REGULAMIN OCHRONY DANYCH OSOBOWYCH W INSTYTUCIE SLAWISTYKI POLSKIEJ AKADEMII NAUK

SPIS TREŚCI

Niniejszy regulamin stanowi wyciąg najistotniejszych zasad zawartych w Polityce Ochrony Danych Osobowych wraz z Instrukcją zarządzania systemem informatycznym.
Obowiązuje wszystkich pracowników, mających upoważnienia do przetwarzania danych osobowych.

1. Definicje

1. **Polityka** – rozumie się przez to Politykę Ochrony Danych Osobowych w Instytucie Slawistyki PAN.
2. **Administrator** – Instytut Slawistyki PAN, decydujący o celach i środkach przetwarzania danych osobowych.
3. **Inspektor Ochrony Danych (IOD)** – osoba powołana przez Dyrektora Instytutu Slawistyki PAN, odpowiedzialna za organizację ochrony danych osobowych.
4. **RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).
5. **Ustawa** – ustawa z dnia 10 maja 2018 roku o ochranie danych osobowych (Dz. U. z 2018 poz. 1000).
6. **Dane osobowe (dane)** – to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. Tożsamość tej osoby fizycznej.
7. **Zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów.
8. **Przetwarzanie danych osobowych** – to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych, i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję,

rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

9. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
10. **Ograniczenie przetwarzania** – polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
11. **Anonimizacja** – zmiana danych osobowych, w której wyniku dane te tracą charakter danych osobowych.
12. **Zgoda osoby, której dane dotyczą** – 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.
13. **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.
14. **Ocena skutków w ochronie danych (analiza ryzyka)** – proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo, i jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych, zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.
15. **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
16. **Administrator systemu informatycznego (ASI)** – osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.
17. **Użytkownik** – pracownik Instytut Slawistyki PAN posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych.
18. **Zabezpieczenie systemu informatycznego** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów

technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

19. **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde.
20. **Podmiot przetwarzający (procesor)** – osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora;
21. **Pseudonimizacja** - przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
22. **Szczególne kategorie danych osobowych (dane wrażliwe)** – ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby lub orientacji seksualnej. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.
23. **Profilowanie** – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

2. Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT

1. Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z komputerów stacjonarnych, urządzeń przenośnych, serwera, drukarek.
2. Użytkownik zobowiązany jest korzystać ze Sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
3. Użytkownik zobowiązany jest do zabezpieczenia Sprzętu IT przed dostępem osób nieupoważnionych, w szczególności dotyczy to informacji wyświetlanych na ekranach monitorów.
4. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
5. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

3. Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.
2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę / Zleceniodawcę na swoje własne potrzeby ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę / Zleceniodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD/DVD, dysków i pamięci przenośnych, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.

6. W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca / Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

4. Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące automatycznie system operacyjny komputera).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą „https:”.
7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie dotyczy to żądania podania takich informacji przez rzekomy bank.
8. Użytkownicy mogą korzystać z Internetu dla celów prywatnych wyłącznie okazjonalnie, powinno ono być ograniczone do niezbędnego minimum.
9. Korzystanie z Internetu dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność systemu informatycznego Pracodawcy / Zleceniodawcy.

10. Przy korzystaniu z Internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
11. W zakresie dozwolonym przepisami prawa Pracodawca / Zleceniodawca zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad.
12. Ponadto, w uzasadnionym zakresie, Pracodawca / Zleceniodawca zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie.
13. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

5. Zasady korzystania z poczty elektronicznej

1. Pracownik otrzymuje indywidualny adres mailowy według wzorca: imie.nazwisko@ispan.waw.pl
2. Pracownik jest zobowiązany do zachowania hasła w poufności i nieujawniania go osobo trzecim.
3. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
4. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
5. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne. Hasło należy przesłać odrębną wiadomością elektroniczną (dalej: „mailem") lub inną metodą, np. telefonicznie lub SMS-em.
6. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
7. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
8. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.

9. Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
10. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
11. Użytkownicy nie powinni rozsyłać maili zawierających załączniki o dużym rozmiarze.
12. Użytkownicy powinni systematycznie kasować niepotrzebne maile.
13. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć funkcji „Ukryte do wiadomości – UDW”.
14. Program do obsługi poczty elektronicznej jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
15. Użytkownicy mają prawo korzystać z programu do obsługi poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie. Powinno być ono ograniczone do niezbędnego minimum.
16. Korzystanie z programu do obsługi poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
17. Przy korzystaniu z programu do obsługi poczty elektronicznej Użytkownicy są obowiązanie do przestrzegania prawa własności przemysłowej i prawa autorskiego.
18. Użytkownikom zabrania się korzystać z programu do obsługi poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania i przepisów prawa.
19. Użytkownik bez zgody Pracodawcy / Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

6. Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.

2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

7. Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Za nadawanie upoważnień odpowiada Administrator.
2. Każdy użytkownik systemu przed nadaniem upoważnienia musi:
    a. zapoznać się z niniejszym Regulaminem;
    b. odbyć szkolenie z zasad ochrony danych osobowych;
    c. podpisać Oświadczenie o poufności.
3. IOD bądź Administrator nadaje pisemne upoważnienia Pracownikom i Zleceniobiorcom.
4. Upoważnienie nadawane jest do zbiorów w wersji papierowej i elektronicznej.
5. W przypadku, gdy upoważnienie udzielane jest do zbioru w wersji elektronicznej, nadawany jest użytkownikowi identyfikator w systemie.
6. W przypadku anulowania upoważnienia identyfikator użytkownika jest blokowany w systemie.

8. Polityka haseł

1. Hasło dostępu do zbioru danych składa się co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).
2. Zmiana hasła do systemu następuje nie rzadziej niż co 90 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3. Jeżeli zmiany hasła nie wymusza system, wówczas do zmiany hasła zobowiązany jest użytkownik.
4. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.

5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6. Hasło nie może być takie samo, jak 5 poprzednich haseł.
7. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
8. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom bez zgody Pracodawcy / Przełożonego.

9. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, nieupoważnionym pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. **Polityka czystego ekranu**.
3. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
4. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. wylogować się z systemu informatycznego, a jeśli to wymagane – następnie wyłączyć sprzęt komputerowy,
    b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

10. Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Elektroniczne nośniki to: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.
2. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy / Zleceniodawcy.
3. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane.

4. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe, należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.
5. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji IOD.

11. Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz kierownicy właściwych jednostek organizacyjnych.
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach, zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3. Użytkownicy są zobowiązani do stosowania „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu dokumentów, np. w szafach, biurkach, pomieszczeniach, przed kradzieżą lub dostępem osób nieupoważnionych.
4. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

12. Polityka kluczy

1. Polityka kluczy obejmuje wszystkie siedziby INSTYTUTU SLAWISTYKI PAN w Warszawie, Poznaniu i Krakowie, w szczególności dostęp do budynku oraz pomieszczeń.
2. Obowiązuje pięciodniowy tydzień pracy, od poniedziałku do piątku, w godzinach 9:00- 16:00
3. Pomieszczenia otwierane są kluczami znajdującymi się w posiadaniu i pod opieką pracowników.

4. Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych.
5. Klucze zapasowe przechowywane są w sekretariacie. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz w sytuacjach awaryjnych za zgodą osób uprawnionych. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.
6. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
7. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
8. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
9. Po zakończeniu pracy klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
10. Po zakończeniu pracy pracownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności:
    - wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych,
    - wyłączenia oświetlenia,
    - zabezpieczenia i zamknięcia okien i drzwi,
    - zamknięcia szaf i szafek na klucz oraz zabezpieczenia kluczy,
    - zastosowania Polityki czystego biurka – zabronione jest pozostawianie niezabezpieczonych dokumentów zawierających dane osobowych po zakończeniu pracy.
11. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

13. Zapewnienie poufności danych osobowych

1. Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez Pracodawcę / Zleceniodawcę.
2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem, o ile nie są one jawne.

3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne.
4. Zabrania się przekazywania w tym bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

14. Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Użytkownik zobowiązany jest do powiadomienia IOD lub ASI w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Typowe sytuacje, w których użytkownik powinien powiadomić IOD:
    a. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
    b. dokumentacja jest niszczona bez użycia niszczarki,
    c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
    d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
    e. ustawienie monitorów pozwala na wgląd osób postronnych do danych osobowych,
    f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia IOD,
    g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej, ustnej,
    h. telefoniczne próby wyłudzenia danych osobowych,
    i. kradzież komputerów lub CD, twardych dysków, pen-drive z danymi osobowymi,
    j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
    l. hasła do systemów przyklejone są w pobliżu komputera.

15. Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.