4. Administrator Danych powierza przetwarzanie danych osobowych w formie usługi zewnętrznej na podstawie umowy powierzania danych do przetwarzania. Każdorazowo należy dostosować umowę powierzenia do przekazywanych danych (przykładowy wzór patrz **Załącznik nr 4 Umowa powierzenia**)
5. Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia danych do przetwarzania oraz zobowiązany jest do stosowania zabezpieczeń określonych w art. 28 RODO.

Procedura nadawania uprawnień do przetwarzania danych osobowych

Procedura opisuje zasady przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania danych osobowych w systemie informatycznym lub w zbiorach papierowych. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty poufności przez osoby nieupoważnione.

1. Przyznanie i anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym wraz z uprawnieniami do przetwarzania tych danych realizowane jest na zlecenie Dyrektora Szkoły. Upoważnienie przekazywane jest IOD(patrz **Załącznik nr 5 Upoważnienie do przetwarzania danych osobowych**)
2. IOD jest zobowiązany do aktualizacji upoważnień i ich zakresu (np. z powodu zatrudnienia, urlopu, dostępu do zbiorów lub zmiany stanowiska pracy) oraz do prowadzenia ewidencji upoważnień.
3. Jeśli jest to wymagane, Dyrektor Szkoły określa dla osoby upoważnionej jej zakres uprawnień w systemach informatycznych.
4. IOD odpowiada za przechowywanie i aktualizację wszystkich Upoważnień.

E. SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

1. Przed rozpoczęciem przetwarzania danych osobowych pracownik powinien zostać przeszkolony przez Administratora Bezpieczeństwa Informacji.
2. Szkolenie powinno obejmować następujące zagadnienia:
   a. Przepisy o ochronie danych osobowych.
   b. Zasady przetwarzania danych osobowych.
   c. Procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych .
   d. Zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.
   e. Zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych.
   f. Zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe.
   g. Sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego.
   h. Odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

2.2. ŚRODKI OCHRONY FIZYCZNEJ OCHRONY DANYCH OSOBOWYCH

1. Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami drewnianymi pełnymi.
2. Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
3. Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych metalowych i niemetalowych szafach.
4. Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są na dysku sieciowym w postaci kopii elektronicznej.
5. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
6. Każde elektroniczne urządzenie (np. komputer stacjonarny, laptop, smartfon, tablet) oraz każdy elektroniczny nośnik informacji (np. zewnętrzny dysk twardy, pendrive) może być wykorzystywany do przechowywania danych osobowych tylko i wyłącznie pod warunkiem uprzedniego zaszyfrowania urządzenia lub nośnika, w celu uniemożliwienia odczytu danych osobom nieuprawnionym.