może być używane wyłącznie przez tego użytkownika, któremu zostały nadane. Przekazywanie loginu i hasła innym osobom jest zabronione. Dotyczy to również haseł, które utraciły swą ważność.

Hasła mogą być przez użytkowników przechowywane wyłącznie w formie zaszyfrowanej, zabezpieczonej hasłem głównym spełniającym ogólne wymogi dotyczące haseł. Zabrania się przechowywania haseł w postaci jawnej.

Na potrzeby wykonywania zadań związanych z administrowaniem systemami informatycznymi, ASI uprawniony jest do uzyskiwania informacji o hasłach dostępu użytkownika w systemach

informatycznych. ASI nadaje użytkownikowi nowe hasło w przypadku utraty hasła obowiązującego.

ASI zapisuje główny identyfikator oraz hasła dostępu po każdej ich zmianie i umieszcza je w kopercie, a następnie przekazuje zamkniętą kopertę do przechowania w wyznaczonym do tego miejscu. Koperta taka może być awaryjnie udostępniona innemu ASI za zgodą IOD. IOD, jeżeli ten został powołany, prowadzi w formie papierowej lub elektronicznej rejestr udostępnionych awaryjnie haseł. Po awaryjnym użyciu hasła dokonuje się jego zmiany.

6. Cofnięcie upoważnień

W razie:

1) rozwiązania stosunku pracy lub innej umowy cywilnoprawnej, na podstawie której zatrudniona jest osoba upoważniona do przetwarzania danych;

2) wystąpienia zagrożenia, iż przetwarzanie danych przez osobę upoważnioną do przetwarzania danych generuje istotne ryzyko wystąpienia naruszenia;

ASI, na wniosek osoby bezpośrednio przełożonej nad osobą upoważnioną do przetwarzania danych, dokonuje niezwłocznie cofnięcia lub zawieszenia wszelkich lub wybranych uprawnień do przetwarzania danych w systemie informatycznym, które taka osoba posiada.

Osobie takiej niezwłocznie cofa się także upoważnienie do przetwarzania danych lub rozwiązuje się z nią umowę powierzenia przetwarzania danych osobowych (zależy, które dotyczy). Za wykonanie tych czynności odpowiada osoba bezpośrednio przełożona nad osobą upoważnioną do przetwarzania danych.

V. Organizacja procesów przetwarzania danych osobowych

1. Procedury rozpoczęcia, zawieszenia i zakończenia pracy z systemem informatycznym

Rozpoczęcie pracy z systemem informatycznym:

Przystępując do pracy z systemem informatycznym użytkownik zobowiązany jest do zweryfikowania, w miarę posiadanej wiedzy i istniejących możliwości, stanu zabezpieczeń stacji roboczej oraz systemu informatycznego.

Zawieszenie pracy z systemem informatycznym:

Użytkownik zobowiązany jest do dokonania blokady stacji roboczej w przypadku tymczasowego zaprzestania pracy z systemem informatycznym połączonego z opuszczeniem stanowiska pracy oraz w każdym przypadku, gdy zachodzi niebezpieczeństwo uzyskania przez osoby nieupoważnione wglądu w wyświetlone na monitorze dane osobowe.

Odblokowanie stacji roboczej następuje po wprowadzeniu identyfikatora użytkownika oraz hasła dostępu lub innego środka uwierzytelniania.

Wprowadza się zabezpieczenie poprzez automatyczne zablokowania stacji roboczej w razie braku aktywności użytkownika przez 5 minut.

Zakończenie pracy z systemem informatycznym:

Zakończenie pracy z systemem informatycznym odbywa się poprzez zamknięcie wszelkich uruchomionych programów i aplikacji oraz przeprowadzenie operacji wylogowania.

Pozostałe zalecenia

Monitory urządzeń służących do przetwarzania danych osobowych znajdujące się w pomieszczeniach, do których dostęp mają osoby nieupoważnione, winny być ustawione w sposób uniemożliwiający tym osobom uzyskanie wglądu do wyświetlanych danych osobowych. Zaleca się zastosowanie filtrów polaryzujących zakładanych na ekrany monitorów, które to uniemożliwią podgląd informacji osobom stojących z boku monitora.

Przetwarzane w systemie informatycznym dane osobowe winny być przechowywane na nośnikach sieciowych (serwer, One Drive, inne podobne i bezpieczne sposoby przechowywania danych), przy jednoczesnym minimalizowaniu przypadków przechowywania danych osobowych na nośnikach lokalnych.

2. Praca z urządzeniami przenośnymi

Użytkownicy wykorzystujący urządzenia przenośne służące do przetwarzania danych osobowych, w tym w szczególności poza obszarem przetwarzania danych osobowych, określonym w załączniku nr 1 do niniejszej polityki, są zobowiązani do:

- transportowania urządzeń przenośnych w
- korzystania tylko i wyłącznie z zaszyfrowanych nośników danych (pendrive, hdd USB)
- sposób minimalizujący ryzyko ich kradzieży, zagubienia lub uszkodzenia;
- przechowywania urządzeń przenośnych w sposób minimalizujący ryzyko ich kradzieży lub uszkodzenia, w tym pod nadzorem osób upoważnionych lub w zamykanych na klucz pomieszczeniach;
- zabezpieczenia urządzeń przenośnych przed dostępem osób nieupoważnionych, w tym pracy z urządzeniami przenośnymi w sposób uniemożliwiający uzyskanie wglądu do przetwarzanych danych osobowych przez osoby nieupoważnione;
- przetwarzania, w tym przechowywania danych osobowych na nośnikach sieciowych (serwer), przy jednoczesnym minimalizowaniu przypadków przechowywania danych osobowych na nośnikach lokalnych (np. dysk twardy urządzenia przenośnego).

3. Praca z urządzeniami drukującymi oraz skanującymi

Użytkownicy korzystający ze współdzielonych urządzeń drukujących i skanujących zobowiązani są do:

- notyfikowania bezpośrednim przełożonym wszelkich awarii urządzeń drukujących;
- nadzorowania procesu wydruku lub skanowania dokumentów (zakaz pozostawiania dokumentów bez nadzoru po zakończeniu procesu ich wydruku lub skanowania).

4. Zarządzanie kopiami zapasowymi danych osobowych oraz systemów informatycznych służących do ich przetwarzania

W celu zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych przyjęto do stosowania zasadę przetwarzania informacji zawartych w bazach danych w oparciu o architekturę klient – serwer. Wynika stąd praktyka przetwarzania danych w bazach danych na dedykowanych dla systemów informatycznych serwerach. Jeśli stosowane dotychczas rozwiązania nie są zgodne z architekturą klient – serwer, zapewnia się możliwość przechowywania gromadzonych za ich pomocą danych na wyznaczonym serwerze plików.

