**INSTRUKCJA** **ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**

**służącym do przetwarzania danych osobowych**

1. **CEL OPRACOWANIA DOKUMENTU**

Celem niniejszego dokumentu jest określenie sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, używanymi przez **Katarzynę Kaźmierczak**, prowadzącą działalność gospodarczą pod nazwą : **Poznaj Duszę Katarzyna Kaźmierczak**, ul. Fabryczna 16A, 62-030 Luboń (zwaną dalej jako **Przedsiębiorcą**).

1. **DEFINICJE**
2. **administrator danych** – Katarzyna Kaźmierczak,
3. **dane osobowe –** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne),
4. **informatyczne nośniki danych –** materiały lub urządzenia służące do zapisywania, przechowywania i odczytywania danych osobowych w postaci cyfrowej lub analogowej,
5. **odbiorca danych** – każdy, komu udostępnia się dane osobowe, z wyłączeniem: (i) osoby, której dane dotyczą; (ii) osoby upoważnionej do przetwarzania danych; (iii) przedstawiciela, o którym mowa w art. 31a Ustawy; (iv) podmiotu przetwarzającego dane osobowe na zlecenie administratora; (v) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępnianie w związku z prowadzonym postępowaniem;
6. **Polityka bezpieczeństwa** – dokument wewnętrzny wydany przez Przedsiębiorcę,
7. **przetwarzanie danych osobowych –** jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie udostępnianie i usuwanie, a zwłaszcza te które wykonuje się w systemach informatycznych,
8. **System Informatyczny** lub **System** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych u Przedsiębiorcy;
9. **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą (”anonimizacja”),
	1. **ZAKRES ZASTOSOWANIA**

Instrukcja określa zasady zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, a w szczególności:

1. procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w Systemie Informatycznym;
2. metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3. procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników Systemu;
4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5. sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
6. sposób zabezpieczenia Systemu Informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania;
7. sposoby realizacji w Systemie wymogów dotyczących przetwarzania danych;
8. procedury wykonywania przeglądów i konserwacji Systemu oraz nośników informacji służących do przetwarzania danych.
	1. **REJESTROWANIE I WYREJESTROWANIE UŻYTKOWNIKA – NADAWANIE UPRAWNIEŃ**
9. Użytkownikiem Systemu Informatycznego, mającym dostęp do danych osobowych (osobą upoważnioną) może być osoba, której nadano upoważnienie do przetwarzania danych osobowych.
10. Uzyskanie uprawnień następuje na dwóch poziomach:
11. Zarejestrowanie w systemie (założenie konta),
12. Nadanie upoważnienia do przetwarzania danych osobowych.
13. Uprawnienia osób upoważnionych do przetwarzania danych osobowych są rejestrowane w systemie informatycznym oraz odnotowywane w „Ewidencji osób upoważnionych do przetwarzania danych osobowych”. Wszystkie formularze i inne dokumenty związane z rejestrowaniem i wyrejestrowaniem użytkownikówsą archiwizowane i przechowywane.
14. **SPOSÓB UWIERZYTELNIANIA UŻYTKOWNIKA I ZASADY KORZYSTANIA Z HASEŁ**
15. Każdorazowe uwierzytelnienie użytkownika w systemie informatycznym następuje po podaniu identyfikatora i hasła.
16. U Przedsiębiorcy obowiązują następujące zasady korzystania z haseł:
	1. Hasło użytkownika składa się z co najmniej z 4 znaków,
	2. Elementy systemu informatycznego związane z bezpieczeństwem dostępu są tak sparametryzowane, aby wymusić stosowanie podanych zasad.
17. Prawidłowe wykonywanie obowiązków związanych z korzystaniem przez użytkowników z haseł nadzoruje osoba odpowiedzialna za obsługę informatyczną. Nadzór ten w szczególności polega na okresowym monitorowaniu funkcjonowania mechanizmu uwierzytelniania.
18. **PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY**
19. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
20. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
21. Włączenia komputera,
22. Uwierzytelnienia się (logowania) w systemie informatycznym za pomocą swojego identyfikatora i hasła,
23. Uwierzytelnienia się (logowania) w ramach bazy danych.
24. Niedopuszczalne jest logowanie się z wykorzystaniem identyfikatora i hasła innego użytkownika.
25. Przy opuszczaniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy uniemożliwić osobom nieuprawnionym dostęp do Systemu Informatycznego, np. poprzez zastosowanie wygaszacza ekranu wymagającego podania hasła lub poprzez wylogowanie się z Systemu.
26. Zakończenie przez użytkownika pracy w systemie informatycznym następuje po wylogowaniu się z Systemu. Po zakończeniu pracy użytkownik zobowiązany jest zabezpieczyć swoje stanowisko pracy, w szczególności informatyczne nośniki danych, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych oraz wyłączyć komputer, bądź pozamykać wszystkie otwarte bazy danych, pliki i aplikacje i zablokować konsolę.
27. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania się w systemie informatycznym oraz/lub bazie danych użytkownik niezwłocznie powiadamia o nich pracownika odpowiedzialnego za obsługę informatyczną.
28. **PROCEDURA TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA**
29. Administrator danych odpowiada za okresowe wykonanie kopii bezpieczeństwa danych gromadzonych w Systemie Informatycznym, przy pomocy przewidzianych przez System Informatyczny narzędzi.
30. Nośniki z backupem są okresowo sprawdzane pod kątem ich przydatności do odtworzenia danych.
31. **SPOSÓB I CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII INFORMATYCZNYCH ORAZ WYDRUKÓW**
32. Za zewnętrzne nośniki danych uważa się w szczególności :
* dyskietki, dyskietki zip;
* dyski CD-R, CD-RW, DVD-R, DVD-RW itp.;
* twarde dyski wymienne;
* taśmy magnetyczne;
* komputery przenośne;
* inne nośniki, służące do przechowywania danych i mogące być przenoszone niezależnie od sprzętu komputerowego.
1. Dane osobowe w postaci elektronicznej, za wyjątkiem kopii bezpieczeństwa, mogą być wynoszone poza obszar przetwarzania danych osobowych określony w Polityce Bezpieczeństwa tylko w przypadku zapisania ich na przeznaczonym do tego komputerze przenośnym.
2. Wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych.
3. Po zakończeniu pracy przez użytkowników Systemu Informatycznego wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamykanych szafach biurowych lub kasetkach.
4. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, są pozbawiane przez administratora danych zapisu tych danych, a w przypadku, gdy nie jest to możliwe, są uszkadzane w sposób uniemożliwiający ich odczytanie.
5. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do naprawy są pozbawiane przez administratora danych zapisu tych danych.
6. Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z danymi osobowymi należy dokonywać w sposób uniemożliwiający odczyt danych osobowych.
7. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.
8. Dostęp do wydruków z Systemu Informatycznego zawierających dane osobowe mają wyłącznie osoby do tego upoważnione.
9. Wydruki są przechowywane w miejscu uniemożliwiającym bezpośredni do nich dostęp osobom niepowołanym.
10. **PROCEDURA I SPOSÓB ZABEZPIECZENIA PRZED OPROGRAMOWANIEM, KTÓREGO CELEM JEST NIEUPRAWNIONY DOSTĘP DO ZASOBÓW SYSTEMU INFORMATYCZNEGO ORAZ POSTĘPOWANIE W PRZYPADKU AWARII ZASILANIA**
11. Na wszystkich komputerach (w tym także komputerach przenośnych) oraz serwerach zostało zainstalowane oprogramowanie antywirusowe oraz oprogramowanie zapobiegające nieuprawnionemu dostępowi do Systemu Informatycznego.
12. W przypadku stwierdzenia wystąpienia wirusa administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do podjęcia działań zmierzających do wykrycia źródła pojawienia się wirusa w Systemie Informatycznym, jego wyeliminowania, a jeśli jest to niemożliwe – do usunięcia zainfekowanego pliku.
13. Sprzęt komputerowy służący do przetwarzania danych osobowych jest wyposażony w urządzenia podtrzymujące zasilanie.
14. W przypadku wystąpienia przerw w dostawie energii elektrycznej administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
* zakończenia trwających procesów;
* zakończenia pracy sprzętu (np. komputera).
1. Po przywróceniu zasilania i upewnieniu się, że jest ono trwałe, administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
* włączenia sprzętu komputerowego;
* kontroli poprawności jego funkcjonowania i działania Systemu Informatycznego.
1. W przypadku stwierdzenia nieprawidłowości działania Systemu Informatycznego administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do niezwłocznego podjęcia czynności, związanych z usunięciem awarii, opisanych w punkcie 3 poniżej.
2. **PROCEDURA USUWANIA AWARII SPRZĘTU LUB OPROGRAMOWANIA**
3. W przypadku wystąpienia awarii Systemu Informatycznego pracownik lub współpracownik, który ją stwierdził zobowiązany jest do zgłoszenia faktu wystąpienia awarii administratorowi danych lub osobie odpowiedzialnej za obsługę informatyczną.
4. Administrator danych lub osoba odpowiedzialna za obsługę informatyczną zobowiązany jest do niezwłocznego podjęcia czynności zmierzających do usunięcia awarii np. poprzez wezwanie serwisu.
5. Po usunięciu awarii administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
* uruchomienia Systemu Informatycznego;
* kontroli poprawności jego funkcjonowania;
* kontroli integralności danych.
1. W przypadku stwierdzenia uszkodzenia danych zgromadzonych w Systemie, administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do otworzenia danych z ostatniej posiadanej kopii bezpieczeństwa (backup).
2. W przypadku gdy usunięcie awarii wymaga przekazania sprzętu komputerowego na zewnątrz, przed przekazaniem tego sprzętu administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do usunięcia z dysków twardych wszystkich danych, po ich uprzednim skopiowaniu na inny nośnik. Jeśli z przyczyn technicznych jest to niemożliwe, osoba przekazująca sprzęt ze strony Przedsiębiorcy zobowiązana jest uzyskać od serwisanta protokół przyjęcia danych i zobowiązanie do zachowania ich poufności.
3. **SPOSÓB REALIZACJI WYMOGU ZAPISANIA W SYSTEMIE INFORMATYCZNYM INFORMACJI O ODBIORCACH DANYCH**
4. Aktualnie dane osobowe nie są udostępniane innym podmiotom, niż wynika to z przepisów prawa.
5. W przypadku udostępniania danych osobowych w Systemie Informatycznym możliwe jest sporządzenie i wydrukowanie raportu, zawierającym następujące informacje:
* identyfikatora osoby, której dane dotyczą;
* odbiorcy danych;
* zakresu udostępnienia danych osobowych;
* daty operacji udostępnienia.
1. **SPOSÓB I CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII INFORMATYCZNYCH ORAZ WYDRUKÓW**
2. Dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w specjalnie do tego celu przeznaczonych segregatorach, w szafach zamykanych na klucz.
3. Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z danymi osobowymi należy dokonywać w sposób uniemożliwiający odczyt danych osobowych.
4. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.
5. **PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFORMATYCZNEGO ORAZ INFORMATYCZNYCH NOŚNIKÓW DANYCH**
6. Przegląd i konserwacja Systemu Informatycznego oraz informatycznych nośników danych zawierających dane osobowe dokonywane są poprzez:
7. sprawdzanie zgodności danych z dokumentami,
8. analizę zgłaszanych uwag użytkowników.
9. Przeglądu i konserwacji Systemu Informatycznego dokonuje administrator danych, osoba odpowiedziana za obsługę informatyczną lub inny upoważniony pracownik. Dopuszczalne jest zlecenie/powierzenie przeglądów i konserwacji zbiorów danych wyspecjalizowanym podmiotom zewnętrznym na podstawie pisemnych umów.
10. Przekazywane na zewnątrz Informatyczne nośniki danych (komputery, dyski, laptopy), dla celów naprawy czy konserwacji, nie zawierają baz (zbiorów) danych osobowych.