POLITYKA
BEZPIECZEŃSTWA INFORMACJI

C4 Bydgoszcz sp. z o.o.
ul. Dąbrowa 62, 85-147 Bydgoszcz

S P I S T R E Ś C I

Załącznik nr 1 Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych
Załącznik nr 2 Instrukcja postępowania na wypadek sytuacji nadzwyczajnej związanej z zagrożeniem terrorystycznym

Rozdział II
Wstęp
Zasady ogólne dotyczące Polityki ochrony danych osobowych

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz. U. 2014r., poz. 1182 z późn. zm.),
   2. Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),
3. Ustawą z dnia 7 listopada 2014r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014r., poz. 1662),
4. Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014r. w sprawie wzorów zgłoszenia i odwołania administratorów bezpieczeństwa informacji (Dz. U z 2014r., poz. 1934),
5. Ustawą z dnia 7 września 1991r. o systemie oświaty (Dz. U. z 2004r., Nr 256, poz. 2572 z późn. zm.),
6. Ustawa z dnia 26 stycznia 1982r. Karta Nauczyciela (Dz. U. z 2014r., poz. 191 z późn. zm.),
7. Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2015r., poz. 45 z późn. zm.),
8. Rozporządzeniem Ministra Edukacji Narodowej i Sportu z dnia z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (D. U z dnia 2 września 2014r., poz. 1170 z późn. zm.),
9. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. 2015r., poz. 745),
10. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015 poz. 719).

W celu zabezpieczenia danych gromadzonych i przetwarzanych w **C4 Bydgoszcz sp. z o.o.** oraz w celu podniesienia bezpieczeństwa w przetwarzających je systemach informatycznych, a w szczególności w celu ochrony danych osobowych, wprowadza się określone w niniejszym dokumencie zasady postępowania. Prezes Firmy, realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych, dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane

dalszemu przetwarzaniu niezgodnemu z tymi celami,
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Polityka bezpieczeństwa odnosi się do danych osobowych przetwarzanych w zbiorach:

1) tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.

Dane osobowe przetwarzane są w celu:

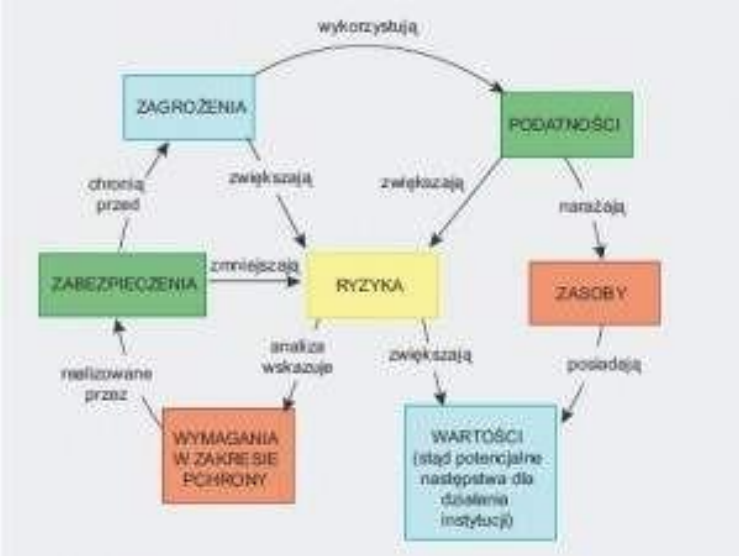
1) realizacji statutowych zadań i obowiązków,
2) zapewnienia prawidłowej, zgodnej z prawem polityki personalnej i bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia nawiązywanych przez Firmę działający jako pracodawca w rozumieniu art. 3 kodeksu pracy,
3) dla realizacji innych usprawiedliwionych celów i zadań Firmy z poszanowaniem praw i wolności osób powierzających Firmie swoje dane.

Celem wprowadzenia niniejszej Polityki Bezpieczeństwa jest:

1) ochrona danych osobowych przetwarzanych i gromadzonych w Firmie i dotyczy:
   a) zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,
   b) metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,
   c) procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,
   d) ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,
   e) określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny,
2) zmniejszenie ryzyka utraty informacji,
3) określenia zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych,

4) podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych danych,

Polityka została opracowana zgodnie z wymogami określonymi w § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
Przy opracowaniu dokumentacji wzięto pod uwagę poniższe aspekty



Integralną częścią Polityki Bezpieczeństwa Informacji jest opracowana i wdrożona Instrukcja Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją Zarządzania systemem informatycznym ODO". Określa ona sposób Zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. **poufność danych** - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. **integralność danych** - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. **integralność systemu** rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Zasady określone przez niniejszy dokument mają zastosowanie do całego systemu

przetwarzania danych w tym do systemu informatycznego Firmy, a w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których są przetwarzane lub będą informacje podlegające ochronie,
2) informacji będących własnością Firmy, o ile zostały przekazane Firmie na podstawie umów lub porozumień ,
3) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,
4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie.

