INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH
BEST LINGUA Monika Mazur

	Data	Podpis
Opracowanie:	Maj 2018	
Zatwierdzenie:	01.06.2018	
Aktualizacja:	01.03.2026	
Aktualizacja:	16.03.2026	
Aktualizacja		

§1

Ilekroć w niniejszym dokumencie jest mowa o:

a) Przedsiębiorstwo – należy przez to rozumieć BEST LINGUA Monika Mazur; Nazwa skrócona BEST LINGUA;
b) Administrator Danych Osobowych – należy przez to rozumieć przedsiębiorstwo BEST LINGUA Monika Mazur, ul. Reformacka 6, 35-026 Rzeszów, NIP: 8161405781.
c) Osoby przetwarzające dane – należy przez to rozumieć wszystkie osoby upoważnione do przetwarzania danych osobowych, czyli pracownika przedsiębiorstwa, osobę wykonującą pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osobę odbywającą staż, praktykę w przedsiębiorstwie lub wolontariusza.
d) Użytkownik systemu – należy przez to rozumieć osoby upoważnione przez Administratora Danych Osobowych do przetwarzania danych osobowych w systemie informatycznym przedsiębiorstwa. Użytkownikiem może być pracownik przedsiębiorstwa, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż, praktykę w przedsiębiorstwie lub wolontariusz, o ile zostali upoważnieni do dostępu do danych osobowych osób fizycznych.
e) Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
f) Incydent ochrony danych osobowych – sytuacja która może przyczynić się do wystąpienia naruszenia ochrony danych osobowych.

§2

Celem niniejszego dokumentu jest określenie na podstawie art. 33 oraz 34 Rozporządzenia 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 (dalej RODO), jednolitych zasad postępowania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych przetwarzanych w przedsiębiorstwie BEST LINGUA Monika Mazur zarówno w systemach informatycznych, innych elektronicznych nośnikach informacji, jak również w dokumentach mających postać papierową. Zasady postępowania mają umożliwić szybkie podjęcie działań korygujących oraz określenia zasad zgłaszania naruszeń ochrony danych osobowych i zawiadamiania organu nadzorczego oraz osoby, której dane dotyczą.

§3

1. Przez naruszenie bezpieczeństwa danych osobowych rozumie się wszelkie zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę:

a) utraty danych osobowych;
b) naruszenia poufności, integralności lub dostępności danych osobowych;
c) naruszenia niezawodności systemów służących do przetwarzania danych osobowych.

2. Przez naruszenie bezpieczeństwa danych osobowych rozumie się także odstępstwo od obowiązujących w przedsiębiorstwie procedur mających znaczenie dla bezpieczeństwa danych osobowych, choćby nie prowadziły do skutków wymienionych w ust. 1.
3. Naruszenie bezpieczeństwa danych osobowych może być skutkiem szkodliwego wpływu niewłaściwego oddziaływania czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.; niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu, umyślnym lub nieumyślnym działaniem, a nawet zaniechaniem działania

użytkowników przetwarzających dane osobowe.

4. Przykłady zdarzeń lub działań naruszających bezpieczeństwo danych osobowych (incydenty naruszenia bezpieczeństwa danych osobowych) określa załącznik nr 1 do niniejszej instrukcji.

§ 4

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
2. Każda osoba (tj. użytkownik systemu oraz inny pracownik BEST LINGUA), która stwierdza naruszenie lub zaistnienie okoliczności wskazujących na naruszenie systemu ochrony danych osobowych, określonych w załączniku nr 1 do niniejszej Instrukcji, zobowiązana jest do niezwłocznego zgłoszenia tego faktu Administratorowi Danych Osobowych.
3. W zgłoszeniu, o którym mowa w ust. 2, należy podać:
    a) opis naruszenia bezpieczeństwa danych osobowych;
    b) opis sytuacji i oznaczenie czasu w jakim stwierdzono naruszenie bezpieczeństwa danych osobowych;
    c) informacje niezbędne do ustalenia przyczyny naruszenia bezpieczeństwa danych osobowych;
    d) opis działań podjętych po ujawnieniu zdarzenia.

