Ochrona danych osobowych oraz bezpieczeństwo informacji w call / contact center

DANE OSOBOWE	
ZWYKŁE	**SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH (DANE WRAŻLIWE / SENSYTYWNE)**
Wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, które nie należą do szczególnych kategorii danych osobowych	**Wymagają szczególnej ochrony**, ponieważ ich przetwarzanie niesie za sobą wysokie ryzyko dla podstawowych praw i wolności osób, których dotyczą te dane

DANE OSOBOWE ZWYKŁE	
▪ IMIĘ	▪ NUMER DOWODU OSOBISTEGO
▪ NAZWISKO	▪ NUMER TELEFONU
▪ ADRES E-MAIL	▪ IMIONA RODZICÓW
▪ ADRES ZAMIESZKANIA	▪ KOLOR OCZU
▪ PESEL	▪ DANE O LOKALIZACJI
▪ NIP	▪ DATA URODZENIA
▪ STANOWISKO	▪ WIEK
▪ NUMER RACHUNKU BANKOWEGO	▪ ADRES ZAMELDOWANIA

SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH

Dane ujawniające pochodzenie rasowe lub etniczne

- Informacja o przynależności do grupy etnicznej.
- Informacja o przynależności rasowej.

Dane ujawniające poglądy polityczne

- Informacja o deklarowaniu poparcia lub braku poparcia dla danej partii politycznej
- Informacja o deklarowaniu poparcia dla działań osób sprawujących władzę polityczną

Dane ujawniające przekonania religijne lub światopoglądowe

- Informacja o przynależności wyznaniowej
- Informacja o tym, że ktoś deklaruje się jako ateista, agnostyk

Dane ujawniające przynależność do związków zawodowych

- Informacja o przynależności do związku zawodowego

SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH

Dane genetyczne

- Informacje o odziedziczonych lub nabytych cechach genetycznych (np. analiza próbki biologicznej)
- Wyniki badań genetycznych

Dane biometryczne

- Wizerunek twarzy (skan rysów twarzy lub fotografia, o ile jest przetwarzana specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości)
- Dane daktyloskopijne (np. odcisk palca)
- Skan siatkówki oka

Dane dotyczące zdrowia

- Informacje o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej
- Informacje zbierane podczas rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej
- Informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych
- Wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym

Dane dotyczące seksualności lub orientacji seksualnej

- Informacja o orientacji seksualnej dane osoby (deklarowanie się jako np. hetero-, homo- lub biseksualista)
- Informacja dotycząca życia seksualnego