Indywidualne stacje robocze, do których dostęp posiadają użytkownicy stanowią jedynie końcówki klienckie systemu informatycznego. Wszelkie informacje (w tym dane osobowe) przetwarzane przy

pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane bezpośrednio na serwerach. W szczególnych przypadkach, za zgodą administratora bezpieczeństwa informacji, aplikacje oraz dane, w tym dane osobowe, mogą być przechowywane lokalnie na stanowiskach komputerowych niepodłączonych do sieci LAN/WAN. W takich przypadkach obowiązek wykonania kopii zapasowej systemu informatycznego oraz codziennego wykonywania kopii zapasowej bazy danych oraz ich bezpiecznego przechowywania spoczywa bezpośrednio na użytkowniku danej stacji roboczej.

Kopie zapasowe baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonywane są:

- w cyklu dobowym, przy użyciu oprogramowania aplikacji archiwizujących, tworzone są pełne kopie baz danych, w tym plików konfiguracyjnych systemów informatycznych,
- w cyklu miesięcznym tworzony jest automatyczny, pełny backup systemu (łącznie z kopią systemu operacyjnego serwera).

W uzasadnionych przypadkach, za zgodą administratora danych osobowych, dopuszcza się możliwość odstąpienia od stosowania zasad wykonywania kopii zapasowych określonych powyżej.

ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Elektroniczne nośniki informacji zawierające dane osobowe, w tym pamięci flash, dyski optyczne, taśmy magnetyczne i dyski twarde przechowywane są w obszarze przetwarzania danych osobowych określonym w załączniku nr 1 do niniejszej polityki. Po zakończeniu pracy z danym nośnikiem, użytkownik zobowiązany jest do jego zabezpieczenia poprzez umieszczenie w zamykanej szafie lub kasetce.

Elektroniczne nośniki informacji zawierające dane osobowe oznacza się w sposób umożliwiający ich identyfikację.

Elektroniczne nośniki informacji zawierające dane osobowe mogą być przekazywane osobom upoważnionym do przetwarzania danych osobowych w odpowiednim zakresie oraz innym podmiotom wyłącznie za uprzednią zgodą administratora danych osobowych.

Dane osobowe przenoszone z wykorzystaniem elektronicznych nośników informacji usuwa się z tych nośników po ich poprawnym przeniesieniu do miejsca docelowego. Nośniki zawierające nieaktualne dane osobowe oraz nośniki uszkodzone niszczy się w sposób uniemożliwiający odzyskanie zawartych na nich danych.

Przekazywanie i niszczenie elektronicznych nośników informacji służących do przetwarzania danych osobowych odbywa się na podstawie protokołu podpisanego przez ASI oraz właściwych użytkowników. Protokół przekazuje się do administratora bezpieczeństwa informacji.

Nośniki sieciowe (serwer) przechowywane są w odrębnych, zamkniętych pomieszczeniach, specjalnie do tego przeznaczonych, do których dostęp posiadają wyłącznie osoby upoważnione.

Kopie zapasowe danych osobowych oraz systemów informatycznych służących do ich przetwarzania przechowuje się w sposób uniemożliwiający dostęp do tych danych i systemów przez osoby nieupoważnione. Dostęp do kopii zapasowych posiada wyłącznie administrator danych osobowych, IOD oraz ASI.

VI. Bezpieczeństwo danych osobowych

1. Ocena zagrożeń i ryzyk

Identyfikuje się następujące kategorie zagrożeń bezpieczeństwa przetwarzania danych osobowych oraz towarzyszących tym zagrożeniom ryzyk:

- zagrożenia losowe zewnętrzne, obejmujące w szczególności klęski żywiołowe i przerwy w dostawie energii elektrycznej niezależne od administratora danych osobowych, mogą prowadzić do utraty danych lub naruszenia ich integralności;
- zagrożenia losowe wewnętrzne, obejmujące w szczególności błędy ludzkie, awarie sprzętowe, błędy oprogramowania, mogą prowadzić do utraty danych lub naruszenia ich integralności oraz do naruszenia poufności przetwarzanych danych osobowych;
- zagrożenia związane z działaniem zamierzonym osób trzecich, obejmujące wszelkie działania osób trzecich, w tym pracowników administratora danych osobowych, nakierowane na dokonanie czynności naruszających bezpieczeństwo danych osobowych, mogą prowadzić do utraty danych lub naruszenia ich integralności oraz do naruszenia poufności przetwarzanych danych osobowych.

Dokonuje się, nie rzadziej niż raz na 12 miesięcy, okresowego przeglądu ryzyk.

2. Środki techniczne i organizacyjne służące zapewnieniu bezpieczeństwa przetwarzania danych osobowych

Stosuje się określone w tabelach poniżej środki techniczne i organizacyjne służące zapewnieniu bezpieczeństwa przetwarzanych danych osobowych.

<u>Środki techniczne</u>

Środki techniczne	Zabezpieczony obszar	Uwagi
Zamykane szafy	Klub fitness w Oświęcimiu przy ul. Krakowskiej 2A	Są zamykane szafy.
Zamykane szafy	Klub fitness w Katowicach przy ul. Konduktorskiej 37	Są zamykane szafy.
Zamykane pomieszczenia	Klub fitness w Oświęcimiu przy ul. Krakowskiej 2A	Pomieszczenia posiadają drzwi z kluczem, w godzinach pracy ma do nich dostęp serwis sprzątający. Drzwi wejściowe do budynku oraz pomieszczeń GYM FOR YOU nie są antywłamaniowe.

Zamykane pomieszczenia	Klub fitness w Katowicach przy ul. Konduktorskiej 37	Pomieszczenia posiadają drzwi z kluczem, w godzinach pracy oraz po godzinach pracy ma do nich dostęp serwis sprzątający. Drzwi wejściowe do budynku oraz pomieszczeń GYM FOR YOU nie są antywłamaniowe.
Alarm/Monitoring	Klub fitness w Oświęcimiu przy ul. Krakowskiej 2A	W budynku funkcjonuje system alarmowy. Monitorowane są pomieszczenia w budynku za wyjątkiem szatni i strefy wellness, a także teren wokół budynku. Rejestrator i dyski znajdują się w pomieszczeniu Managera w siedzibie GYM FOR YOU (u zarządcy budynku).
Alarm/Monitoring	Klub fitness w Katowicach przy ul. Konduktorskiej 37	W budynku nie funkcjonuje system alarmowy. Monitorowane są pomieszczenia w budynku za wyjątkiem szatni i strefy wellness. Rejestrator i dyski znajdują się w pomieszczeniu Managera w siedzibie GYM FOR YOU (u zarządcy budynku).

