POLITYKA BEZPIECZEŃSTWA INFORMACJI

w spółce działającej pod firmą

"4 Results Spółka z ograniczoną odpowiedzialnością" z siedzibą w Warszawie

Niniejsza Polityka bezpieczeństwa, zwana dalej "Polityką", została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym z Rozporządzaniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej: "RODO").

Definicje:

1.	**Administrator Danych**	4 Results Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie przy ulicy Puławskiej 457 Warszawie (02 - 844), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000242220
2.	**Dane osobowe**	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3.	**Użytkownik**	osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych,
4.	**Przetwarzanie danych**	jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych**,**
5.	**Identyfikator Użytkownika**	ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do Przetwarzania danych osobowych w systemie informatycznym (Użytkownika),
6.	**Hasło**	ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi).

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w spółce 4 Results Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie (adres: Puławska 457, 02 - 844 Warszawa), niezależnie od formy ich przetwarzania (przetwarzanie tradycyjne zbiory ewidencje, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.

2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.

3. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:

   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,

   b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,

   c) monitorowanie zastosowanych środków ochrony.

4. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszenie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi i wewnętrznymi.

5. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u administratora danych

1. Dane osobowe mogą być gromadzone i przetwarzane w systemach informatycznych oraz w zbiorach papierowych takich jak kartoteki, księgi, wykazy, czy innych zbiorach ewidencyjnych.

2. Ochronie podlegają dane, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.

3. Administrator Danych prowadzi rejestr czynności przetwarzania danych osobowych.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych u Administratora Danych.

2. Wszystkie dane osobowe są Przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przepisami prawa:

   a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla Przetwarzania danych,

   b) dane osobowe są Przetwarzane rzetelnie i w sposób przejrzysty,

   c) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie Przetwarzane dalej w sposób niezgodny z tymi celami,

   d) dane osobowe są Przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych,

   e) dane osobowe są prawidłowe i w razie potrzeby uaktualniane,

   f) czas przechowywania Danych osobowych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane,

   g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO,

   h) dane osobowe są zabezpieczone przed naruszeniami zasad ich ochrony.

3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:

   a) naruszenie bezpieczeństwa systemów informatycznych, w których Przetwarzane są Dane osobowe,

   b) udostępnienie lub umożliwienie udostępnienia danych osobom lub podmiotom do tego nieuprawnionym,

   c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia Danym osobowym ochrony,

   d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia,

   e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania,

   f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych,

   g) naruszenie praw osób, których dane są przetwarzane.

4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony Danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.

5. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:

   a) pracownicy byli odpowiednio przygotowani do swoich obowiązków,

   b) każdy przetwarzający Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z "Upoważnieniem do przetwarzania danych osobowych", stanowiący Załącznik Nr 1 do niniejszej Polityki Bezpieczeństwa,

   c) każdy pracownik (współpracownik) przetwarzający Dane osobowe został zapoznany ze stosowanymi przepisami w tym zakresie (w szczególności RODO oraz Polityką Bezpieczeństwa), a także podjął stosowne zobowiązania, wedle Załącznika Nr 3 do niniejszej Polityki Bezpieczeństwa.

6. Pracownicy i współpracownicy zobowiązani są do:

   a) ścisłego przestrzegania zakresu nadanego upoważnienia,

   b) przetwarzania i ochrony danych osobowych zgodnie z przepisami,

   c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,

   d) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych w jednostce,

   e) ochrony danych osobowych przez przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem, dostępem do danych osobowych oraz przetwarzaniem,

   f) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

IV. <u>Zasady przetwarzania danych osobowych, realizacja obowiązków informacyjnych</u>

1. Przetwarzanie danych osobowych jest jedynie dopuszczalne w następujących przypadkach:

   a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,

   b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze Danych,

   c) jest niezbędne osobie, której dane dotyczą w celu wywiązania się z umowy, której jest stroną lub jej życzenie w celu podjęcia niezbędnych działań przed zawarciem umowy,

d) jest niezbędne do wykonania określonych prawem zadań, realizowanych w interesie publicznym,

e) przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych.