PRZETWARZANIE

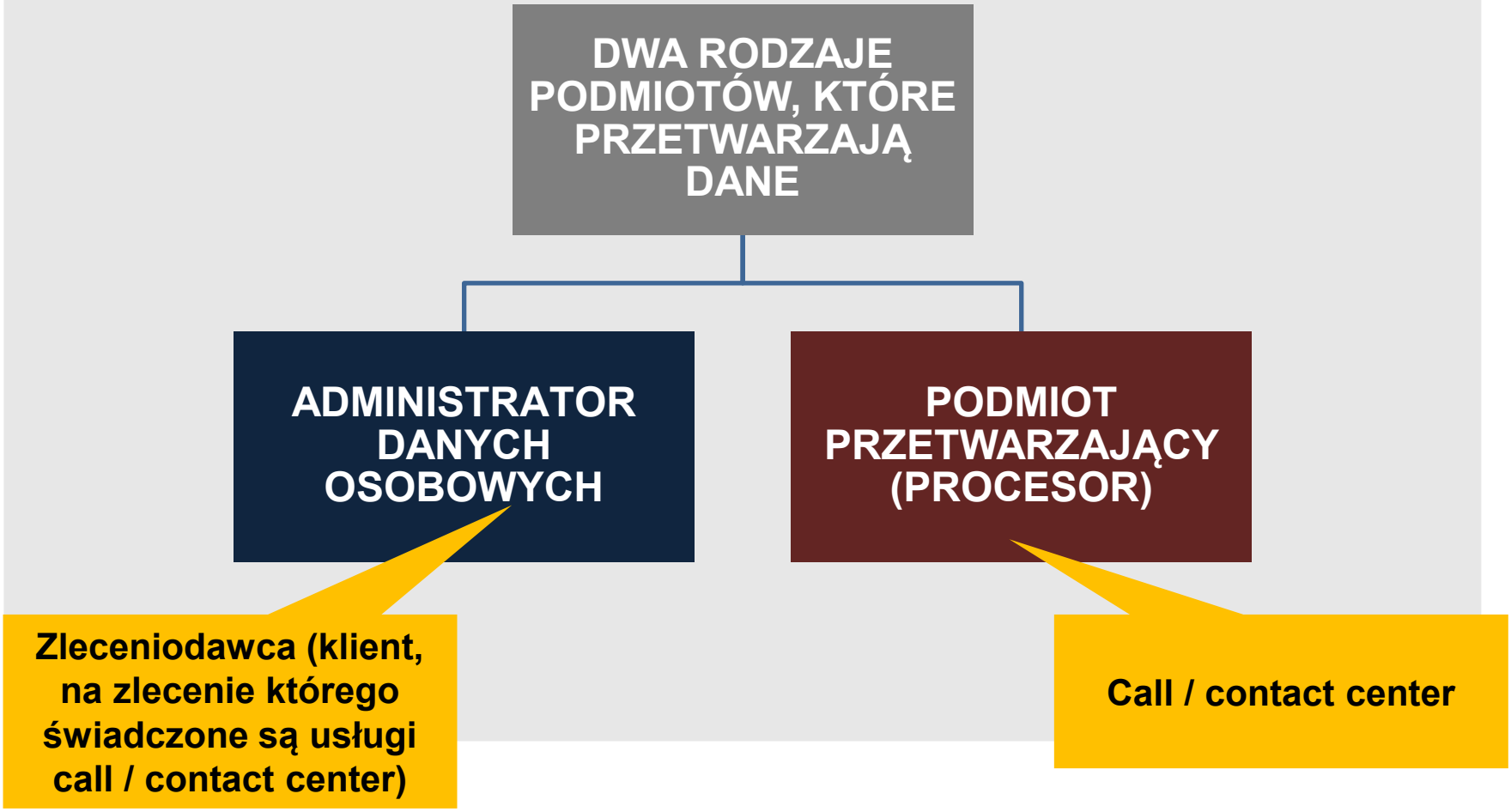
WSZELKIE OPERACJE WYKONYWANE NA DANYCH OSOBOWYCH, W SZCZEGÓLNOŚCI:

▪ MODYFIKOWANIE	▪ PRZEGLĄDANIE
▪ UTRWALANIE	▪ **USUWANIE**
▪ ORGANIZOWANIE	▪ UJAWNIANIE
▪ PORZĄDKOWANIE	▪ DOPASOWYWANIE
▪ PRZECHOWYWANIE	▪ ŁĄCZENIE
▪ ADAPTOWANIE	▪ OGRANICZANIE
▪ **ZBIERANIE**	▪ **WYKORZYSTYWANIE**
▪ POBIERANIE	▪ NISZCZENIE

Zbieranie danych osobowych podczas kontaktu telefonicznego stanowi przetwarzanie danych

Wykorzystywanie danych w celu nawiązania kontaktu telefonicznego stanowi przetwarzanie danych

ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY



ADMINISTRATOR	PODMIOT PRZETWARZAJĄCY (PROCESOR)
Decyduje o celach i sposobach przetwarzania danych osobowych (w jakim celu dane osobowe zostaną wykorzystane, jak długo będą przechowywane, w jaki sposób będą przechowywane).	Przetwarza dane osobowe **w imieniu Administratora oraz na jego zlecenie**. **Nie decyduje** o celach ani sposobach przetwarzania danych.
Wydaje polecenia Podmiotowi przetwarzającemu.	Przetwarza dane **wyłącznie na udokumentowane polecenie** Administratora.
Podejmuje decyzję o realizacji praw osób, których dotyczą dane osobowe (w przypadku zgłoszenia żądania wycofania zgody / sprzeciwu wobec przetwarzania / usunięcia danych, decyduje o tym, czy przetwarzanie zostanie zaprzestane / dane zostaną usunięte).	**Pomaga administratorowi w realizacji praw osób, ale nie jest uprawniony do samodzielnego decydowania** o zaprzestaniu przetwarzania / usuwaniu danych. W przypadku zgłoszenia takiego żądania jedynie informuje o tym Administratora, a usuwa dane jedynie na wyraźne polecenie administratora.

ADMINISTRATOR	PODMIOT PRZETWARZAJĄCY (PROCESOR)
Klient zleca call / contact center np.: (i) przeprowadzenie akcji marketingowej; (ii) obsługę sprzedaży; (iii) obsługę infolinii, **co wiąże się z przetwarzaniem danych osobowych osób, z którymi kontaktują się konsultanci**	Call / contact center świadczy usługę na zlecenie klienta i **przetwarza dane osobowe w imieniu Klienta**.
Klient jest administratorem danych osobowych osób, z którymi kontaktuje się call / contact center, dlatego w trakcie rozmowy wskazuje się, że administratorem danych osobowych jest klient (np. *Administratorem Pana danych osobowych jest... / Dzwonię **w imieniu** ...).*	Call / contact center jest podmiotem przetwarzającym (procesorem), dlatego podczas rozmowy nie podaje się danych spółki, która świadczy usługi call / contact center.

ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

DANE OSOBOWE MUSZĄ BYĆ:	
Przetwarzane **zgodnie z prawem, rzetelnie i w sposób przejrzysty** dla osoby, której dane dotyczą.	**ZGODNOŚĆ Z PRAWEM, RZETELNOŚĆ, PRZEJRZYSTOŚĆ**
Zbierane w **konkretnych, wyraźnych i prawnie uzasadnionych celach** i nieprzetwarzane dalej w sposób niezgodny z tymi celami.	**OGRANICZENIE CELU**
Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.	**MINIMALIZACJA**
Prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.	**PRAWIDŁOWOŚĆ**
Przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, **przez okres nie dłuższy, niż jest to niezbędne do celów**, w których dane te są przetwarzane.	**OGRANICZENIE PRZECHOWYWANIA**
Przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.	**INTEGRALNOŚĆ I POUFNOŚĆ**
Administrator jest odpowiedzialny za przestrzeganie ww. zasad i musi być w stanie wykazać ich przestrzeganie.	**ROZLICZALNOŚĆ**

LP.	PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH ZWYKŁYCH	PODSTAWA PRAWNA
1.	Osoba, której dane dotyczą wyraziła **zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów.	**Art. 6 ust. 1 lit. a) RODO**
2.	Przetwarzanie jest **niezbędne do wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.	**Art. 6 ust. 1 lit. b) RODO**
3.	Przetwarzanie jest niezbędne do wypełnienia **obowiązku prawnego ciążącego na administratorze**.	**Art. 6 ust. 1 lit. c) RODO**
4.	Przetwarzanie jest niezbędne do **ochrony żywotnych interesów osoby**, której dane dotyczą, lub innej osoby fizycznej.	**Art. 6 ust. 1 lit. d) RODO**
5.	Przetwarzanie jest niezbędne do **wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej** powierzonej administratorów.	**Art. 6 ust. 1 lit. e) RODO**
6.	Przetwarzanie jest niezbędne do celów wynikających z **prawnie uzasadnionych interesów** realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.	**Art. 6 ust. 1 lit. f) RODO**

OCHRONA DANYCH OSOBOWYCH W ZWIĄZKU ZE ŚWIADCZENIEM USŁUG CALL / CONTACT CENTER – INSTRUKCJA POSTĘPOWANIA DLA KONSULTANTÓW

ZAŁOŻENIA

Instrukcja określa **zasady i procedury przetwarzania danych osobowych w związku ze świadczeniem usług call / contact center** na rzecz klientów Spółki (dalej jako: „**Zleceniodawcy**").