Środki organizacyjne

Środki organizacyjne	Dotyczy	Uwagi
Rejestr kluczy	Klub fitness w Oświęcimiu przy ul. Krakowskiej 2A ; Klub fitness w Katowicach przy ul. Konduktorskiej 37	Brak rejestru kluczy i ewidencji wejść i wyjść.
Ewidencja wejść i wyjść		

Karty pracownicze	Klub fitness w Oświęcimiu przy ul. Krakowskiej 2A ; Klub fitness w Katowicach przy ul. Konduktorskiej 37	Brak pracowniczych kart dostępu.
Ochrona	Klub fitness w Oświęcimiu przy ul. Krakowskiej 2A ;	Budynek jest ochraniany po godzinach pracy oraz w weekendy.
Ochrona	Klub fitness w Katowicach przy ul. Konduktorskiej 37	Budynek jest stale ochraniany, ochronę zapewnia zarządca budynku.

3. Procedury wykonywania przeglądów i konserwacji systemów informatycznych oraz nośników informacji służących do przetwarzania danych osobowych

Prawidłowość działania systemów informatycznych służących przetwarzaniu danych osobowych jest monitorowana na bieżąco przez ASI. Niezależnie od powyższego ASI dokonuje cyklicznych sprawdzeń prawidłowości wykonywanych kopii zapasowych.

Prace serwisowe związane z naprawami i konserwacją systemów informatycznych wykonywane są przez ASI lub podmioty trzecie – autoryzowanych dostawców oprogramowania, na podstawie umów łączących te podmioty z administratorem danych osobowych, zawierających odpowiednie postanowienia w przedmiocie powierzenia przetwarzania danych osobowych. Nadzór nad pracami serwisowymi wykonywanymi przez podmioty trzecie, o których mowa w zdaniu poprzednim sprawuje ASI.

Przeglądy urządzeń oraz nośników elektronicznych służących do przetwarzania danych osobowych dokonywane są zgodnie z warunkami gwarancji producentów tych urządzeń i nośników.

Prace serwisowe związane z naprawami i konserwacją urządzeń oraz nośników służących do przetwarzania danych osobowych wykonywane są przez podmioty trzecie, pod nadzorem ASI.

W przypadku konieczności przeprowadzenia prac serwisowych, o których mowa powyżej, w siedzibie podmiotu trzeciego, usuwa się z urządzenia przeznaczonego do konserwacji lub naprawy wszelkie nośniki danych zawierające dane osobowe, a jeżeli nie jest to możliwe, dokonuje się usunięcia przechowywanych na tych nośnikach danych osobowych oraz systemów

informatycznych służących do przetwarzania danych osobowych. Przed przeprowadzeniem operacji usunięcia danych i systemów informatycznych sporządza się kopię zapasową tych danych.

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, w tym dane osobowe, przeznaczone do:

- likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

Odzyskanie utraconych danych z uszkodzonych nośników odbywa się przy udziale ASI. Operacja odzyskiwania utraconych danych może zostać wykonana jedynie przez wyspecjalizowany podmiot zewnętrzny.

Zabrania się dokonywania napraw uszkodzonych elektronicznych nośników danych (np. dysków twardych).

Niedozwolone jest dokonywanie samodzielnych napraw sprzętu służącego do przetwarzania danych osobowych przez osoby nieupoważnione. Każda powstała usterka powinna być zgłoszona kierownikowi odpowiedniej komórki organizacyjnej oraz ASI. Naprawy dokonywane są przez ASI lub wyspecjalizowany podmiot zewnętrzny.

4. Zarządzanie incydentami bezpieczeństwa danych osobowych

Osoba upoważniona oraz każdy inny pracownik zobowiązani są do zgłaszania wszelkich wykrytych incydentów lub niepożądanych zdarzeń związanych z bezpieczeństwem przetwarzania danych osobowych, w trybie i na zasadach określonych niniejszą polityką.

Ocena bezpieczeństwa przetwarzania danych osobowych winna być dokonywana w szczególności na podstawie oceny:

- stanu zabezpieczeń technicznych zastosowanych w celu zabezpieczenia danych osobowych;
- stanu technicznego budynków i pomieszczeń tworzących obszar przetwarzania danych osobowych oraz stanu technicznego ich wyposażenia;
- zawartości zbiorów danych osobowych.

Wszelkie wykryte incydenty winny niezwłocznie zostać zgłoszone bezpośredniemu przełożonemu w formie pisemnej, elektronicznej (e-mail), telefonicznej lub ustnej wraz z określeniem sytuacji i czasu, w jakim zostały one zauważone. O stwierdzonych incydentach informuje się również IOD oraz ASI, jeżeli incydent dotyczy przetwarzania danych w systemie informatycznym. Informację o stwierdzonym incydencie przekazuje do IOD i ASI bezpośredni przełożony osoby zgłaszającej incydent.

Jeżeli istnieje taka możliwość, osoba zgłaszająca incydent winna podjąć akcję korekcyjną, polegającą na doraźnym wyeliminowaniu skutków incydentu. Bezpośredni przełożony osoby zgłaszającej incydent we współdziałaniu z IOD i ASI:

- podejmują czynności niezbędne dla powstrzymania niepożądanych skutków zdarzenia;
- podejmują czynności niezbędne dla ustalenia przyczyn i sprawców zdarzenia;

- podejmują decyzję o wstrzymaniu bieżącej pracy w celu zabezpieczenia miejsca zdarzenia;
- uprawnieni są do uzyskania wyjaśnień od świadków zdarzenia;
- powiadamiają administratora danych osobowych o zaistniałym zdarzeniu.

Jako incydenty kwalifikować należy w szczególności:

- odnotowany brak zabezpieczenia przetwarzanych danych osobowych lub obszaru przetwarzania danych osobowych;
- ujawnienie stosowanych zabezpieczeń danych osobowych osobom trzecim;
- uzyskanie dostępu do przetwarzanych danych przez osobę nieupoważnioną,
- kradzież nośników zawierających dane osobowe,
- nieautoryzowane usunięcie danych osobowych, przy jednoczesnym braku aktualnej kopii zapasowej.

Po wyeliminowaniu bezpośredniego zagrożenia bezpieczeństwa danych osobowych administrator danych osobowych we współdziałaniu z IOD i ASI przeprowadza analizę stanu zabezpieczeń danych osobowych w celu potwierdzenia lub wykluczenia możliwości wystąpienia dalszych naruszeń ochrony danych osobowych, a w szczególności:

- kontroluje stan urządzeń wykorzystywanych do przetwarzania danych osobowych;
- kontroluje zawartość zbioru danych osobowych, którego incydent dotyczył;
- kontroluje sposób działania systemu informatycznego przeznaczonego do przetwarzania danych osobowych, którego incydent dotyczył;
- kontroluje stan zabezpieczeń.

