**DEKLARACJA**

**wdrożonych zasad bezpieczeństwa**

**w Krajowym Sekretariacie Metalowców NSZZ „Solidarność”**

Niniejszy dokument określa zasady bezpieczeństwa informacji i ochrony danych osobowych stosowane przez administratora w celu spełnienia wymagań 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.

**Analiza ryzyka pod kątem prywatności i ochrony danych**

1. Dokonuje się oceny ryzyka pod kątem prywatności i ochrony danych osobowych   
z uwzględnieniem czynników wewnętrznych i zewnętrznych, uwzględniając   
w szczególności: wielkość, strukturę organizacyjną, możliwości techniczne czy też rodzaj, zakres i cel przetwarzania danych.

2. Przeglądy analizy ryzyka wykonywane są cyklicznie lub w przypadku istotnych zmian, jednakże nie rzadziej niż raz w roku.

3. Analiza ryzyka przeprowadzona jest w następujących krokach:

a. ustalenie procesu przetwarzania, czyli ustalenie jakie dane są przetwarzane, w jaki sposób dane są zbierane, jak są wykorzystywane i przechowywane;

b. kontrola prawna, czyli upewnienie się, że proces przetwarzania jest zgodny z prawem, spełnia wszystkie wymagania administratora danych oraz wszystkie obowiązki względem klienta, pracownika, współpracownika;

c. określenie realnych zagrożeń dla danych osobowych, tj. takich zagrożeń, które mogłyby skutkować utratą danych, ich nieuprawnioną zmianą lub nieuprawnionym udostępnieniem. Nie są rozpatrywane zagrożenia, których wystąpienie jest bardzo mało prawdopodobne lub niemożliwe;

d. analiza jakie zabezpieczenie są stosowane by zapobiec zidentyfikowanym zagrożeniom oraz weryfikacja czy stosowane zabezpieczenia są wystarczające. Jeśli nie są wystarczające, to należy rozważyć zmianę lub zastosowanie dodatkowych zabezpieczeń.

4. Podejmuje się działania i wdraża zidentyfikowane w wyniku analizy ryzyka dodatkowe zabezpieczenia.

**Rejestr kategorii czynności przetwarzania**

Prowadzi się rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora danych osobowych.

**Zasady bezpieczeństwa informacji i ochrony danych osobowych**

1. Zasada czystego biurka i czystego ekranu:

a. opuszczając swoje miejsce pracy nawet na chwilę, pamiętaj o tym, by zablokować komputer;

b. nie pozostawiaj na biurku dokumentów bez nadzoru;

c. po zakończonej pracy zabezpiecz dokumenty papierowe i inne nośniki danych.

2. Zasada zamykania drzwi do pokoju:

a. pamiętaj, by za każdym razem, kiedy wychodzisz ze swojego pokoju, zamykać

drzwi na klucz. Otwarte pomieszczenie to swobodny dostęp do dokumentów i innych wartościowych przedmiotów, które się w nim znajdują.

3. Zasada noszenia kluczy przy sobie:

a. nie pożyczaj kluczy do pokoju;

b. osoby z zewnątrz mogą przebywać w pomieszczeniach wyłącznie w towarzystwie osób upoważnionych.

4. Zasada niezdradzania tajemnic oraz nierozmawiania o sprawach służbowych poza pracą:

a. wszelkie wiadomości uzyskane w związku z wykonywanymi czynnościami służbowymi wymagają ochrony przed nieuprawnionym ujawnieniem. Dlatego nie rozmawiaj o sprawach służbowych, przebywając poza pracą. Prowadząc w miejscu publicznym służbową rozmowę telefoniczną, zachowaj dyskrecję i unikaj możliwości jej podsłuchania;

b. jeżeli udostępniasz dane osobowe dokładnie zweryfikuj tożsamość odbiorcy. Musisz mieć pewność, że ta osoba jest upoważniona do ich otrzymania.