Celem Instrukcji jest **zapewnienie przetwarzania danych osobowych w związku ze świadczeniem usług call / contact center w sposób zgodny z obowiązującymi przepisami prawa**, w szczególności z przepisami *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, dalej jako: „**RODO**" oraz regulacjami wewnętrznymi obowiązującymi w Grupie Kapitałowej Arteria (dalej jako: „**GK Arteria**").

W razie jakichkolwiek wątpliwości lub problemów związanych z ochroną danych osobowych w związku z prowadzonym projektem, jak i ze stosowaniem Instrukcji, należy niezwłocznie skontaktować się z Kierownikiem Projektu.

REGULACJE WEWNĘTRZNE OBOWIĄZUJĄCE W GK ARTERIA – (I) DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH	
Polityka bezpieczeństwa – zasady ochrony danych osobowych (dokument główny)	
1.	Załącznik numer 1 – Procedura przetwarzania danych osobowych w rekrutacji i zatrudnieniu
2.	Załącznik numer 2 – Procedura stosowania monitoringu
3.	Załącznik numer 3 – Procedura realizacji praw osób, których dotyczą dane osobowe
4.	Załącznik numer 4 – Polityka przekazywania danych
5.	Załącznik numer 5 – Ocena skutków przetwarzania dla ochrony danych
6.	Załącznik numer 6 – Polityka dotycząca naruszeń ochrony danych
7.	Załącznik numer 7 – Stosowanie zasady prywatności na etapie projektowania
8.	Załącznik numer 8 – Polityka retencji danych osobowych
9.	Załącznik numer 9 – Procedura postępowania w przypadku kontroli przestrzegania przepisów o ochronie danych osobowych
10.	Załącznik numer 10 – Procedura pozyskiwania zgód na przetwarzanie danych osobowych oraz przetwarzania danych w celach marketingowych
11.	Załącznik numer 11 – Właściwe zabezpieczanie danych osobowych i doskonalenie systemów bezpieczeństwa użytkowanych zasobów

KAŻDA OSOBA, KTÓREJ DANE DOTYCZĄ, MA PRAWO DO:

1.	**DOSTĘPU DO DANYCH OSOBOWYCH**
2.	**SPROSTOWANIA DANYCH**
3.	**USUNIĘCIA DANYCH („PRAWO DO BYCIA ZAPOMNIANYM”)**
4.	**OGRANICZENIA PRZETWARZANIA**
5.	**PRZENOSZENIA DANYCH**
6.	**WNIESIENIA SPRZECIWU WOBEC PRZETWARZANIA DANYCH OSOBOWYCH**
7.	**WYCOFANIA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH**

Osoby, z którymi kontaktuje się konsultant, mogą zgłaszać telefonicznie skargi i wnioski związane z realizacją ww. praw.

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH – ROZLICZALNOŚĆ	
1.	Jeżeli podczas rozmowy pobierana jest zgoda na przetwarzanie danych osobowych, to call / contact center musi być w stanie udowodnić Klientowi, że zgoda taka została pobrana.
2.	Administrator (Klient call / contact center) powinien być w stanie **wykazać, że zgoda została udzielona (np. w przypadku kontroli przestrzegania przepisów o ochronie danych).** Jest w stanie to wykazać jedynie, jeżeli otrzyma od call / contact center dowód pobrania zgody.
3.	W sytuacji, gdy zgoda pobierana jest **za pośrednictwem telefonu**, należy odczytać rozmówcy treść zgody oraz poprosić o wypowiedzenie słów: „Wyrażam zgodę”, „Zgadzam się” lub „Tak”. **Przebieg takiej rozmowy powinien zostać utrwalony.**