Sposób i zakres udostępniania dokumentu.

1. Z niniejszym dokumentem powinni zapoznać się wszyscy pracownicy, a w szczególności:
   1) osoby upoważnione do przetwarzania danych osobowych w zbiorach i bazach danych,
   2) obsługa informatyczna Firmy,

2. Za rozpowszechnienie dokumentu i umożliwienie zapoznania się z nim przez wszystkich pracowników odpowiedzialny jest ABI.
3. Dokument powinien zostać umieszczony w formie elektronicznej, na wewnętrznych zasobach sieciowych, do których dostęp posiadają wszyscy pracownicy lub w uzasadnionych przypadkach powinien zostać im przedłożony w formie papierowej.

Rozdział III
Definicje

Przez użyte w Polityce określenia należy rozumieć:

1) **ADO -** Administratora Danych Osobowych – Firma (Prezes Firmy)**,** organ, jednostka organizacyjna decydująca (samodzielnie) o celach i środkach przetwarzania danych osobowych (art. 7 pkt 4). Jest to podmiot praw i obowiązków, który sprawuje władztwo nad przetwarzaniem danych osobowych przez zaciąganie zobowiązań i rozporządzanie prawami. Nie ma przy tym znaczenia fakt, czy podmiot ten jest w posiadaniu przetwarzanych danych lub sam je przetwarza. Zadania w zakresie ochrony danych osobowych AD realizuje za pośrednictwem bezpośrednio mu podległego Administratora bezpieczeństwa Informacji **(Załącznik** – Schemat organizacji bezpieczeństwa informacji).

2) **ABI -** osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Bezpieczeństwa Informacji zgodnie z art.36a ustawy, zgłoszony na podstawie art. 46b ust. 1 do rejestru Generalnemu Inspektorowi Ochrony Danych Osobowych;
3) **ASI -** osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji Administratora Systemu Informatycznego Firmy;
4) **Dane osobowe (dane)** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) **Zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;
6) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
7) **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
8) **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
9) **Przetwarzanie danych** - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
10) **Użytkownik danych** – każdy pracownik, który wykonując czynności służbowe, przetwarza dane osobowe, tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie;
11) **Osoba upoważniona** – osoba posiadająca upoważnienie wydane przez ABI lub osobę uprawnioną przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu;
12) **Osoba uprawniona** – osoba posiadająca upoważnienie wydane przez ABI do wykonywania w jego imieniu określonych czynności;
13) **Sieć telekomunikacyjna** – sieć o definicji zawartej w Ustawie z dnia 16 lipca 2004r. – Prawo telekomunikacyjne (Dz. U. z 2014r., poz. 243, z późn. zm).
14) **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom dostęp do danych osobowych znajdujących się w tym systemie;

15) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, połączeń sieciowych i narzędzi programowych zastosowanych w celu przetwarzania danych;
16) **Bezpieczeństwo systemu informatycznego** – wdrożone przez Firmę lub ABI, środki organizacyjne i techniczne w celu zabezpieczenia oraz ochrony danych przed nieautoryzowanym dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem;

Rozdział IV
Administrator Bezpieczeństwa Informacji Administratora Systemu Informatycznego

Zadania i obowiązki

Administratora Bezpieczeństwa Informacji powołuje na podstawie art. 36 a ustawy Administrator Danych. Podlega on bezpośrednio Kierownikowi Jednostki Organizacyjnej/ AD – Prezesowi Firmy.

Administratorem bezpieczeństwa informacji może być osoba, która:

1. ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
2. posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
3. nie była karana za umyślne przestępstwo.

Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.

Administrator danych jest ponadto obowiązany zgłosić Generalnemu Inspektorowi

Ochrony Danych Osobowych zmianę informacji objętych zgłoszeniem w terminie 14 dni od dnia zmiany.

Do zadań administratora bezpieczeństwa informacji należy:

1. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   b. nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
   c. zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
2. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt. 2–4a i 7.