Po przywróceniu prawidłowego stanu zabezpieczeń danych osobowych sporządza się raport zawierający informacje na temat:

- charakteru incydentu wraz ze wskazaniem kategorii i przybliżonej ilości osób, których dane dotyczą oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie;
- miejsca i czasu stwierdzenia wystąpienia incydentu;
- możliwych konsekwencji naruszenia ochrony danych osobowych;
- podjętych środków mających na celu zaradzeniu naruszenia ochrony danych osobowych lub zminimalizowaniu jego ewentualnych skutków;
- rekomendacji środków służących minimalizacji ryzyka wystąpienia tożsamych incydentów w przyszłości.

Niezależnie od powyższego, w przypadku naruszenia ochrony danych osobowych, administrator danych osobowych bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Zgłoszenie to musi co najmniej:

- opisywać okoliczności zdarzenia stanowiącego naruszenie ochrony danych osobowych oraz jego ustalonych lub podejrzewanych przyczyn;
- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli - i w zakresie, w jakim - informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

Administrator danych osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie to jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz musi co najmniej:

- zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie osoby, której dane dotyczą, nie jest wymagane, w następujących przypadkach:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- wymagałoby ono niewspółmiernie dużego wysiłku (w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób).

5. Szkolenia z zakresu ochrony danych osobowych

IOD opracowuje elektroniczne materiały szkoleniowe z zakresu ochrony danych osobowych. Materiały te udostępnia się osobom upoważnionym w zwyczajowo przyjęty sposób.

Osoby upoważnione obowiązane są do zapoznania się z materiałami szkoleniowymi udostępnionymi im w zwyczajowo przyjęty sposób.

Dopuszcza się możliwość podejmowania również innych działań o charakterze szkoleniowym niż opisane powyżej.

VII. Zgoda osób, których dane dotyczą

Ilekroć brak jest innej podstawy przetwarzania danych osobowych, o których mowa w art. 6 RODO, zaś Administrator uznaje przetwarzanie tychże danych za konieczne, pozyskuje się zgodę osoby, której dane dotyczą, na przetwarzania danych osobowych.

Każda zgoda na przetwarzanie danych powinna charakteryzować się następującymi cechami:

a) dobrowolność – zgoda może być ważna tylko jeżeli osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru, przy czym nie zachodzi ryzyko wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji, jeśli nie wyrazi zgody. Jeżeli konsekwencje wyrażenia zgody nie dają się pogodzić ze swobodą wyboru, zgoda nie jest dobrowolna;

b) konkretność – aby zgoda była ważna, musi być konkretna - niedopuszczalna jest ogólna zgoda bez określenia dokładnego celu przetwarzania;

c) świadomość – zgoda na przetwarzanie danych osobowych nie może mieć charakteru abstrakcyjnego, lecz winna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania;

d) jednoznaczność – zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania.

Zgoda winna być wyrażona w formie elektronicznej lub pisemnej.

Zgodę podmiot, którego dane dotycząc, zawsze może odwołać w dowolnej formie – odwołanie ma skutek jedynie na przyszłość.

Przed pobraniem danych osobowych na podstawie zgody osoby, które dane dotyczą, Administrator realizuje obowiązek informacyjny, o którym mowa w art. VIII niniejszej Polityki.

VIII. Obowiązki informacyjne

1. Obowiązek informacyjny

Administrator danych osobowych podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności gdy informacje są kierowane do dziecka - udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa poniżej. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Informacje podawane są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo

- odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

2. **Informacje podawane w przypadku zbierania danych osobowych od osoby, której dane dotyczą**

Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

- swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
- gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;
- cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane

dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa powyżej.

Opisany w niniejszym pkt 2 obowiązek informacyjny nie ma zastosowania, gdy - i w zakresie, w jakim - osoba, której dane dotyczą, dysponuje już tymi informacjami.

Wzór informacji wypełniających obowiązek informacyjny, o którym mowa w niniejszym pkt 2, stanowi Załącznik 5 do niniejszej polityki.

3. **Informacje podawane w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą**

Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:

- swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
- gdy ma to zastosowanie - dane kontaktowe IOD;
- cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
- kategorie odnośnych danych osobowych;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO- prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz - przynajmniej w tych przypadkach

- istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Informacje, o których mowa w niniejszym pkt 3, administrator podaje:

- w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
- jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
- jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w niniejszym pkt 3.

Obowiązek informacyjny, o którym mowa w niniejszym pkt 3, nie ma zastosowania, gdy - i w zakresie, w jakim:

- osoba, której dane dotyczą, dysponuje już tymi informacjami;
- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile obowiązek, o którym mowa w niniejszym pkt 3, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
- pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Wzór informacji wypełniających obowiązek informacyjny, o którym mowa w niniejszym pkt 3, stanowi Załącznik 6 do niniejszej polityki.

IX. Prawa osób, których dane dotyczą

Osoba, które dane dotyczą, ma prawo do:

1) żądania od administratora dostępu do swoich danych osobowych;
2) ich sprostowania, usunięcia lub ograniczenia przetwarzania;

3) wniesienia sprzeciwu wobec przetwarzania;

4) przenoszenia danych;

5) wniesienia skargi do organu nadzorczego.

Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności gdy informacje są kierowane do dziecka - prowadzić z osobą, której dane dotyczą, wszelką komunikację dotyczącą praw tej osoby w zakresie przetwarzania danych osobowych, opisanych w niniejszym Artykule VIII polityki. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw opisanych w niniejszym Artykule VIII polityki.

Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem opisanym w niniejszym Artykule VIII polityki. . W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Komunikacja i działania podejmowane w związku z wykonywaniem praw opisanych w niniejszym Artykule VIII polityki są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
- odmówić podjęcia działań w związku z żądaniem.

X. Postanowienia końcowe

Niniejsza polityka wchodzi w życie z dniem 25 maja 2018r.

Do zapoznania się z niniejszą polityką i jej stosowania zobowiązany jest administrator danych osobowych, IOD oraz wszyscy pracownicy, w tym osoby świadczące usługi na podstawie umów cywilnoprawnych.

Administrator danych osobowych oraz IOD mają prawo do kontroli stosowania określonych niniejszą polityką zasad ochrony danych osobowych w każdym czasie. W zakresie stosowania zasad odnoszących się do pracy w systemach informatycznych, prawo kontroli przysługuje również ASI.

Kierownicy poszczególnych komórek organizacyjnych uprawnieni są do skierowania odpowiedniego wniosku do administratora danych osobowych albo IOD, jeżeli ten został powołany, w przypadku zaistnienia potrzeby wprowadzenia zmian w niniejszej polityce i zmiany obowiązujących zasad przetwarzania danych osobowych.

W zakresie nieuregulowanym w niniejszej polityce, zastosowanie znajdują postanowienia RODO i UODO.