2. W przypadku zbierania danych osobowych od osoby, której one dotyczą, pracownik/współpracownik podczas pozyskiwania danych osobowych zobowiązany jest podać jej następujące informacje:

a) nazwę, adres i dane kontaktowe spółki jako Administratora Danych,

b) cele przetwarzania tych danych oraz podstawę prawną przetwarzania,

c) jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez spółkę, należy wykazać ten interes,

d) informacje o odbiorcach danych osobowych lub kategoriach odbiorców jeżeli istnieją,

e) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia tego okresu,

f) informacje o prawie żądania od administratora dostępu do swoich danych oraz ich poprawienia, usunięcia lub ograniczenia przetwarzania, o prawie wniesienia sprzeciwu wobec ich przetwarzania, a także o prawie do przenoszenia danych,

g) jeżeli podstawą przetwarzania jest zgoda - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed cofnięciem,

h) informację o prawie wniesienia skargi do organu nadzorczego,

i) informację, czy podanie danych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualnie konsekwencje niepodania danych.

3. W przypadku zbierania danych osobowych w sposób inny niż od osoby, której one dotyczą, pracownik/współpracownik, który takie dane pozyskał powiadamia osobę, której dane dotyczą w zakresie opisanym w ust. 2 powyżej, a ponadto informuję ją o kategoriach odnośnych danych osobowych oraz o źródle pochodzenia tych danych.

4. Obowiązek informacyjny spoczywa na pracowniku/współpracowniku odpowiedzialnym za załatwienie sprawy i w pełnym zakresie dotyczy tradycyjnych form korespondencji.

5. W przypadku korespondencji przesyłanej drogą elektroniczną, w wiadomości e - maila wysyłanego prze pracownika zamieszcza się informację dotyczącą ochrony danych osobowych.

6. Obowiązek informacyjny realizują również pracownicy Spółki w ramach rozmów telefonicznych prowadzonych z klientami (osoby fizyczne), o ile w ten sposób pozyskują dane osobowe.

7. Obowiązku informacyjnego nie stosuje się w przypadku, gdy osoba której dane dotyczą dysponuje już tymi informacjami.

8. W przypadku, jeżeli dane osobowe pozyskiwane są w sposób inny niż od osoby, której dane dotyczą, obowiązku informacyjnego nie stosuje się wtedy, gdy:

   a) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, a w szczególności w przypadku przetwarzania do celów archiwalnych, w interesie publicznym, do celów badań naukowych lub do celów historycznych lub do celów statystycznych, z zastrzeżeniem stosownych warunków i zabezpieczeń lub o ile obowiązek informacyjnym, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania,

   b) prawo UE lub prawo krajowe zezwala na przetwarzanie danych i przewiduje odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,

   c) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie UE lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy dopuszczony odrębnymi przepisami prawa.

V. Powierzenie danych osobowych do przetwarzania innemu podmiotowi

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.

2. Podmiot, o którym mowa w ust. 1 powyżej, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie powierzenia.

3. Podmiot, o którym mowa w ust. 1 powyżej, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające powierzony mu zbiór danych osobowych oraz spełnić wymagania określone w przepisach RODO.

4. W przypadkach, o których mowa w ust. 1 - 3 powyżej, odpowiedzialność za przestrzeganie bezpieczeństwa powierzonych danych spoczywa na Administratorze Danych oraz podmiocie przetwarzającym.

5. W umowie, o której mowa w ust. 1 powyżej, wyraźnie określa się przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, jak również co najmniej:

   a) wskazuje się konieczność posiadania przez podmiot współpracujący wdrożonych rozwiązań zapewniających bezpieczeństwo danym osobowym (systemu bezpieczeństwa danych osobowych),

   b) zastrzega się prawo dokonania przeglądu ww. systemu przez przedstawiciela Spółki lub podmiot wskazany przez Administratora Danych,

   c) wprowadza zapisy zobowiązujące stronę do zachowania w tajemnicy powierzonych informacji,

   d) zobowiązuje się podmiot przetwarzający do usunięcie powierzonych danych z wszelkich nośników, jeżeli jest to konieczne z punktu wiedzenia Administratora Danych oraz możliwe z punktu widzenia regulacji prawnych, po zakończeniu świadczenia usług związanych z przetwarzaniem,

   e) wskazuje na sankcje prawno - finansowe związane z niedotrzymaniem warunków umowy.