W przypadku stwierdzenia nieprawidłowości w zakresie zabezpieczenia danych osobowych Administrator Bezpieczeństwa Informacji ma obowiązek:

1. pouczać i instruować osoby, które dopuściły się uchybień, a także raportować o błędach Prezesowi mając na celu przywrócenie stanu prawidłowego,
2. zwracać się do Firmy o dokonanie zmian w zakresie stosowanych zabezpieczeń organizacyjnych i technicznych,
3. przedstawiać Prezesowi Sprawozdania/ raporty dotyczące stanu zabezpieczenia danych osobowych, w tym propozycję poprawiające bezpieczeństwo danych oraz wnioski dotyczące odpowiedzialności osób winnych uchybień,

Administrator Bezpieczeństwa Informacji nadzoruje pracę **Administratora Systemu Informatycznego.**

Do zadań Administratora Systemu Informatycznego należy:

1. Zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3. na wniosek AD/ABI przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

4. nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5. podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
6. wyrejestrowuje użytkowników na polecenie AD/ABI
7. zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych,
8. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
9. prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
10. sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
11. podejmuje działania służące zapewnieniu niezawodności zasilania komputerów (w tym zapewnienie awaryjnych źródeł zasilania – UPS), innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

ABI i ASI zostają powołani Zarządzeniem Prezesa Firmy.

Rozdział V
Przetwarzanie danych osobowych

Administrator danych **(Prezes Firmy),** aby przetwarzać dane osobowe zgodnie z przepisami ustawy o ochronie danych osobowych, musi spełnić jeden z warunków decydujący o tym, że takie działanie jest legalne, a ponadto we właściwy sposób zabezpieczać zgromadzone dane, dbać o interesy osób, których dane dotyczą i respektować ich prawa gwarantowane ustawą o ochronie danych osobowych.

Z punktu widzenia przepisów o ochronie danych osobowych istotne jest przede wszystkim to, aby administrator danych osobowych, przetwarzając dane:
spełniał przynajmniej jeden warunek uprawniający go do wykonywania operacji na danych osobowych - w odniesieniu do danych zwykłych, jak np. imię, nazwisko czy adres zamieszkania określono je w art. 23 ust 1 pkt. 1-5 ustawy o ochronie danych osobowych. Spełnienie jednego z poniższych warunków stanowi o zgodnym z prawem przetwarzaniu danych osobowych, gdyż przesłanki te są równoprawne, a jednocześnie autonomiczne.

Ponadto Administrator danych jest zobowiązany do:

1. Rejestracji zbiorów danych o ile przepis ma zastosowanie.
   Zgodnie z art. 40. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 i 1a.";
   Obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane, o których mowa w art. 27 ust. 1 (tzw. dane wrażliwe) , nie podlega administrator danych, który powołał Administratora Bezpieczeństwa Informacji i zgłosił go Generalnemu Inspektorowi Ochrony Danych Osobowych do rejestracji, z zastrzeżeniem art. 46e ust. 2 ustawy.

Powyższy przepis dot. zwolnienia z obowiązku rejestracji ma zastosowanie w stosunku do C4 Bydgoszcz sp. z o.o. w Bydgoszczy.
Firma dokonała powołania ABI i zgłosiła go do rejestru Generalnego Inspektora Ochrony Danych Osobowych.

2. **Stosowania odpowiednie zabezpieczenia**, o których stanowią przepisy rozdziału 5 ustawy o ochronie danych osobowych oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – administrator jest bowiem zobowiązany zastosować środki techniczne i organizacyjne zapewniające przetwarzanym danym odpowiednią ochronę, a przede wszystkim zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zebraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1 ustawy o ochronie danych osobowych),

3. **Dopełnienia obowiązku informacyjnego** ustanowionego w art. 24 ust. 1 oraz art. 25 ust. 1 ustawy o ochronie danych osobowych, chyba że administrator danych jest z niego zwolniony – w przypadku zbierania danych bezpośrednio od osoby, której dotyczą (art. 24) administrator musi poinformować ją o swojej nazwie i adresie, celu zbierania, odbiorcach danych (także tych przewidywanych), prawie dostępu do danych i prawie ich poprawiania, a także o dobrowolności albo obowiązku ich podania (a gdy obowiązek ten istnieje – o jego podstawie prawnej). W przypadku zbierania danych nie od osoby, której one dotyczą (art. 25), administrator – zaraz po utrwaleniu danych – musi poinformować osobę, której one dotyczą, o swojej nazwie i adresie, celu i zakresie zbierania danych, a zwłaszcza o ich odbiorcach, źródle, z którego dane pozyskał, prawie dostępu do danych i prawie ich poprawiania, a także o prawie żądania zaprzestania przetwarzania danych lub wniesienia sprzeciwu wobec przetwarzania danych,

4. **Dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą**, poprzez zapewnienie, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane, przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (o czym stanowi art. 26 ust. 1 pkt. 1 – 4 ustawy o ochronie danych osobowych),

5. **Respektowania prawa osób, których dane dotyczą** – prawa te wymienione są w rozdziale 4 ustawy o ochronie danych osobowych i dotyczą kontroli procesu przetwarzania danych.