Następujące dokumenty stanowią integralną część niniejszej polityki:

- Załącznik nr 1 – obszar czynności przetwarzania
- Załącznik nr 2 – wzór rejestru czynności przetwarzania danych osobowych;
- Załącznik nr 3 - wzór upoważnienia do przetwarzania danych osobowych;
- Załącznik nr 4 – wzór ewidencji osób upoważnionych do przetwarzania danych osobowych;
- Załącznik nr 5 - wzór informacji wypełniających obowiązek informacyjny w przypadku zbierania danych osobowych od osoby, której dane dotyczą
- Załącznik nr 6 - wzór informacji wypełniających obowiązek informacyjny w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą
- Załącznik 7 – wzór umowy powierzenia przetwarzania danych osobowych
- Załącznik 8 - ocena skutków przetwarzania monitoringu terenu przy ul. Krakowskiej 2A w Oświęcimiu oraz pomieszczeń w budynku

Załącznik 1 - Obszar czynności przetwarzania

Obszarem czynności przetwarzania danych osobowych są:

1) Pomieszczenia administratora danych osobowych przy ul. Krakowskiej 2A w Oświęcimiu
2) Pomieszczenia administratora danych osobowych przy ul. Konduktorskiej 37 w Katowicach

Załącznik 2 – Wzór rejestru czynności przetwarzania danych osobowych

KARTA 1

1. Firma Administratora i jego dane kontaktowe:

Administratorem danych osobowych jest:

GYM FOR YOU Spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach przy ul. Konduktorskiej 33, 40-155 Katowice, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000505211, REGON: 243541101, NIP: 6521724028, o kapitale zakładowym 5.000,00 zł

Adres e-mail: [•]

2. Dane Inspektora Ochrony Danych:

[•]

3. Przetwarzane dane osobowe:

Niniejsza karta rejestru czynności przetwarzania danych osobowych dotyczy następujących danych osobowych:

[•]

Ww. dane osobowe dotyczą następujących kategorii osób:

[•]

4. **Cele przetwarzania danych osobowych:**

Dane osobowe przetwarzane są w następujących celach:

[•]

5. **Kategorie odbiorców, którym dane osobowe zostały lub mogą zostać ujawnione**

Dane osobowe zostały lub mogą zostać ujawnione następującym kategoriom odbiorców:

[•]

6. **Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowych**

Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowych.

7. **Planowane terminy usunięcia danych osobowych**

Dane osobowe będą usuwane w terminie, w jakim zezwalają na to przepisy prawa (jeśli dotyczy) lub z dniem przedawnienia wzajemnych roszczeń administratora oraz osoby, której dane są przetwarzane – w zależności od tego, który z tych terminów przypada później.

8. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.**

[•]

Załącznik nr 3 - wzór upoważnienia do przetwarzania danych osobowych;

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

wydane w dniu [●] przez:

GYM FOR YOU Spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach przy ul. Konduktorskiej 33, 40-155 Katowice, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000505211, REGON: 243541101, NIP: 6521724028, o kapitale zakładowym 5.000,00 zł

zwaną dalej: **Powierzającym**

Panu/Pani [●], zamieszkałemu/ej w [●] przy ul. [●], nr PESEL [●]

zwanym dalej **Upoważnionym**

GYM FOR YOU Spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach posiadająca status administratora danych osobowych, o którym mowa w niniejszym Upoważnieniu, w rozumieniu przepisów Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „Rozporządzenie" lub „RODO"), **powierza niniejszym Upoważnionemu przetwarzanie danych osobowych na zasadach określonych w niniejszym Upoważnieniu:**

1. Upoważniony może przetwarzać dane osobowe wyłącznie w następujących celach:

   [●]
2. Upoważniony może przetwarzać dane osobowe następujących kategorii osób:

   [●]
3. Upoważniony może przetwarzać następujące dane osobowe:

   [●]
4. Upoważniony będzie przetwarzać dane osobowe wyłącznie na obszarze Europejskiego Obszaru Gospodarczego zdefiniowanego w Porozumieniu o Europejskim Obszarze Gospodarczym (Dz. U. UE L z dnia 3 stycznia 1994 r. z późn. zm.).
5. Upoważniony może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Powierzającego, co dotyczy również przekazywania danych do państwa trzeciego lub organizacji międzynarodowej, chyba, że obowiązek przetwarzania danych osobowych nakładają na Upoważnionego przepisy prawa. W takiej sytuacji informuje on Powierzającego przed rozpoczęciem przetwarzania o tym obowiązku, chyba że przepisy te zabraniają udzielania takiej informacji z uwagi na ważny interes publiczny. Za udokumentowane polecenie Powierzającego uznaje się m.in. e-mail lub wiadomość SMS.
6. Upoważniony jest zobowiązany do przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: „UODO"), RODO oraz przepisów wykonawczych do UODO i RODO.
7. Upoważniony bez udokumentowanego polecenia Powierzającego nie może ujawniać ani przekazywać danych komukolwiek.
8. Upoważniony jest zobowiązany do zachowania danych osobowych w tajemnicy. Tajemnica ta obejmuje również wszelkie informacje dotyczące sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych. Obowiązek zachowania tajemnicy jest bezterminowy, tj. istnieje także po zakończeniu obowiązywania niniejszej Umowy. W momencie ustania stosunku pracy/stosunku cywilnoprawnego pomiędzy Powierzający a Upoważnionym (z jakiegokolwiek powodu), Upoważniony jest zobowiązany do zwrotu Powierzającemu wszelkich powierzonych mu danych, w tym wszelkich nośników materialnych, na których te dane się znajdują.
9. Upoważniony jest zobowiązany do niezwłocznego (nie później niż 24h od wykrycia naruszenia) poinformowania Powierzającego o naruszeniu ochrony danych osobowych.
10. Niniejsze upoważnienie wygasa z chwilą ustania (z jakiejkolwiek przyczyny) umowy o pracę/umowy cywilnoprawnej, na podstawie której Upoważniony jest zatrudniony u Powierzającego.
11. Naruszenie przez Upoważnionego postanowień niniejszego Upoważnienia lub postanowień UODO, RODO lub aktów wykonawczych skutkuje możliwością wypowiedzenia ze skutkiem natychmiastowym umowy cywilnoprawnej, na podstawie której zatrudniony jest Upoważniony/rozwiązania stosunku pracy bez wypowiedzenia z powodu ciężkiego naruszenia podstawowych obowiązków pracowniczych przez Upoważnionego.
12. Zmiana niniejszego Upoważnienia może nastąpić tylko w formie pisemnego aneksu, pod rygorem nieważności.

13. Upoważniony zgadza się na przyjęcie niniejszego Upoważnienia i zobowiązuje się do postępowania zgodnie z jego postanowieniami oraz przepisami UODO, RODO i aktów wykonawczych.