VI. <u>Bezpieczeństwo przetwarzania danych osobowych. Postępowanie z dokumentację zawierającą dane o charakterze osobowym. Warunki techniczne i organizacyjne urządzeń i systemu informatycznego.</u>

1. Wprowadza się zabezpieczenia organizacyjne chroniące przed nieautoryzowanym dostępem do danych osobowych obejmujące wskazane poniżej zasady:

   a) dostęp do danych mają wyłącznie upoważnieni pracownicy Spółki, którzy mogą je przetwarzać wyłącznie na polecenie Administratora lub podmiotu przetwarzającego,

   b) dostęp do pomieszczeń, w których przetwarzane są dane osobowe, posiadają pracownicy Spółki oraz osoby trzecie na podstawie właściwie określonych uprawnień (wynikających np. z zakresów obowiązków, udzielonych delegacji w sprawach merytorycznych itp.) oraz/lub stosownych upoważnień (np. wykaz osób upoważnionych do pobierania kluczy do pomieszczeń, przydzielone kody i/lub karty dostępu itp.),

   c) w pomieszczeniach, o których mowa w lit. b), mogą przebywać osoby postronne (klienci) wyłącznie w obecności i pod nadzorem osób uprawnionych do przebywania w tych pomieszczeniach,

   d) pracownicy przetwarzający dane osobowe są zobowiązani do stosowania tzw. „Polityki czystego biurka" tj. dokumenty oraz nośniki informacji należy zabezpieczyć, np. w zamykanych na klucz szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem

osób nieupoważnionych zarówno podczas chwilowej nieobecności w trakcie godzin pracy jak i po godzinach pracy z uwzględnieniem polityki dostępu do pomieszczeń,

e) dokumenty zawierające dane o charakterze osobowym (również w postaci cyfrowej) powinny być przekazywane pomiędzy uprawnionymi osobami z wykorzystaniem bezpiecznych metod przekazu uniemożliwiających zapoznanie się z ich treścią osobom nieupoważnionym,

f) zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych,

g) zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np. na terenach publicznych miejskich, w lesie,

h) prowadzony jest stały monitoring systemu bezpieczeństwa informacji.

2. Zabezpieczenia systemu informatycznego przetwarzającego dane osobowe winny spełniać następujące warunki:

a) użytkownik rozpoczynający pracę zobowiązany jest dokonać sprawdzenia zabezpieczenia pomieszczenia w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego,

b) system powinien być wyposażony w mechanizmy uwierzytelniające użytkownika oraz kontroli dostępu do tych danych,

c) każdy użytkownik systemu informatycznego, w którym przetwarza się dane osobowe posiada odrębny Identyfikator Użytkownika oraz Hasło,

d) Identyfikator Użytkownika wraz z imieniem i nazwiskiem wpisuje się do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych i rejestruje w systemie informatycznym,

e) bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć wyłącznie użytkownik systemu po podaniu Identyfikatora Użytkownika oraz Hasła,

f) z dostępu do danych osobowych może wyłącznie korzystać upoważniony pracownik, a w pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane,

g) nie należy pozostawiać funkcjonującego systemu bez nadzoru,

h) po zakończeniu pracy użytkownik zobowiązany jest: (i) wylogować się z systemu i poczekać na jego wyłączenie; (ii) sprawdzić czy nie zostały pozostawione bez nadzoru

nośniki informacji; (iii) wyłączyć odbiornik energii elektrycznej, zamknąć pomieszczenie i klucze oddać służbie ochrony.

3. System informatyczny przetwarzający dane osobowe dla każdej osoby, której dane osobowe są przetwarzane, powinien zapewnić odnotowanie:

   a) daty pierwszego wprowadzenia danych tej osoby,

   b) źródła pochodzenia danych, jeżeli dane pochodzić mogą z różnych źródeł,

   c) identyfikator użytkownika wprowadzającego dane.

4. System informatyczny służący do przetwarzania danych osobowych powinien umożliwić udostępnianie na piśmie, w powszechnie zrozumiałej formie, treść danych o każdej osobie, której dane są przetwarzane.