OBOWIĄZKI KONSULTANTA

KONSULTANT JEST OBOWIĄZANY DO:

- zapoznania się z treścią Instrukcji postępowania z danymi osobowymi przez pracowników call / contact center i przestrzegania zasad w niej zawartych. **Instrukcja dostępna jest na stanowisku pracy każdego konsultanta.**
- **zapoznania się z treścią Polityki bezpieczeństwa i przestrzegania zasad w niej zawartych**. W GK Arteria obowiązuje Polityka bezpieczeństwa określająca zasady przetwarzania danych osobowych w spółkach GK Arteria. Każdy konsultant jest obowiązany do zapoznania się z treścią Polityki bezpieczeństwa i przestrzegania zasad w niej zawartych.
- **przetwarzania danych osobowych zgodnie z przepisami o ochronie danych osobowych, w szczególności przepisami RODO**. Przed rozpoczęciem pracy każdy konsultant jest obowiązany **wziąć udział w szkoleniu z zakresu ochrony danych osobowych oraz regulacji wewnętrznych obowiązujących w GK Arteria**.
- **zachowania w tajemnicy danych osobowych. Każdy konsultant jest obowiązany do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.**

ZASADY ŚWIADCZENIA USŁUG CALL / CONTACT CENTER W SPOSÓB ZGODNY Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

ZARZĄDZANIE DOSTĘPEM DO DANYCH OSOBOWYCH ORAZ ZASADY KORZYSTANIA ZE SPRZĘTU SŁUŻBOWEGO

1.	**Zasada czystego biurka.** Na koniec dnia pracy lub w jego trakcie w przypadku wyjścia na dłuższy okres należy uprzątnąć biurko z dokumentów oraz innych nośników danych, tak aby dostęp do nich innych osób był niemożliwy. Niepotrzebne dokumenty należy po zakończeniu pracy zniszczyć w niszczarce.
2.	**Blokada komputera.** W przypadku oddalenia się od komputera na dłuższy czas należy zablokować komputer poprzez naciśnięcie klawiszy Windows + L.
3.	**Zakaz podłączania jakichkolwiek elektronicznych nośników danych, niepochodzących od GK Arteria, do sprzętu służbowego.** Podłączanie jakichkolwiek elektronicznych nośników danych, niepochodzących od GK Arteria, do sprzętu służbowego, jest zabronione.
4.	**Zachowanie hasła dostępu w tajemnicy.** Zabronione jest udostępnianie hasła dostępu innym osobom.

ZARZĄDZANIE DOSTĘPEM DO DANYCH OSOBOWYCH ORAZ ZASADY KORZYSTANIA ZE SPRZĘTU SŁUŻBOWEGO

5.	**Zgłaszanie incydentów.** Konsultant ma obowiązek zgłosić Kierownikowi Projektu każdy incydent bezpieczeństwa, w szczególności: (i) nieuprawnione zniszczenie, utratę, zmodyfikowanie, ujawnienie lub nieuprawniony dostęp do danych – np. pendrive / dokumentów z danymi osobowymi, przesłanie zestawienia danych osobowych do nieuprawnionego odbiorcy, ujawnienie danych osobowych podczas rozmowy telefonicznej z nieuprawnioną osobą), jak również (ii) każdy przypadek uszkodzenia sprzętu służbowego, jak również jakiejkolwiek ingerencji osób nieuprawnionych w system informatyczny lub sprzęt służbowy.

ZARZĄDZANIE DOSTĘPEM DO DANYCH OSOBOWYCH ORAZ ZASADY KORZYSTANIA ZE SPRZĘTU SŁUŻBOWEGO

6.	**Zgłaszanie skarg i wniosków.** Konsultant ma obowiązek zgłosić Kierownikowi Projektu **każdy przypadek skarg i wniosków** osób kontaktujących się z konsultantem za pośrednictwem infolinii lub osób, z którymi kontaktuje się konsultant w celu świadczenia usług call / contact center, w szczególności: (i) kwestionowania dopuszczalności przetwarzania danych osobowych; (ii) wycofania zgody na przetwarzanie danych osobowych; (iii) zgłoszenia sprzeciwu wobec przetwarzania danych osobowych czy (iv) żądania usunięcia danych osobowych.