Powierzający **Upoważniony**

Załącznik nr 4 – wzór ewidencji osób upoważnionych do przetwarzania danych osobowych;

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

U ADMINISTRATORA:

GYM FOR YOU SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Z SIEDZIBĄ W KATOWICACH

Lp.	Imię i nazwisko	Data nadania	Data ustania	Zakres upoważnienia	Identyfikator w systemie informatycznym
1					
2					
3					
4					
5					
6					
7					

Załącznik nr 5 - wzór informacji wypełniających obowiązek informacyjny w przypadku zbierania danych osobowych od osoby, której dane dotyczą

Szanowny Panie/Szanowna Pani,

Zamierzamy pozyskać Pańskie/Pani dane osobowe, dlatego też, zgodnie z art. 12 i art. 13 Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „Rozporządzenie" lub „RODO") podajemy Panu/Pani następujące informacje:

1) GYM FOR YOU Spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach przy ul. Konduktorskiej 33, 40-155 Katowice, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000505211, REGON: 243541101, NIP: 6521724028 posiada status administratora danych osobowych (dalej zwana będzie: Administratorem).

   Punkt kontaktowy – do kontaktu z Administratorem: [●]

2) Administrator nie powołał Inspektora Ochrony Danych.

3) Dane osobowe przetwarzane są w następujących celach:

   [●]

   Na podstawie [●] RODO.

   Prawnie uzasadnione interesy realizowane przez Administratora to: [●]

4) Kategorie odbiorców danych osobowych to:

   [●]

5) Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

6) Dane osobowe będą usuwane w terminie, w jakim zezwalają na to przepisy prawa (jeśli dotyczy) lub z dniem przedawnienia wzajemnych roszczeń administratora oraz osoby, której dane są przetwarzane – w zależności od tego, który z tych terminów przypada później;

7) Posiada Pan/Pani prawo do żądania od Administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także o prawo do przenoszenia danych;

8) Jeśli przetwarzanie danych odbywa się na podstawie Pana/Pani zgody, posiada Pan/Pani prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

9) Posiada Pan/Pani prawo do wniesienia skargi do organu nadzorczego;

10) Podanie danych osobowych jest wymogiem umownym oraz warunkiem zawarcia umowy oraz iż jestem zobowiązana/y do ich podania, a w razie braku ich podania – umowa pomiędzy mną a Administratorem lub jednym ze współadministratorów nie może zostać zawarta;

11) Administrator nie stosuje zautomatyzowanego podejmowania decyzji, w tym nie stosuje profilowania.

Załącznik nr 6 - wzór informacji wypełniających obowiązek informacyjny w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą

Szanowny Panie/Szanowna Pani,

Pozyskaliśmy Pańskie/Pani dane osobowe, dlatego też, zgodnie z art. 12 i art. 14 Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „Rozporządzenie" lub „RODO") podajemy Panu/Pani następujące informacje:

1) GYM FOR YOU Spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach przy ul. Konduktorskiej 33, 40-155 Katowice, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000505211, REGON: 243541101, NIP: 6521724028 posiada status administratora danych osobowych (dalej zwana będzie: Administratorem).

   Punkt kontaktowy – do kontaktu z Administratorem: [●]

2) Administrator nie powołał Inspektora Ochrony Danych.

3) Dane osobowe przetwarzane są w następujących celach:

   [●]

   Na podstawie [●] RODO.

   Prawnie uzasadnione interesy realizowane przez Administratora to: [●]

4) Kategorie przetwarzanych danych osobowych to:

   [●]

5) Kategorie odbiorców danych osobowych to:

[●]

6) Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

7) Dane osobowe będą usuwane w terminie, w jakim zezwalają na to przepisy prawa (jeśli dotyczy) lub z dniem przedawnienia wzajemnych roszczeń Administratora oraz osoby, której dane są przetwarzane – w zależności od tego, który z tych terminów przypada później

8) Ma Pan/Pani prawo do żądania od Administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub prawo do wniesienia sprzeciwu wobec przetwarzania, a także o prawo do przenoszenia danych

9) Jeśli przetwarzanie danych odbywa się na podstawie Pana/Pani zgody, posiada Pan/Pani prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

10) Ma Pan/Pani prawo do wniesienia skargi do organu nadzorczego

11) Administrator nie stosuje zautomatyzowanego podejmowania decyzji, w tym nie stosuje profilowania.

12) Źródło, z którego Administrator pozyskał Pańskie/Pani dane osobowe to : [●]

Załącznik 7 – wzór umowy powierzenia przetwarzania danych osobowych

UMOWA

POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu [●] w [●] pomiędzy:

GYM FOR YOU Spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach przy ul. Konduktorskiej 33, 40-155 Katowice, wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000505211, REGON: 243541101, NIP: 6521724028, o kapitale zakładowym 5.000,00 zł

zwanądalej: **Powierzającym**

a

[●] z siedzibą w [●] ([●]), wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w [●] pod numerem KRS: [●], NIP: [●], REGON: [●], o kapitale zakładowym [●] zł, reprezentowaną przez:

(1) [●]

(2) [●]

opcjonalnie w przypadku osób fizycznych;

[●] prowadzącym/ą działalność gospodarcza pod firmą [●] z siedzibą w [●] wpisanym/ą do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, NIP [●], PESEL [●]

zwanym/ą dalej **Procesorem**

zwanymi dalej również łącznie **„Stronami”** lub każda z osobna **„Stroną”**.

§1

1. GYM FOR YOU Spółka z ograniczoną odpowiedzialnością z siedzibą w Katowicach posiada status administratora danych osobowych, o których mowa w niniejszej umowie, w rozumieniu przepisów Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „Rozporządzenie” lub „RODO”).

2. Powierzający w rozumieniu art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: „UODO”) oraz art. 28 ust. 3 i 4 RODO powierza Procesorowi przetwarzanie danych osobowych na zasadach określonych w niniejszej Umowie.

3. Procesor może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Powierzającego, co dotyczy również przekazywania danych do państwa trzeciego lub organizacji międzynarodowej, chyba, że obowiązek przetwarzania danych osobowych nakładają na Procesora przepisy prawa. W takiej sytuacji informuje on Powierzającego przed rozpoczęciem przetwarzania o tym obowiązku, chyba że przepisy te zabraniają udzielania takiej informacji z uwagi na ważny interes publiczny. Za udokumentowane polecenie Powierzającego uznaje się m.in. e-mail lub wiadomość SMS.

§2

1. Niniejsza Umowa zawarta jest w celu wykonania umowy [●] z dnia [●], albowiem do wykonania tej ostatniej przez Procesora konieczne jest przetwarzanie przez Procesora danych osobowych, o których mowa w niniejszym paragrafie.
2. Procesor może przetwarzać dane osobowe wyłącznie w następujących celach:

   [●]
3. Procesor może przetwarzać dane osobowe następujących kategorii osób:

   [●]
4. Procesor może przetwarzać następujące dane osobowe:

[●]

5. Procesor będzie przetwarzać dane osobowe wyłącznie na obszarze Europejskiego Obszaru Gospodarczego zdefiniowanego w Porozumieniu o Europejskim Obszarze Gospodarczym (Dz. U. UE L z dnia 3 stycznia 1994 r. z późn. zm.).