§ 5

1. W razie stwierdzenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych, Administrator Danych Osobowych ma obowiązek niezwłocznie:
    a) przystąpić do zidentyfikowania i oceny zaistniałej sytuacji, biorąc pod uwagę w szczególności stan pomieszczeń oraz wielkość negatywnych następstw zdarzenia, w celu potwierdzenia lub wykluczenia faktu naruszenia bezpieczeństwa danych osobowych;
    b) zabezpieczyć elementy systemu informatycznego, w szczególności przed dostępem osób trzecich;
    c) podjąć stosowne do zaistniałej sytuacji działania mające na celu zminimalizowanie lub całkowite wyeliminowanie niepożądanych skutków zdarzenia oraz zapobieżenie dalszym zagrożeniom bezpieczeństwa danych osobowych;
    d) wstrzymać bieżące czynności w celu zabezpieczenia dowodów umożliwiających ustalenie przyczyn i skutków naruszenia ochrony danych;
    e) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia;
    f) w miarę możliwości podjąć działania mające na celu ustanie przyczyn lub osób odpowiedzialnych za zaistnienie zdarzenia;
    g) wstępnie udokumentować zdarzenie.
2. W przypadku, gdy zdarzenie dotyczyło danych osobowych przetwarzanych w systemie informatycznym, Administrator Danych Osobowych zobowiązany jest podjąć działania we własnym zakresie, w celu przywrócenia normalnego działania systemu sprzed czasu zdarzenia. Jeżeli zdarzenie doprowadziło do uszkodzenia bazy danych, odtwarza się ją z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego naruszenia bezpieczeństwa danych osobowych.

§ 6

1. W przypadku potwierdzenia wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych, Administrator Danych Osobowych sporządza raport naruszenia bezpieczeństwa danych osobowych.

2. Raport powinien zawierać co najmniej:
    a) określenie daty i godziny wystąpienia zdarzenia lub działania (jeżeli możliwe jest jego ustalenie);
    b) wskazanie osoby powiadamiającej o zaistniałym zdarzeniu (imię, nazwisko, stanowisko służbowe);
    c) opis lokalizacji zdarzenia;
    d) opis naruszenia bezpieczeństwa;
    e) wskazanie przyczyn wystąpienia zdarzenia (jeżeli możliwe jest ich ustalenie);
    f) opis skutków zdarzenia;
    g) opis działań podjętych po stwierdzeniu naruszenia bezpieczeństwa;
    h) propozycje rozwiązań ograniczających lub eliminujących możliwość wystąpienia zdarzenia w przyszłości;
    i) datę i podpis osoby sporządzającej raport.
3. Wzór raportu stanowi załącznik nr 3 do niniejszej Instrukcji.
4. Informację o stwierdzonym incydencie naruszenia bezpieczeństwa danych osobowych należy odnotować w dokumentacji zbioru danych osobowych.

§ 7

1. Po przeprowadzeniu analizy zaistniałego zdarzenia i rozważeniu propozycji rozwiązań zawartych w raporcie, należy przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
2. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie osób biorących udział w przetwarzaniu danych.
3. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innego złośliwego oprogramowania, należy potwierdzić funkcjonowanie ochrony antywirusowej.
4. Jeżeli przyczyną zdarzenia było zaniedbanie pracownika, który dopuścił się zaniedbania może zostać pociągnięty do odpowiedzialności określonej w przepisach Kodeksu pracy.

§ 8

1. W przypadku zaginięcia komputera przenośnego, elektronicznych lub magnetycznych nośników informacji, na których zgromadzone były dane klientów i kontrahentów BEST LINGUA, użytkownik posługujący się wymienionym sprzętem niezwłocznie powiadamia Administratora Danych Osobowych, a ponadto w przypadku kradzieży, najbliższą jednostkę Policji.
2. W sytuacji, o której mowa w ust. 1 Administrator Danych Osobowych lub upoważniona przez niego osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajścia, który powinna podpisać także osoba, której skradziono lub której zaginął sprzęt.
3. W przypadku kradzieży nośnika magnetycznego Administrator Danych Osobowych lub upoważniona przez niego osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

§ 9

1. W celu realizacji zadań wynikających z niniejszej instrukcji Administrator Danych Osobowych ma prawo podejmować wszelkie działania prawnie dopuszczalne, a w szczególności ma prawo:
    a) żądać wyjaśnień od wszystkich pracowników lub innych osób przetwarzających dane osobowe w przedsiębiorstwie;
    b) podejmować czynności sprawdzające lub kontrolne;
    c) nakazać przerwanie przetwarzania danych osobowych.
2. Odmowa udzielenia wyjaśnień lub współpracy z Administratorem Danych Osobowych stanowi naruszenie obowiązków pracowniczych.