VII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe w tym kopii zapasowych

1. Przez nośniki danych osobowych należy rozumieć wszystkie media, niezależnie od postaci w jakiej występują, które służą do przechowywania danych osobowych, w szczególności:

   a) wszelkiego rodzaju dyskietki,

   b) taśmy magnetyczne,

   c) dyski optyczne,

   d) dyski wymienne,

   e) dyski twarde wymontowane z komputerów,

   f) wydruki,

   g) inne media nie wymienione powyżej, które umożliwiają przechowywanie danych osobowych.

2. Wszelkie nośniki, na których znajdują się dane osobowe podlegają ochronie w takim samym stopniu jak dane, które się na nich znajdują.

3. Przechowywanie nośników zawierających dane osobowe powinno odbywać się w warunkach zapewniających zachowanie wymaganego poziomu bezpieczeństwa danych osobowych znajdujących się na tych nośnikach w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.

4. Nośniki elektroniczne przeznaczone do przechowywania danych osobowych powinny się charakteryzować odpowiednią trwałością zapisu, zależną od planowanego okresu przechowywania na nich danych osobowych.

5. Przechowywane nośniki zawierające dane osobowe powinny być wyraźnie oznaczone w sposób umożliwiający ich identyfikację w celu:

   a) zapobiegania przypadkowemu udostępnieniu ich do ponownego użycia,

   b) zapobiegania nieumyślnemu ujawnieniu danych osobowych,

   c) powiadomienia potencjalnych użytkowników o konieczności szczególnej ochrony tych nośników.

6. Dane osobowe przechowywane na nośnikach powinny być z nich usuwane w momencie ustania przyczyn, dla których miały być one przechowywane na nośnikach lub też po upływie czasu przez jaki miały się one znajdować na nośnikach.

7. Przez zniszczenie nośników informacji rozumie się takie działania, które prowadzą do pozbawienia ich cech pozwalających na identyfikację (odczytanie) danych osobowych znajdujących się na tych nośnikach.

8. Osoba upoważniona przez Administratora Danych Osobowych jest odpowiedzialna za niszczenie nośników magnetycznych zawierających dane osobowe oraz za dokumentowanie tych procesów.

9. Nośniki magnetyczne zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych.

10. Nośniki papierowe (wydruki) nie przeznaczone do ponownego użytku oraz nie archiwizowane powinny być natychmiast niszczone. Sposób zniszczenia powinien zapewniać niemożliwość odtworzenia znajdujących się na nośnikach papierowych danych osobowych.

VIII. Procedury nadawania, zmiany oraz odbierania upoważnienia do przetwarzania danych osobowych

1. Upoważnienie do przetwarzania danych osobowych nadawane jest przez Zarząd spółki.

2. Warunkiem wydania pracownikowi upoważnienia do przetwarzania danych osobowych jest podpisanie przez użytkownika oświadczenia o zapoznaniu się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych oraz o zachowaniu uzyskanych danych w tajemnicy, który stanowi Załącznik Nr 2 do niniejszej Polityki bezpieczeństwa.

3. W szczególnie uzasadnionych przypadkach upoważnienie do przetwarzania danych osobowych może zostać nadane innej osobie niż pracownik spółki, w tym przypadku postanowienie ust. 2 powyżej stosuje się również wobec takiej osoby.

4. Jeżeli zmianie ulegają warunki zatrudnienia osoby upoważnionej do przetwarzania danych osobowych, mające bezpośredni związek z przypisanymi tej osobie czynnościami przetwarzania danych osobowych (np. rozwiązanie umowy o pracę, wygaśnięcie umowy o świadczenie usług,

umowy zlecenia, innej umowy cywilno-prawnej), aktualizuję się upoważnienie pracownika do przetwarzania danych osobowych, o ile zmiana taka wywiera wpływ na zakres upoważnienia danej osoby do przetwarzania danych osobowych.

