investrade

**Procedura obsługi żądań dostępu do danych**

**Cel procedury:**
Zapewnienie prawidłowej obsługi żądań dostępu do danych osobowych zgodnie z wymogami prawnymi (w szczególności RODO) oraz ochrona danych przed nieautoryzowanym ujawnieniem.

**Zakres procedury:**
Procedura obejmuje wszystkie żądania dostępu do danych osobowych wpływające od osób fizycznych (podmiotów danych), organów państwowych lub stron trzecich.

---

**Etapy obsługi żądania:**

1. **Zgłoszenie żądania:**
    - Żądanie może zostać złożone pisemnie, elektronicznie (poprzez dedykowany adres e-mail) lub osobiście w siedzibie firmy.
    - Każde zgłoszenie powinno zawierać: imię i nazwisko wnioskodawcy, szczegóły dotyczące danych, których żądanie dotyczy, oraz podstawę prawną (jeśli dotyczy).
2. **Weryfikacja tożsamości wnioskodawcy:**
    - Przed udostępnieniem danych konieczne jest potwierdzenie tożsamości wnioskodawcy poprzez weryfikację dokumentu tożsamości lub innych danych potwierdzających.
3. **Analiza zasadności żądania:**
    - Dział odpowiedzialny za ochronę danych (Inspektor Ochrony Danych lub osoba wyznaczona) analizuje zasadność żądania w oparciu o obowiązujące przepisy prawne.
4. **Realizacja żądania:**
    - Udostępnienie danych powinno nastąpić w terminie 30 dni od dnia otrzymania żądania. W uzasadnionych przypadkach możliwe jest przedłużenie tego terminu o dodatkowe 60 dni, z powiadomieniem wnioskodawcy o przyczynach opóźnienia.
    - Jeśli żądanie jest bezzasadne, wnioskodawca zostanie poinformowany o powodach odmowy.
5. **Rejestracja żądania:**
    - Każde żądanie musi zostać zarejestrowane w wewnętrznym rejestrze żądań, zawierającym datę zgłoszenia, treść żądania, wynik analizy oraz sposób realizacji.

---

**Opis działania zapór sieciowych (firewalli)**

**Cel:**
Zapory sieciowe (firewalle) w firmie Investrade sp. z o.o. mają na celu ochronę sieci wewnętrznej oraz danych firmowych przed nieautoryzowanym dostępem, atakami z zewnątrz oraz potencjalnymi zagrożeniami.

investrade

**Rodzaje stosowanych zapór sieciowych:**

1. **Zapory sprzętowe:**
    - Chronią ruch sieciowy na poziomie fizycznym.
    - Kontrolują przepływ danych pomiędzy siecią wewnętrzną a Internetem.
2. **Zapory programowe:**
    - Zainstalowane na komputerach i serwerach w celu ochrony poszczególnych urządzeń.
    - Monitorują i filtrują ruch w czasie rzeczywistym.

**Główne funkcje firewalli:**

- **Filtrowanie ruchu sieciowego:** Blokowanie nieautoryzowanych połączeń i dopuszczanie jedynie ruchu zgodnego z ustalonymi regułami.
- **Wykrywanie zagrożeń:** Rozpoznawanie i blokowanie potencjalnych ataków, takich jak próby włamania czy ataki typu DDoS.
- **Rejestrowanie zdarzeń:** Tworzenie logów dotyczących ruchu sieciowego oraz potencjalnych incydentów.

**Zarządzanie zaporami:**

- Konfiguracja i monitorowanie zapór sieciowych jest prowadzone przez wyznaczony dział IT lub zewnętrznego dostawcę usług.
- Regularne aktualizacje i przeglądy konfiguracji firewalli zapewniają skuteczność ochrony.

**Audyt i testowanie:**

- Zapory sieciowe są regularnie testowane pod kątem skuteczności działania.
- Przeprowadzane są audyty, aby zapewnić zgodność z najlepszymi praktykami i standardami branżowymi.

---

**Odpowiedzialność za realizację procedur:**

- Za wdrożenie i utrzymanie procedury obsługi żądań dostępu do danych odpowiada Inspektor Ochrony Danych (IOD).
- Za konfigurację, monitorowanie i zarządzanie zaporami sieciowymi odpowiada Dział IT lub wyznaczony zewnętrzny dostawca usług IT.

Data publikacji: 24.10.2025, Lublin