UWAGA: W przypadku zgłoszenia żądania usunięcia danych osobowych należy poinformować osobę, że żądanie zostało przyjęte i zostanie rozpatrzone przez administratora oraz odnotować wycofanie zgody lub zgłoszenie sprzeciwu wobec przetwarzanie danych i prośbę o usunięcie danych w systemie, ale nie należy usuwać danych osobowych. Żądanie takie należy także zgłosić Kierownikowi Projektu oraz zaprzestać kontaktowania się z osobą, która wycofała zgodę lub zgłosiła sprzeciw wobec przetwarzania i poprosiła o usunięcie danych osobowych.

PHISHING

Czym jest phishing?

Phishing (czyt. fiszing) to rodzaj oszustwa polegającego na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia informacji, zainfekowania sprzętu złośliwym oprogramowaniem lub nakłonienia ofiary do określonych działań.

Jak rozpoznać phishing?

Otrzymasz komunikaty nakłaniające do:

- ujawnienia informacji osobistych (loginy, hasła, dane kart płatniczych, PESEL, inne)
- pobrania wskazanych plików, zwykle za pośrednictwem poczty elektronicznej, SMSem
- wejście na stronę internetową poprzez kliknięcie w link w wiadomości

PHISHING

Jak się bronić?

- Weryfikuj nadawcę wiadomości, sprawdź dokładnie adres e-mail. Przestępcy używają podobnych adresów do rzeczywistych, które mogą różnić się jednym znakiem
- Ochraniaj swoje hasła i nie ujawniaj ich nikomu
- W wiadomościach od przestępców często zdarzają się literówki, błędy gramatyczne lub brak polskich znaków
- Nie przekazuj nikomu poufnych danych — przez telefon, osobiście lub przez e-mail
- Nie pobieraj i nie otwieraj załączników do wiadomości, których się nie spodziewasz
- **Jeśli otrzymana wiadomość budzi podejrzenie, powiadom przełożonego lub Dział IT**

PHISHING

Jak się bronić?

- Sprawdzaj adresy stron, **nie klikaj,** tylko najedź myszką na link w wiadomości. W wielu przypadkach phishingu adresy strony wyglądają na poprawne i legalne, ale adresy URL mogą być błędnie wpisane lub domena może się różnić (.com zamiast .gov)

Przykłady:
orlen**pl**.com zamiast orlen.pl → dodanie „pl" do adresu
paczka-gls.com zamiast gls-group.com → użycie nazwy znanej firmy w adresie
peka**oo**24.com zamiast pekao24.pl → dodatkowa litera w adresie
e**-tollgov**.pl zamiast etoll.gov.pl → wykorzystanie sekwencji przypominającej rządową domenę

Phishing – przykład wiadomości opublikowany przez Komendę Policji

1 Sprawdź nadawcę wiadomości

Sprawdź dokładnie adres e-mail nadawcy - przestępcy często podszywają się pod adresy **podobne do rzeczywistych**, zmieniając w nich np. pojedyncze znaki.

2 Zwracaj uwagę na błędy językowe

Przestępcy często popełniają błędy w treści wiadomości – wszelkie błędy gramatyczne lub ortograficzne a także brak polskich znaków mogą wskazywać na atak.

Temat Ukrywanie dochodow. Sprawa PL53254812
Od Ministerstwo Finansów (sadca@asdfadscv.com)
Do
Data Śr 10:17
Dzien dobry,

W trakcie naszych kontroli ujawnilismy ukrycie Pana/Pani dochodow, w zwiazku z czym bedzie przeprowadzona kontrola podatkowa.