§ 10

1. W przypadku naruszenia ochrony danych osobowych Administrator Danych Osobowych ma obowiązek w ciągu 72 godzin po stwierdzeniu naruszenia zgłosić ten fakt organowi nadzorczemu (PUODO), chyba że jest mało prawdopodobne by naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych.
2. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
3. Zgłoszenie, o którym mowa w ust. 1 musi:

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 oznaczenie osoby kontaktowej, od której można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez Administratora Danych Osobowych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

4. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych Administrator Danych Osobowych ma obowiązek poinformowania tych osób w ciągu 72 godzin po stwierdzeniu naruszenia.
5. Zawiadomienie, o którym mowa w ust. 4 powinno być sporządzone, jasnym i prostym językiem opisujące charakter naruszenia ochrony danych osobowych oraz zawierające co najmniej:

a) imię i nazwisko oraz dane kontaktowe Administratora;
b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
c) opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

6. Administrator Danych Osobowych jest zobligowany do prowadzenia rejestru incydentów naruszeń danych BEST LINGUA, jeżeli takie wystąpią, stanowiącym załącznik nr 2 do niniejszej Instrukcji.

§ 11

1. Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są:
    a) osoby przetwarzające dane osobowe;
    b) Administrator Danych Osobowych.
2. Nadzór nad prawidłowym wykonywaniem obowiązków określonych w ust. 1 sprawuje Administrator Danych Osobowych.
3. Nieprzestrzeganie zasad postępowania określonych w niniejszej Instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną pociągnięcia pracownika do odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.
4. Jeżeli skutkiem działania określonego w ust. 3 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów ustawy o ochronie danych osobowych i Kodeksu karnego.

Zatwierdzam
Monika Mazur
Administrator Danych Osobowych

Załączniki:

Załącznik nr 1 – Przykłady zdarzeń lub działań naruszających bezpieczeństwo danych osobowych w BEST LINGUA Monika Mazur

Załącznik nr 2 – Rejestr naruszeń ochrony danych osobowych w przedsiębiorstwie BEST LINGUA Monika Mazur

Załącznik nr 3 – Wzór raportu z naruszenia ochrony danych

Załącznik nr 1. *Przykłady zdarzeń lub działań naruszających bezpieczeństwo danych osobowych w BEST LINGUA Monika Mazur*

KOD NARUSZENIA	FORMY	NARUSZENIE / INCYDENT	SPOSÓB POSTĘPOWANIA
A	**FORMA NARUSZENIA BEZPIEECZEŃSTWA DANYCH OSOBOWYCH PRZEZ PRACOWNIKA ZATRUDNIONEGO PRZY PRZETWARZANIU DANYCH**		
A.1	**W ZAKRESIE WIEDZY:**		
A.1.1	Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym	INCYDENT	• Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji • Sporządzić raport z opisem, jaka informacja została ujawniona • Powiadomić Administratora Danych Osobowych
A.2	**W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA**		
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych	INCYDENT	• Niezwłocznie zakończyć działanie aplikacji • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez nieuprawnione osoby	NARUSZENIE	• Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze • Pouczyć osobę, która dopuściła do takiej sytuacji • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci	INCYDENT	• Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie • Natychmiast zmienić hasła • Powiadomić Administratora Danych Osobowych • Sporządzić raport

A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym, nie będących pracownikami	NARUSZENIE	• Wezwać osobę nieuprawnioną do opuszczenia stanowiska • Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane • Przerwać działające programy • Niezwłocznie powiadomić Administratora • Sporządzić raport
A.2.5	Samodzielne instalowanie jakiegokolwiek oprogramowania	INCYDENT	• Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała • Odinstalować programów • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.2.6	Modyfikowanie parametrów systemu i aplikacji	INCYDENT	• Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.2.7	Odczytywanie zewnętrznych nośników informacji przed sprawdzeniem ich programem antywirusowym	INCYDENT	• Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania • Wykonanie kontroli antywirusowej • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.3	**W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE**		
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	INCYDENT	• Zabezpieczyć dokumenty • Sporządzić raport • Powiadomić Administratora Danych Osobowych
A.3.2	Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych	INCYDENT	• Powiadomić Administratora Danych Osobowych • Zabezpieczyć dokumenty • Sporządzić raport