Naruszenie przepisów o ochronie danych osobowych może narazić administratora danych na odpowiedzialność administracyjną przez GIODO, jak i karną, stosownie do przepisów karnych ustawy o ochronie danych osobowych (art. 49 – art. 54a).

Warunki przetwarzania danych osobowych

1. Przetwarzanie danych osobowych dotyczy wszelkich danych osobowych zgromadzonych w **zbiorach tradycyjnych** a w szczególności: skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych oraz **w systemach informatycznych** w tym bazach danych oraz plikach zawierających dane osobowe.
2. Przetwarzanie danych osobowych jest dopuszczalne jedynie przy spełnieniu co najmniej jednej z poniższych przesłanek (Art. 23 ustawy):
   a) osoba, której dane osobowe dotyczą wyrazi na to zgodę,
   b) przetwarzanie danych jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
   c) przetwarzanie danych osobowych jest konieczne do realizacji umowy, gdy osoba której dane dotyczą jest stroną tej umowy lub gdy jest to niezbędne do podjęcia działań poprzedzających zawarcie umowy – na żądanie osoby, której dane osobowe dotyczą,
   d) przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
   e) przetwarzanie danych jest niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez Administratora danych osobowych albo odbiorców danych, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.
3. Zgoda, o której mowa w **pkt. a** może dotyczyć także przetwarzania danych osobowych w przyszłości pod warunkiem, że cel ich przetwarzania nie zmieni się
4. W przypadku, gdy przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dotyczą, a uzyskanie jej zgody nie jest możliwe,

Administrator Danych może przetwarzać jej dane osobowe do czasu, gdy uzyskanie tej zgody będzie możliwe.

5. **Administrator Danych Osobowych** w procesie przetwarzania danych osobowych zobowiązany jest do:
   a) adekwatnego przetwarzania danych zgodnie z potrzebami i zgodnie z prawem,
   b) zbierania danych dla określonych, zgodnych z prawem celów,
   c) dbałości o poprawność merytoryczną danych osobowych,
   d) przechowywania danych umożliwiających identyfikację osób, których dotyczą, przez czas nie dłuższy niż jest to niezbędne dla realizacji celu dla którego dane zebrano,
6. W przypadku zbierania danych osobowych, Administrator obowiązany jest poinformować osobę, której dane dotyczą o:
   a) adresie swojej siedziby i pełnej nazwie,
   b) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
   c) prawie dostępu do treści swoich danych,
   d) prawie do ich poprawienia.
7. W przypadku gdy Administrator Danych zbiera dane osobowe nie od osoby, której dane dotyczą, Administrator Danych oprócz obowiązków określonych powyżej winien poinformować osobę, której dane osobowe zbiera o:
   a) źródle pozyskania danych,
   b) prawie wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na szczególną sytuację – w wypadkach wskazanych w ustawie,
   c) prawie wniesienia sprzeciwu, gdy Administrator Danych zamierza wykorzystać te dane dla celów marketingowych lub w przypadku przekazania tych danych innemu Administratorowi Danych – w wypadkach wskazanych w ustawie.

Rozdział VI
Udostępnianie danych osobowych

1. Administrator Danych Osobowych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Udostępnienie danych osobowych następuje na pisemny, umotywowany wniosek, chyba że przepis szczególny stanowi inaczej.
3. Wniosek o udostępnienie danych osobowych powinien zawierać:
   a. informacje umożliwiające wyszukanie żądanych danych w zbiorze danych,
   b. wskazywać zakres żądanych danych,
   c. wskazywać ich przeznaczenie.
4. W przypadku, gdy o udostępnienie danych osobowych występują inne niż określone w pkt. 1 osoby i podmioty, wniosek powinien dodatkowo w sposób

wiarygodny uzasadniać potrzebę ich posiadania oraz wykazywać, że udostępnienie danych nie naruszy praw i wolności osoby, której dane dotyczą.