§3

Procesor jest zobowiązany do przestrzegania przepisów UODO, RODO oraz przepisów wykonawczych do UODO i RODO, w tym w szczególności Procesor jest zobowiązany do przedsięwzięcia wszelkich środków (w tym organizacyjnych i technicznych) niezbędnych do wywiązania się z przestrzegania ww. przepisów prawa.

§4

1. Powierzający ma prawo do kontroli sposobu wykonywania niniejszej Umowy przez Procesora odnośnie zobowiązań, o których mowa w niniejszej Umowie. Warunkiem przeprowadzenia kontroli jest zawiadomienie Procesora w terminie nie krótszym niż 3 dni przed planowanym terminem jej przeprowadzenia.
2. Procesor zobowiązuje się udostępnić Powierzającemu wszelkie informacje niezbędne do wykazania spełnienia nałożonych na niego niniejszą Umową zobowiązań.
3. Procesor zobowiązuje się umożliwić Powierzającemu lub audytorowi przez nich upoważnionemu przeprowadzanie audytów, w tym inspekcji, i pomagać w ich przeprowadzeniu.
4. Uprawnienia określone niniejszym § 4 przysługują Powierzającemu lub właściwemu administratorowi odpowiednio w stosunku do Podwykonawców, o których mowa w § 7 ust. 1 niniejszej Umowy, w przypadku powierzenia przez Procesora przetwarzania danych Podwykonawcom, zgodnie z § 7 Umowy. Procesor zobowiązuje się zapewnić takie uprawnienia dla Powierzającego w umowach zawartych z Podwykonawcami.

§5

1. Procesor zobowiązuje się do posiadania odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa przetwarzania danych uwzględniający stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
2. Środki, o których mowa w ustępie poprzednim, to między innymi w stosownych przypadkach:
   a) pseudonimizacja i szyfrowanie danych osobowych;
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

§6

1. Biorąc pod uwagę charakter przetwarzania danych, Procesor zobowiązuje się do pomocy Powierzającemu, poprzez odpowiednie środki techniczne i organizacyjne, w

wywiązaniu się z obowiązku odpowiedzi na żądania osoby, której dane dotyczą, w szczególności w zakresie wykonywania jej praw określonych w Rozdziale III RODO.

2. Biorąc pod uwagę charakter przetwarzania danych oraz posiadane informacje, Procesor zobowiązuje się do pomocy Powierzającemu w zakresie wywiązywania się z obowiązków wymienionych w art. 32-34 w Sekcji 2 i art. 35-36 Sekcji 3 Rozdziału IV Rozporządzenia, tj. w szczególności dotyczących wdrażania odpowiednich środków technicznych i organizacyjnych, zgłaszania naruszenia ochrony danych osobowych przez Powierzającego organowi nadzorczemu oraz osobie, której dane dotyczą, co oznacza udzielenie Powierzającemu, na każde jego żądanie i we wskazanym przez niego terminie, wszelkich wyjaśnień i innych form wsparcia, w tym informacji o stanie faktycznym, które pomogą Powierzającemu w spełnieniu jego obowiązków wynikających z przepisów RODO.
3. Procesor zobowiązuje się niezwłocznie informować Powierzającego, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie przepisów RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych osobowych.

§7

1. Powierzający wyraża zgodę, aby Procesor powierzył dalej przetwarzanie danych osobowych (dalej "Podpowierzenie") i wykonywanie zadań wynikających z Umowy podmiotowi trzeciemu (dalej "Podwykonawca"), pod warunkami (spełnionymi łącznie), że:
   a) Procesor powiadomi uprzednio Powierzającego, mailem lub w formie pisemnej, o swoim zamiarze Podpowierzenia;
   b) Powierzający zachowuje prawo sprzeciwu wobec zamiaru Podpowierzenia lub zmiany jego warunków przez Procesora;
   c) zakres i cel Podpowierzenia nie będzie szerszy niż wynikający z Umowy;
   d) przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Powierzającego zostaną zachowane w umowie Podpowierzenia odpowiednio do warunków, opisanych w niniejszej Umowie;
   e) Podpowierzenie będzie niezbędne dla realizacji celów związanych z procesami lub projektami wynikającymi z Umowy;
   f) Podpowierzenie nie naruszy interesów Powierzającego ani osób, których dane osobowe są przetwarzane;
   g) umowa Podpowierzenia zostanie zawarta z Podwykonawcą na piśmie, zgodnie z obowiązującymi przepisami dotyczącymi powierzania przetwarzania danych osobowych z zastrzeżeniem, że wszelkie obowiązki Procesora, wynikające z niniejszej Umowy, Procesor zastosuje odpowiednio do Podwykonawcy w umowie Podpowierzenia;
   h) Podwykonawca spełnia obowiązki wynikające z przepisów RODO, nakładane bezpośrednio na podmiot przetwarzający w rozumieniu Rozporządzenia, w tym w szczególności wdrożenia środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych, o których mowa w §4 i §5 niniejszej Umowy.
2. Procesor w umowie Podpowierzenia zobowiąże Podwykonawców do przestrzegania przy przetwarzaniu powierzonych danych obowiązków dotyczących ochrony danych na poziomie, co najmniej określonym w niniejszej Umowie oraz w przepisach RODO.

3. Jeżeli Podwykonawca nie wywiąże się ze spoczywających na nim obowiązków określonych w niniejszej Umowie, UODO lub RODO, pełna odpowiedzialność wobec Powierzającego za wypełnienie tych obowiązków spoczywa na Procesorze, który odpowiada za działania Podwykonawcy jak za działania własne.