A.3.3	Niszczenie dokumentów zawierających dane osobowe w sposób umożliwiający ich odczytanie	NARUSZENIE	• Zabezpieczyć niewłaściwie zniszczone dokumenty • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.3.4	Dopuszczanie do kopiowania dokumentów przez osoby do tego nieuprawnione i utraty kontroli nad kopią	NARUSZENIE	• Zaprzestać kopiowania • Odzyskać i zabezpieczyć wykonaną kopię • Powiadomić Administratora Danych Osobowych • W zależności od kopiowanych dokumentów podjęcie kolejnych kroków w tym prawnych • Sporządzić raport
A.3.5	Dopuszczanie, aby inne osoby nieuprawnione odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe	NARUSZENIE	• Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności • Wyłączyć monitor • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.3.6	Sporządzanie kopii danych przez osoby do tego nieuprawnione na nośnikach danych	NARUSZENIE	• Spowodować zaprzestanie kopiowania • Odzyskać i zabezpieczyć wykonaną kopi • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.3.7	Utrata kontroli nad kopią danych osobowych	NARUSZENIE	• Podjąć próbę odzyskania kopii • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.4	**W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH**		
A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych	INCYDENT	• Zabezpieczyć (zamknąć) pomieszczenie • Powiadomić Administratora Danych Osobowych

A.4.2	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie ich do kontaktu ze sprzętem komputerowym	INCYDENT	• Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia • Należy spróbować ustalić ich tożsamość • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.4.3	Umożliwienie osobom nieupoważnionym aby podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji	Decyzja po ustaleniu zakresu ingerencji	• Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania • Postarać się ustalić ich tożsamość • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.5	**W ZAKRESIE POMIESZCZEŃ, W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI**		
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby nieupoważnione dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.)	Decyzja po ustaleniu zakresu ingerencji	• Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ewentualnego opuszczenia pomieszczeń • Postarać się ustalić ich tożsamość • Powiadomić Administratora Danych Osobowych • Sporządzić raport
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowanie takiego faktu	Decyzja po ustaleniu zakresu ingerencji	• Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń • Postarać się ustalić ich tożsamość • Powiadomić Administratora Danych Osobowych • Sporządzić raport
B	**ZJAWISKA ŚWIADCZĄCE O MOŻLIWOŚCI NARUSZENIA OCHRONY DANYCH OSOBOWYCH**		
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach	Decyzja po ustaleniu zakresu ingerencji	• Powiadomić Administratora Danych Osobowych • Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji • Sporządzić raport

B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu	Decyzja po ustaleniu zakresu ingerencji	• Powiadomić Administratora Danych Osobowych • Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji • Sporządzić raport
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych		
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych		
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania		
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Decyzja po ustaleniu zakresu ingerencji	• Postępować zgodnie z właściwymi przepisami • Powiadomić niezwłocznie Administratora Danych Osobowych • Sporządzić raport
C	**FORMY NARUSZENIA OCHRONY DANYCH OSOBOWYCH PRZEZ OBSŁUGĘ INFORMATYCZNĄ W KONTAKTACH Z UŻYTKOWNIKIEM**		
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej. Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika	INCYDENT	• Powiadomić niezwłocznie Administratora Danych Osobowych • Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji • Sporządzić raport
C.2	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika	INCYDENT	

Załącznik nr 2. *Rejestr naruszeń ochrony danych osobowych w przedsiębiorstwie BEST LINGUA Monika Mazur*

Rejestr naruszeń ochrony danych osobowych przetwarzanych w przedsiębiorstwie BEST LINGUA Monika Mazur

Data naruszenia	Osoba zgłaszająca naruszenie	Krótki opis naruszenia, okoliczności naruszenia i skutki	Miejsce wystąpienia naruszenia	Zbiór danych, którego dotyczy naruszenie	Obowiązek zgłoszenia organowi nadzorczemu (TAK/NIE)	Obowiązek zawiadomienia osoby, której dane dotyczą (TAK/NIE)	Podjęte działania zaradcze	Podpis Administratora

Załącznik nr 3 – Wzór raportu z naruszenia ochrony danych

RAPORT O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Sporządzający raport:

1. Imię i nazwisko ……..

2. Stanowisko (funkcja) .....

3. Kod formy naruszenia danych (wg tabeli – jeżeli jest) ……
4. Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (kondygnacja, godzina, numer i nazwa pomieszczenia, osoba powiadamiająca o naruszeniu)

.....

……

……

5. Osoba powodująca naruszenie (która swoim działaniem lub zaniechaniem przyczyniła się do naruszenia ochrony danych osobowych)

.....

(Imię i nazwisko, jeżeli zostało ustalone)

6. Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych

……

(Imiona i nazwiska, jeżeli zostały ustalone)

7. Informacja o danych, które zostały lub mogły zostać ujawnione

.....

8. Zabezpieczone materiały lub inne dowody związane z wydarzeniem

.....

9. Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania)

……

……

……

……