5. Dane osobowe udostępniane przez Administratora Danych mogą być wykorzystane przez odbiorców danych oraz organy państwowe i samorządu terytorialnego wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Podmiotami uprawnionymi do żądania udostępnienia danych osobowych są:

a) podmioty upoważnione z mocy prawa, na podstawie przepisów szczególnych - np. Policja, Sądy, Prokuratura, itp.), którym inne jednostki organizacyjne zobowiązane są udostępniać dane osobowe na podstawie obowiązujących przepisów prawa,
b) podmioty nieupoważnione z mocy prawa, tj. inne niż wymienione w pkt. 1, które muszą złożyć wniosek o udostępnienie danych osobowych w formie pisemnej.

Podmiotom, o których mowa wyżej - pkt. a Administrator Danych Osobowych udostępnia posiadane w zbiorze dane osobowe także w celach innych niż włączenie do zbioru danych , np. w celach informacyjnych.
Podmiotom określonym w pkt. b Administrator Danych Osobowych udostępnia posiadane w zbiorze dane osobowe w celach innych niż włączenie do zbioru danych, wyłącznie wówczas gdy w sposób wiarygodny uzasadnią potrzebę posiadania tych danych a udostępnienie danych nie naruszy praw i wolności osób, których dane dotyczą.
Administrator Danych Osobowych odmawia udostępnienia danych osobowych ze zbioru danych jeżeli udostępnienie tych danych spowodowałoby:

1. ujawnienie wiadomości stanowiących tajemnicę w rozumieniu ustawy o ochronie informacji niejawnych,
2. zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
3. zagrożenie podstawowego interesu gospodarczego lub finansowego państwa,
4. istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

Odmowa udostępnienia danych osobowych winna nastąpić na piśmie z jednoczesnym wskazaniem przyczyn odmowy.
W przypadku stwierdzenia, że osoba wnosząca o udzielenie informacji nie jest osobą uprawnioną do ich otrzymania, Administrator Danych Osobowych powinien odmówić udzielenia informacji, powołując się na przepisy ustawy o ochronie danych osobowych oraz wyjaśnić jakie dokumenty lub informacje są niezbędne do ich udostępnienia.

Rozdział VII
Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. System bezpieczeństwa fizycznego

Obszarem przetwarzania danych są budynki, w których zlokalizowane jest **C4 Bydgoszcz sp. z o.o.** (pomieszczenia lub ich części) w którym przetwarzane są dane osobowe, znajdujące się w Bydgoszczy przy ul. Dąbrowej 62, szczegóły zostały opisane w **Wykazie zbiorów** (elementem są obszary przetwarzania oraz zabezpieczenie techniczne).

Przetwarzanie danych osobowych z użyciem stacjonarnego/ przenośnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych.

Przetwarzanie danych osobowych przy pomocy sprzętu przenośnego poza obszarem przetwarzania danych osobowych jest możliwe wyłącznie po:

1. uzyskaniu zgody Administratora Danych (w szczególnych przypadkach ABI)
2. Zapoznaniu się i podpisaniu Regulaminu użytkowania komputerów przenośnych

Przetwarzanie danych jest zabronione, jeśli nie są zapewnione warunki ochrony danych osobowych określone w niniejszej Polityce.

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze stosowanymi środkami ochrony fizycznej oraz wskazaniem programów zastosowanych do przetwarzania tych danych, opisany jest w **Załączniku - Wykaz zbiorów danych osobowych.**

Rozdział VIII
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Opis struktury zbiorów danych osobowych przedstawiono w Załączniku do Instrukcji zarządzania systemu przetwarzającego dane osobowe. Wymagane jest wskazanie wszystkich tych danych, występujących w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą.

Potwierdzeniem realizacji powyższych zapisów rozdziału są:

1. Wydruk ze struktury relacyjnej bazy danych (identyfikatory pól w bazie należy opisać w sposób zrozumiały dla kontrolera;
2. Dokumentacja techniczna oprogramowania lub instrukcja obsługi programu w zakresie przetwarzania danych osobowych;
3. Zrzuty ekranowe z opisem danych osobowych, które są na nich widoczne wraz w powiązaniami z polami na innych zrzutach ekranowych;

4. Opisu tekstowego pól informacyjnych z danymi osobowymi i ich powiązań z innymi danymi w programie.

Sposób przepływu danych pomiędzy poszczególnymi systemami

Sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe przedstawiono w **Załączniku - Sposób przepływu danych**

Rozdział IX
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

A. Zabezpieczenia fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej

Zabezpieczenia fizyczne opisane są w **Załączniku - Wykaz zbiorów danych osobowych"**