Dokument wskazujacy na naruszenia o skladaniu falszywego dochodow zalaczony w e-maile.Sankcja na przeprowadzenie sciagania podatkowego rowniez jest zalaczona do dokumentu.

Prosimy o stawiennictwo do nas do biura w dniu 09.11.2016 do 14:00 ze wszystkimi swoimi dochodami za rok 2016, a takze interesuja nas niektore transakcje przeprowadzane w roku biezacym.

W razie jakichkolwiek pytan prosimy o kontakt telefonicznie lub przez e-mail. Dane kontaktowe znajduja sie ponizej, nalezy podac w pismie numer sprawy "PL53254812" i osobisty kod.

Ministerstwo Finansow
ul. Swietokrzyska 12
00-916 Warszawa
NIP: 526-025-02-74
REGON: 000002217

http://www.dsferuerr.co.uk/
Click to follow link
Odwiedź stronę Ministerstwa

3 Nie uruchamiaj nieoczekiwanych załączników

Jeżeli nie oczekiwałeś załącznika to go **nie otwieraj**. Jeżeli znasz nadawcę **potwierdź telefonicznie** czy rzeczywiście przesłał Ci załącznik.

4 Sprawdzaj dokąd prowadzą odnośniki

Zatrzymaj kursor nad odnośnikiem aby sprawdzić dokąd **dokładnie prowadzi link**. Nigdy **nie klikaj linków** do których nie masz pełnego zaufania.

CA-W & DZC

PHISHING – skutki ataku

Jakie mogą być skutki ataku phishingowego?

- Kradzież tożsamości
- Udostępnienie wrażliwych danych
- Konsekwencje finansowe
- Utrata kontroli nad komputerem lub całym systemem informatycznym

ZACHOWAJ BEZPIECZEŃSTWO W SIECI!

Media społecznościowe

Pamiętaj!

- W mediach społecznościowych nie jesteś anonimowy.
- Publikacje powinny być pisane tak, aby w żaden sposób nie można było uznać Twojej prywatnej opinii za oficjalne stanowisko Spółki lub Klientów Spółki.
- Ujawnienie tajemnicy przedsiębiorstwa może spowodować straty wizerunkowe i finansowe.
- Koleżeński stosunek do współpracowników to także jeden z podstawowych obowiązków pracowniczych, udostępnianie postów obraźliwych w ich stosunku może być poczytany za mobbing.

Tworzenie haseł

Wybierając hasło należy unikać:

- powtórzenia loginu,
- słów, które znajdziemy w słowniku, np. football, mojehaslo, bydgoszcz,
- ciągów znaków występujących obok siebie na klawiaturze, np. 123qwerty, zxcvbnm, !@#123,
- własnego imienia i nazwiska, imion bliskich osób, dzieci,
- kombinacji, które można łatwo odgadnąć posiadając podstawową wiedzę o użytkowniku, np. data urodzin, adres zamieszkania, numer telefonu.

ZAPAMIĘTAJ!

- Nikomu nie udostępniaj swoich loginów i haseł do systemów informatycznych oraz kart dostępu.
- Loguj się wyłącznie przy wykorzystaniu własnego identyfikatora oraz hasła.
- Opuszczając stanowisko pracy zabezpiecz komputer (uruchomienie wygaszacza ekranu z aktywnym hasłem).
- Po zakończeniu pracy wyloguj się z systemu informatycznego i nie pozostawiaj na biurku żadnych dokumentów.
- Wchodząc do zabezpieczonych pomieszczeń korzystaj wyłącznie z przydzielonej karty dostępu.
- Nie pozostawiaj bez nadzoru jakichkolwiek dokumentów zawierających dane osobowe lub tajemnicę przedsiębiorstwa.
- W przypadku naruszenia zasad bezpieczeństwa zawsze poinformuj swojego przełożonego oraz postępuj zgodnie z obowiązującymi procedurami.