§8

1. Procesor oświadcza, że każda osoba (np. pracownik etatowy, osoba świadcząca czynności na podstawie umów cywilnoprawnych, inne osoby wykonujące czynności na rzecz Procesora), która zostanie dopuszczona do przetwarzania powierzonych przez Powierzającego danych osobowych zostanie zobowiązana do zachowania tych danych w tajemnicy. Tajemnica ta obejmuje również wszelkie informacje dotyczące sposobów zabezpieczenia powierzonych do przetwarzania danych osobowych. Do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia zobowiązany jest także Procesor, a samo zobowiązanie obejmuje podmioty, wymienione w niniejszym ustępie bezterminowo, tj. także po zakończeniu obowiązywania niniejszej Umowy. Postanowienia dotyczące zachowania tajemnicy, o której mowa w niniejszym ustępie, Procesor ma obowiązek stosować odpowiednio także wobec swoich Podwykonawców i osób dopuszczonych przez Podwykonawców do przetwarzania danych osobowych.
2. Procesor po ustaniu z jakiejkolwiek przyczyny umowy opisanej w § 2 ust. 1 Umowy zobowiązany jest do niezwłocznego zwrotu powierzonych mu danych oraz do usunięcia wszystkich ich istniejących kopii, sporządzonych na potrzeby bieżącej pracy, bądź na wyraźne żądanie Powierzającego – dokonać usunięcia powierzonych danych osobowych, zamiast ich zwrotu, chyba, że przepisy prawa nakazują przechowywanie danych osobowych. Na każde życzenie Powierzającego, Procesor ma obowiązek przedstawić w terminie 5 dni pisemny protokół potwierdzający fakt zniszczenia danych osobowych. Sposób zakończenia przetwarzania danych osobowych po sfinalizowaniu realizacji usług na rzecz Powierzającego, opisany w niniejszym ustępie, Procesor powinien wskazać odpowiednio swoim Podwykonawcom, w przypadku Podpowierzenia. Do czasu bezpowrotnego usunięcia danych osobowych przez Powierzającego oraz jego Podwykonawców postanowienia niniejszej Umowy znajdują zastosowanie.

§9

1. Procesor oświadcza, że w razie stwierdzenia naruszenia ochrony danych osobowych niezwłocznie (nie później niż 24h od wykrycia naruszenia) poinformuje o tym Powierzającego.
2. Zgłoszenie, o którym mowa w ust. 1 musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez Procesora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

4. W celu realizacji obowiązków, o których mowa w ust. 1 i 2 powyżej, Procesor jest zobowiązany do dokumentowania wszelkich okoliczności i zebrania wszelkich dowodów, które pomogą Powierzającemu wyjaśnić szczegóły naruszenia, w tym jego charakter, skalę, skutki, czas zdarzenia, osoby odpowiedzialne, osoby poszkodowane.

§10

1. Procesorowi przysługuje prawo kierowania zapytań do Powierzającego w zakresie prawidłowości wykonania przez Procesora obowiązków dotyczących zabezpieczenia powierzonych mu na podstawie niniejszej Umowy danych.
2. Powierzający zobowiązuje się udzielić odpowiedzi na zapytanie, o którym mowa w ust. 1 w terminie 7 dni od daty wpłynięcia zapytania. Udzielenie odpowiedzi może nastąpić w formie elektronicznej.

§11

1. Procesor odpowiada za szkody majątkowe lub niemajątkowe jakie powstały wobec Powierzającego lub osób trzecich w wyniku przetwarzania danych osobowych niezgodnego z Umową lub obowiązkami nałożonymi przez Ustawę lub Rozporządzenie bezpośrednio na Procesora oraz w wyniku działania poza zgodnymi z prawem instrukcjami Powierzającego lub wbrew tym instrukcjom. W razie wyrządzenia szkody przez Procesora, Procesor zwolni Powierzającego w najszerszym możliwym zakresie dozwolonym przez obowiązujące prawo z roszczeń osób poszkodowanych, a także pokryje koszty obsługi prawnej Powierzającego związane z obsługą roszczeń poszkodowanych oraz zwróci koszty sądowe, którymi Powierzający zostanie obciążony.
2. Powierzający odpowiada za szkody majątkowe lub niemajątkowe, jakie powstały wobec osób trzecich w wyniku przetwarzania danych naruszającego Rozporządzenie lub inne przepisy dotyczące ochrony danych osobowych.
3. Jeżeli w tym samym przetwarzaniu biorą udział obie Strony i są odpowiedzialne za szkodę spowodowaną przetwarzaniem zgodnie z ust. 1 i ust. 2, ponoszą one odpowiedzialność solidarną. Strona, która zapłaciła odszkodowanie za całą wyrządzoną wspólnie szkodę, ma prawo żądania od drugiej Strony, która uczestniczyła w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponosi odpowiedzialność, zgodnie z warunkami określonymi w ust. 1 i ust. 2.
4. Procesor ponosi odpowiedzialność za działania lub zaniechania Podwykonawcy, dotyczące przetwarzania powierzonych danych osobowych, jak za działania lub zaniechania własne, przez co postanowienia dotyczące odpowiedzialności Procesora na warunkach opisanych powyżej obejmują także odpowiedzialność Procesora za działania lub zaniechania jego Podwykonawców.

§12

1. Strony oświadczają, że zawierają niniejszą Umowę na czas trwania umowy, o której mowa w §2 ust. 1.
2. Powierzający ma prawo wypowiedzieć Umowę w trybie natychmiastowym, gdy Procesor:
   a) przetwarza dane osobowe w sposób niezgodny z Umową, na co Powierzający zwróci Procesorowi uwagę na piśmie, a Procesor w wyznaczonych przez Powierzającego terminie nie usunie wskazanych naruszeń,
   b) przetwarza dane osobowe niezgodnie z przepisami UODO, RODO lub aktów wykonawczych, na co Powierzający zwróci Procesorowi uwagę na piśmie, a Procesor w wyznaczonych przez Powierzającego terminie nie usunie wskazanych naruszeń.
3. Wypowiedzenie niniejszej Umowy na podstawie jej § 12 ust.2 powoduje możliwość wypowiedzenia ze skutkiem natychmiastowym lub odstąpienia przez Procesora od umowy, o której mowa w §2 ust. 1.

§13

1. Zmiana niniejszej Umowy może nastąpić tylko w formie pisemnego aneksu, pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą umową mają zastosowania przepisy UODO, RODO oraz kodeksu cywilnego.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
4. Umowa wchodzi w życie z dniem podpisania.
5. Z chwilą wejścia w życie niniejszej Umowy tracą moc wszelkie wcześniejsze uzgodnienia (pisemne, ustne, w formie dokumentowej) poczynione między Stronami, a dotyczące kwestii przetwarzania danych osobowych wyszczególnionych w niniejszej Umowie.
6. Jeśli jedno lub kilka postanowień niniejszej Umowy z jakiegoś powodu zostanie (zostaną) uznany/e za nieważny/e lub niemożliwy/e do wprowadzenia w życie pod jakimś względem, to ta nieważność, niezgodność z prawem lub niemożność wprowadzenia w życie nie będą mieć wpływu na żadne inne postanowienie niniejszej Umowy, ale Umowa będzie tak interpretowana, jak gdyby takie nieważne, niezgodne z prawem lub niemożliwe do wprowadzenia w życie postanowienie nigdy nie zostało wprowadzone, a Umowa będzie realizowana w sposób możliwie najbliższy, zgodnie z intencją obu Stron.

Powierzający **Procesor**

Załącznik 8 - Ocena skutków przetwarzania monitoringu terenu przy ul. Krakowskiej 2A w Oświęcimiu oraz pomieszczeń w budynku