1. Budynki, w których zlokalizowany jest obszar przetwarzania danych osobowych są chronione przez system alarmowy posiadający połączenie z agencją ochrony pełniącą nadzór techniczny.
2. Stosuje się monitoring wizyjny, obejmujący swym zasięgiem pomieszczenia (korytarze) ogólnodostępne, którego celem jest podniesienie bezpieczeństwa uczniów i nauczycieli..
3. Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zamykanych na klucz.
4. Kartoteki i dokumenty przechowuje się w szafach metalowych i niemetalowych, zamykanych na klucz.
5. W pomieszczeniach Firmy znajdują się gaśnice przeciw pożarowe.
6. Stosuje się politykę kluczy:
   a) Dostęp do budynków i pomieszczeń biurowych możliwy jest wyłącznie przez osoby upoważnione, które posiadają do nich klucze (kartę identyfikacyjną);
   b) W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie,
   c) Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu,
   d) Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu;
   e) Naruszenie zasad polityki kluczy może spowodować wyciągnięciem następujących konsekwencji: Poniesienie odpowiedzialności wynikających z Kodeksu pracy lub z art. 363 § 1. kodeksu cywilnego.

B. Środki organizacyjne

1. Wyznaczono Administratora Bezpieczeństwa Informacji (ABI) stosownie do art. 36a i został on zgłoszony na podstawie art. 46b do rejestru Generalnego

Inspektora oraz Administrator Systemu Informatycznego (ASI) nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych w tym w systemach informatycznych

1. Została opracowana i wdrożona „Polityka Bezpieczeństwa i Ochrony Danych Osobowych" oraz „Instrukcja Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
2. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych.
3. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
4. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do tych danych zaznajamiane z obwiązującymi przepisami o ochronie danych osobowych, procedurami przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym. Zaznajomienie się z przepisami potwierdzają na piśmie.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy.
6. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego.
7. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
8. Stosuje się zgodnie z art. 31 ustawy **pisemne umowy powierzenia przetwarzania danych** dla współpracy z podwykonawcami/ użytkownikami zewnętrznymi przetwarzającymi dane osobowe, których administratorem danych jest Gimnazjum nr 20.
9. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
10. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
11. Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarkach lub w sposób uniemożliwiający odczytanie zawartych w nich danych.
12. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

C. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. Zastosowano UPS do serwera lub kluczowych komputerów, na których są przetwarzane dane osobowe,
2. Dostęp do komputera/laptopa z danymi osobowymi odbywa się poprzez podanie loginu i hasła,

3. W przypadku dostępu do danych osobowych przez Internet, stosuje się szyfrowanie tego połączenia (SSL lub VPN),
4. W przypadku dostępu do danych osobowych przez Internet, należy uprzednio podać login i hasło,
5. Zastosowano system antywirusowy,
6. Użyto system UTM do ochrony sieci komputerowej,
7. Zastosowano macierze dyskowe w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej,
8. Wdrożono system do monitorowania pracy urządzeń, pracowników oraz do zabezpieczania przed wyciekiem danych.

D. Zabezpieczenia programów przetwarzających dane osobowe

1. Dla osób upoważnionych określono zakres obowiązków i prawa dostępu do danych osobowych.
2. Dostęp do danych osobowych w systemach/programach informatycznych wymaga podania nazwy użytkownika oraz hasła.
3. Użytkownicy systemów/programów informatycznych posiadają w nich konta z określonymi prawami dostępu.
4. Zastosowano wygaszacze ekranu chronione hasłem, uruchamiane po 10 minutach nieaktywności użytkownika.
5. Zmianę haseł wymusza system.
6. Systemy/programy informatyczne pozwalają na rejestrację czynności użytkowników wykonywanych na danych osobowych.

Rozdział X
Instrukcja alarmowa

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie.

Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik C4 Bydgoszcz sp. z o.o. w Bydgoszczy w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub Administratora Bezpieczeństwa Informacji.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu,

ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości
    d. dokumentuje prowadzone postępowania
5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały
    b. zabezpiecza ewentualne dowody
    c. ustala osoby odpowiedzialne za naruszenie
    d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody)
    e. inicjuje działania dyscyplinarne
    f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości
    g. dokumentuje prowadzone postępowania

Szczegółowy sposób postępowania w przypadku wystąpienia incydentu opisuje **Załącznik nr 1** - Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

Rozdział XI
Procedura działań korygujących i zapobiegawczych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych.

2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami stawy o Ochronie Danych Osobowych, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji.