5. Zasada ochrony i korzystania ze sprzętu mobilnego:

a. sprzęt mobilny (laptopy, telefony, pendrive’y itp.) należy zabezpieczyć przed kradzieżą oraz nieuprawnionym dostępem do umieszczonych na nim danych;

b. zwracaj uwagę, aby osoby nieuprawnione nie miały dostępu do treści wyświetlanych na ekranie Twojego monitora;

c. nie korzystaj z nośników danych pochodzących z nieznanego źródła (np. znalezionych pendrive’ów), ponieważ może być na nich zainstalowane złośliwe oprogramowanie.

6. Zasada poufności i niepowtarzalności haseł oraz loginów:

a. w systemach informatycznych każdy pracownik ma spersonalizowany login;

b. nigdy nie ujawniaj swoich haseł dostępu.

7. Zasada czystych drukarek/kser/faksów/koszy oraz niszczenia zbędnych dokumentów:

a. natychmiast po wydrukowaniu dokumenty należy zabierać z drukarek, faksów i kser;

b. zadbaj o to, by wszystkie dokumenty – które nie służą do dalszego wykorzystania – były niszczone w sposób uniemożliwiający ich odczytanie. Przy czym należy w tym przypadku zwracać szczególną uwagę, które dokumenty podlegają zniszczeniu tak, aby nie zniszczyć dokumentów, które należy wykorzystywać w dalszych procesach czy należy je archiwizować;

c. nie pozostawiaj w koszu żadnych dokumentów, które mogą zawierać ważne informacje bądź dane osobowe. Przed wysłaniem dokumentu do wydrukowania upewnij się, że wybrałeś prawidłowe urządzenie.

8. Zasada przechowywania dokumentów:

a. dokumenty przechowuj z dala od widoku osób postronnych, stosując zasadę czystego biurka.

9. Zasada ostrożności w korzystaniu z poczty elektronicznej oraz legalności oprogramowania:

a. nie udostępniaj nikomu swojej skrzynki poczty elektronicznej;

b. odbierając pocztę, zachowaj szczególną ostrożność w przypadku otwierania załączników pochodzących od nieznanych nadawców, czytania wiadomości, co do których istnieje podejrzenie załączenia wirusa komputerowego;

c. nie instaluj żadnego oprogramowania oraz nie przechowuj treści, wobec których nie posiadasz praw autorskich bądź licencji.

10. Zasady organizacji dostępu do poczty elektronicznej i Internetu:

a. zabezpiecz przesyłane drogą elektroniczną poufne informacje, wykorzystując w tym celu mechanizmy szyfrujące.

11. Zgłaszanie incydentów oraz luk w bezpieczeństwie informacji:

a. jeśli zauważysz sytuację, która może spowodować zagrożenie lub ujawnienie informacji służbowych, zgłoś zaobserwowany incydent bądź luki w bezpieczeństwie;

b. wszelkie incydenty bezpieczeństwa zgłaszaj podając jak najwięcej informacji, które pomogą wyjaśnić zdarzenie.

12. Dbanie o poufność, prawidłowość i integralność danych:

a. dbaj o to, aby dane na których pracujesz były prawidłowe.

**Upoważnienia**

1. Osoby które mogą mieć dostęp lub mogą przetwarzać dane osobowe muszą zostać do tego upoważnione.

2. Wymagane jest prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

3. Dodatkowo - ze względu na powierzenie danych - wymaga się, aby osoby te podpisały oświadczenie o zachowaniu poufności.

**Odpowiedzialność**

Naruszenie przepisów ochrony danych osobowych, przez ujawnienie ich osobom lub podmiotom nieuprawnionym, jak też wykorzystanie ich dla celów innych, niż wykonywanie obowiązków służbowych, zagrożone jest odpowiedzialnością cywilną do wysokości szkody poniesionej przez administratora na skutek nie zachowania się do ustalonych procedur związanych z ochroną danych osobowych i karną przewidzianą przez obowiązujące przepisy.

**Szkolenia**

Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby przeszkolone w zakresie zasad bezpieczeństwa oraz stosowania przepisów z zakresu ochrony danych osobowych.

**Przeglądy**

Regularnie dokonuje się weryfikacji, pomiaru i oceny skuteczności środków organizacyjnych i technicznych mających zapewnić bezpieczeństwo informacji oraz ochronę danych osobowych.