IX. Naruszenie zasad ochrony danych osobowych

1. W przypadku stwierdzenia/uzyskania informacji wskazującej na naruszenie zasad ochrony danych należy niezwłocznie:

   a) zapisać informacje o okolicznościach związanych ze zdarzeniem,

   b) jeżeli zasoby systemu informatycznego na to pozwalają, wygenerować i wydrukować dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,

   c) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,

   d) podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym między innymi:

      – fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej,

      – wylogowania użytkownika podejrzanego o naruszenie zasad ochrony danych,

      – zmianę hasła użytkownika, poprzez którego uzyskano nielegalny dostęp, w celu uniknięcia ponownej próby uzyskania takiego dostępu,

      – dokonać szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia zasad ochrony danych osobowych,

      – przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

2. Po przywróceniu normalnego stanu systemu informatycznego należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

3. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw i wolności osób fizycznych.

4. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw i wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki - jeżeli to wykonalne, nie później niż w terminie siedemdziesięciu dwóch (72) godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik Nr 3 do niniejszej Polityki.

5. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

X. Postanowienia końcowe

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

2. Jeżeli skutkiem działania uczestnika procesu przetwarzania danych osobowych jest ujawnienie informacji osobie nieupoważnionej, sprawca może być pociągnięty do odpowiedzialności karnej określonej przepisami karnymi zawartymi w przepisach krajowych regulujących ochronę danych osobowych.

3. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.

4. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:

Załącznik Nr 1

Wzór upoważnienia do przetwarzania danych osobowych

Załącznik Nr 2

Wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe

Załącznik Nr 3

Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzoru

Załącznik Nr 1 - Wzór upoważnienia do przetwarzania danych osobowych

Warszawa, dnia ..... r.

UPOWAŻNIENIE DO PRZETWRAZANIA
DANYCH OSOBOWYCH

Działając w imieniu spółki 4 Results Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie niniejszym upoważniam:

Panią/Pana .....

Stanowisko .....

do przetwarzania danych osobowych w 4 Results Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie w następującym zakresie:

* bez ograniczeń, podgląd danych, wprowadzania danych, opracowywanie danych, zmienianie danych, usuwanie danych, na komputerach przenośnych, na komputerach stacjonarnych.

A. Okres upoważnienia:

- na okres zatrudnienia/współpracy z ..... do dnia ..... włącznie/ bezterminowo *

B. Zakres upoważnienia:

- dane przetwarzane na nośnikach papierowych *,
- dane przetwarzane elektronicznie *,
- dane osobowe obejmujące:

a) .....

b) .....

c) .....

d) .....

_____

(podpis Administratora Danych)

* niepotrzebne skreślić

Załącznik Nr 2 - Wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe

....., dnia ..... r.

.....

imię i nazwisko osoby upoważnionej

.....

stanowisko

.....

miejsce pracy

O Ś W I A D C Z N I E

Oświadczam, że - w związku z wykonywaniem przeze mnie prac na rzecz 4 Results Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie i upoważnieniem mnie do Przetwarzania danych osobowych - zostałem/łam zapoznany/a ze stosowanymi przepisami i standardami ochrony danych osobowych, zobowiązuję się do przestrzegania:

- Przepisów o ochronie danych osobowych, w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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,
- Polityki Bezpieczeństwa informacji w 4 Results Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie.

W związku z powyższym zobowiązuję się do:

a) zapewnienia ochrony danych osobowych przetwarzanych u administratora, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnieniem osobom trzecim i nieuprawnionym, zabieraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,

b) zachowania w tajemnicy, także po zaprzestaniu wykonywania prac, wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych,

c) natychmiastowego zgłaszania do Administratora Danych zaobserwowania próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa Danych osobowych gromadzonych w zbiorach papierowych, a także w formie elektronicznej.

_____

podpis pracownika/współpracownika

Załącznik Nr 3 - Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzoru

……, dnia …… r.

ZGŁOSZENIE INCYDENTU NARUSZENIA
OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydenty naruszenia ochrony danych osobowych:

Dane Administratora Danych Osobowych	
Miejsce i dzień naruszenia	
Kategoria i przybliżona liczba osób, których dane dotyczą	
Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie	
Opis charakteru naruszenia ochrony danych	
Możliwe konsekwencje naruszenia ochrony danych	
Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

_____

podpis osoby uprawnionej do reprezentowania Administratora Danych