Definicje

1. **Incydent** - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
2. **Zagrożenie** – potencjalna możliwość wystąpienia incydentu
3. **Korekcja** – działanie w celu wyeliminowania skutków incydentu.
4. **Działanie korygujące** – jest to działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji.
5. **Działanie zapobiegawcze** – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.
6. **Kontrola** – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki i instrukcji.

Opis czynności

1. ABI jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
    a. zgłoszenia od pracowników
    b. wiedza ABI
    c. wyniki kontroli
2. W przypadku, gdy ABI stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną
3. ABI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, ABI jest zobowiązany do oceny efektywności ich zastosowania.

Rozdział XII
Kontrola systemu ochrony danych osobowych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z kontrolą stanu bezpieczeństwa danych osobowych
2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.

3. Do kontroli stanu ochrony danych osobowych upoważniony jest Administrator Bezpieczeństwa Informacji.
4. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami U.O.D.O.
5. Administrator Bezpieczeństwa Informacji przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.
6. Po dokonanej kontroli ABI przygotowuje i przekazuje sprawozdanie roczne Administratorowi Danych Osobowych. Na jego podstawie inicjowane są działania korygujące lub zapobiegawcze.

Rozdział XIII
Sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych

1. Raz w roku Administrator Bezpieczeństwa Informacji przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych i przekazuje Administratorowi danych
2. Sprawozdanie zgodnie art. 36a ust. 2 pkt. 1 lit. a zawiera:

a. oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania;
b. imię i nazwisko administratora bezpieczeństwa informacji;
c. wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
d. datę rozpoczęcia i zakończenia sprawdzenia;
e. określenie przedmiotu i zakresu sprawdzenia;
f. opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
g. stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
h. wyszczególnienie załączników stanowiących składową część sprawozdania;
i. podpis administratora bezpieczeństwa informacji, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania;
j. datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.";

Rozdział XIV
Firmienia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe winien być poddany przefirmieniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie firmienia odpowiada ABI a za jego zorganizowanie odpowiada Kierownictwo Firmy i przełożony użytkowników.
3. Zakres firmienia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
4. Firmienie zostaje zakończone wydaniem Zaświadczenia o wzięciu udziału w firmieniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie firmienia zasad ochrony danych osobowych **Załącznik - Zaświadczenie o firmieniu ODO**
5. Zaświadczenie przechowywane jest w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do przetwarzania danych osobowych.
6. Po przefirmieniu pracownika Prezes lub upoważniony przez niego ABI wystawia pisemne upoważnienie do przetwarzania danych osobowych **Załącznik - Upoważnienie do przetwarzania danych osobowych**

Rozdział XV
Postanowienia końcowe

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i **nie może być udostępniana** osobom postronnym w żadnej formie bez zgody Prezesa.
2. Z treścią „Polityki bezpieczeństwa" oraz „Instrukcji Zarządzania systemem informatycznym" ma obowiązek zapoznania się każdy użytkownik (osoba przetwarzająca dane osobowe).
3. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa/ Instrukcji przetwarzania danych w systemach informatycznych dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce".
5. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
6. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
7. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2014r., poz. 1182 ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
8. W sprawach nieuregulowanych w niniejszej „Polityce bezpieczeństwa" mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (Dz. U. 2014r. poz. 1182 teks jednolity) oraz wydanych na jej podstawie aktów wykonawczych.

Integralna częścią Polityki Bezpieczeństwa Informacji jest Instrukcja Zarządzania systemem przetwarzającym dane osobowe

Załącznik nr 1

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

1. stwierdzono naruszenie zabezpieczenia systemu informatycznego, lub
2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Każdy pracownik Firmy, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym zobowiązany jest do niezwłocznego poinformowania o tym Administratora Bezpieczeństwa Informacji lub w przypadku jego nieobecności bezpośredniego przełożonego.

Osoba zarządzająca (sprawująca nadzorująca) zbiorem/ bazą danych osobowych lub ASI/ ABI, która stwierdziła lub uzyskał informację wskazującą na naruszenie ochrony tego zbioru/ bazy danych zobowiązana jest do niezwłocznego:

1. **zapisania wszelkich informacji i okoliczności** związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
2. jeżeli zasoby systemu na to pozwalają, **wygenerowania i wydrukowania wszystkich dokumentów i raportów**, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
3. **przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia**, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.
4. **podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu** osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.
    a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
    b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,
    c) zmianę hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu
5. **szczegółowej analizy stanu systemu informatycznego** w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

6. **przywrócenia normalnego działania systemu**, przy czym, jeżeli nastąpiło uszkodzenie bazy/ zbioru 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.

Po przywróceniu normalnego stanu bazy danych osobowych 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.

1. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie
2. wszystkich osób biorących udział w przetwarzaniu danych.
3. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
4. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

Administrator Systemu Informatycznego przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia przekazuje Administratorowi Bezpieczeństwa Informacji. Administrator bezpieczeństwa informacji przeprowadza analizę raportu i uwzględnia go w opracowywaniu corocznego sprawozdania dla Administratora Danych.

W przypadku szczególnego zagrożenia dla bezpieczeństwa danych osobowych informacje o naruszeniu ustawy lub zaistniałym incydencie niezwłocznie przekazuje Administratorowi Danych.

Załącznik nr 2

Instrukcja postępowania na wypadek sytuacji nadzwyczajnej związanej z zagrożeniem terrorystycznym

Do sytuacji nadzwyczajnej związanej z działaniami terrorystycznymi zaliczamy:

- Zagrożenie bombowe,
- Fałszywe alarmy.

Zagrożenie bombowe (jeśli otrzymano groźby)

- Przez telefon: zapamiętać rozmowę w szczegółach (w razie możliwości zapisywać), zwrócić uwagę na wszelkie odgłosy i dźwięki w tle, na szczegóły głosu mówiącego. Jeśli ktoś inny odebrał telefon należy go szczegółowo przepytać.

- Przesyłka pocztowa: zabezpieczyć przesyłkę w celu zachowania śladów (danych) do późniejszej analizy specjalistycznej prowadzonej przez odpowiednie służby.

- Tok postępowania:
  - poinformować natychmiast Zarząd firmy,
  - po konsultacji z przełożonym powiadomić policję, straż pożarną, służby medyczne lub w razie potrzeby inne służby ratownicze /np. patrol saperski/
  - zaalarmować w godzinach pracy Zarząd Firmy,
  - po konsultacji z przełożonymi przeprowadzić ewakuację uczniów (nauczycieli) w sposób nie wywołujący paniki,
  - przeprowadzić planowo i metodycznie przeszukanie pomieszczeń/ obszaru Firmy w obecności osób znających teren, w razie obecności wykonując ich polecenia,
  - w miarę możliwości odciąć dopływ energii elektrycznej.

- Wykrycie bomby (jeśli znaleziono bombę lub istnieje podejrzenie podłożenia bomby) należy:
  - nie dotykać !,
  - otoczyć i zabezpieczyć miejsce ochroną, powiadomić osoby odpowiedzialne za przebieg akcji nadzwyczajnej,
  - nakazać ewakuację terenu,
  - przed ewakuacją zabezpieczyć materiały stanowiące własność Firmy i inna dokumentację,
  - wyłączyć zasilanie elektryczne,
  - usunąć z otoczenia materiały palne,

Ponieważ bomby i inne materiały wybuchowe mogą być eksplodowane drogą radiową, wszystkie nadajniki w tym również aparaty radiowo- telewizyjne i telefony komórkowe w promieniu 250 m należy w miarę możliwości wyłączyć.

- Wybuch bomby:
  - powiadomić Prezesa,
  - wezwać policję, straż pożarną i pogotowie ratunkowe,
  - ewakuować przebywających pracowników (uczniów) po uprzednim sprawdzeniu czy drogi ewakuacji i punkty zborne są wolne od podejrzanych urządzeń lub ładunków wybuchowych,
  - zabezpieczyć materiały niejawne i inną dokumentację,
  - zabezpieczyć dowody rzeczowe, ślady i miejsca eksplozji do chwili przybycia osób funkcyjnych i policji.

Fałszywe alarmy (jeśli otrzymano groźby)

Fałszywe alarmy należy traktować jako rzeczywiste zagrożenie bombowe i postępować analogicznie jak w pkt. w/w.

OŚWIADCZENIE

***dot*.:** zapoznania się z Polityką Bezpieczeństwa Informacji

Oświadczam, że zostałem przeszkolony z treścią **Polityki bezpieczeństwa** Niezastosowanie się do postanowień niniejszej Polityki stanowi ciężkie naruszenie obowiązków pracowniczych określonych w art. 100 § 2 ustawy z dnia 26 czerwca 1974r. Kodeks pracy (t.j. Dz. U. z 2014r., Nr 1502 z późn. zm.). Ponadto zarówno w odniesieniu do pracowników C4 Bydgoszcz sp. z o.o. w Bydgoszczy jak i osób współpracujących powoduje odpowiedzialność cywilno-prawną i karną określoną w odpowiednich przepisach prawa.

L.p.	Imię i nazwisko	Data zapoznania	Podpis