Załącznik 2: Opis zabezpieczających środków technicznych i organizacyjnych do Umowy przetwarzania danych w imieniu Administratora nr PZ-… („Umowa")

Komentarz [A1]: Uzupełnia innogy

Opisane w tym dokumencie środki techniczne i organizacyjne ustala się jako obowiązujące pomiędzy _____ (Administrator) a _____ (Procesor).

Komentarz [A2]: Uzupełnia innogy

Komentarz [A3]: Uzupełnia PRocesor – pełna nazwa firmy

We wszystkich przypadkach, które poniżej odnoszą się do ochrony danych Administratora, należy w szczególności rozumieć ochronę danych osobowych, których administratorem (w rozumieniu Rozporządzenia) jest Administrator.

Pojęcia nie zdefiniowane inaczej w niniejszym załączniku mają znaczenie nadane im w Umowie.

1. Poufność

1.1. Kontrola dostępu fizycznego

1.1.1. Budynki należące lub wykorzystywane jako składnik przedsiębiorstwa Procesora są zabezpieczone urządzeniami alarmowymi.

1.1.2. Drzwi wejściowe do któregokolwiek z ww. budynków są wyposażone w następujące systemy zamykania: system zamków zamykanych manualnie lub system dostępu z wykorzystaniem kart chipowych.

1.2. Kontrola dostępu do zasobów IT

1.2.1. Sieć korporacyjna (komputery firmowe) jest chroniona od strony sieci publicznej przez wdrożone zabezpieczenia sieci IP (np. firewall).

1.2.2. Pracownicy są zobowiązani do przestrzegania następujących zaleceń w odniesieniu do haseł:
- Każdy pracownik ma indywidualne hasło do komputera i ma obowiązek utrzymywania go w tajemnicy;
- Nie używa się haseł zbiorowych;
- Wymuszana jest cykliczna zmiana hasła;
- Wymuszone jest automatyczne blokowanie ekranu.

1.2.3. W interfejsach sieci tj. konta email, FTP są używane skanery antywirusowe.

1.2.4. Na serwerach używany jest skaner antywirusowy.

1.2.5. Na wszystkich stacjach roboczych używany jest skaner antywirusowy.

1.2.6. Aktualizacje oprogramowania związane z bezpieczeństwem są regularnie i automatycznie wgrywane do istniejącego oprogramowania.

1.3. Kontrola dostępu użytkowników do danych

1.3.1. Jeśli istnieje możliwość zdalnej konserwacji/ zdalnego dostępu, to jest on realizowany w sposób bezpieczny.

2. Integralność

2.1. Kontrola przekazywania danych

2.1.1. Komplet danych jest przekazywany bezpośrednio osobie upoważnionej działającej w imieniu Administratora lub wymiana danych pomiędzy Administratorem a Procesorem realizowana jest przy użyciu metod kryptograficznych (np. SFTP, S/MIME, szyfrowany nośnik danych).

2.1.2. Wykonywane jest szyfrowanie dysków lokalnych na przenośnych stacjach roboczych w celu ochrony danych Administratora.

2.1.3. Nośniki kopii zapasowych są bezpiecznie przechowywane.

3. Dostępność

3.1. Kontrola dostępności

3.1.1. Wykonywane są regularnie kopie zapasowe dokumentacji zawierającej dane osobowe oraz danych w formie elektronicznej.

4. Kontrola przetwarzania danych osobowych

4.1. Kontrola zadań

4.1.1. Jeżeli usługa jest świadczona z wykorzystaniem usług cloudowych, przedkłada się również zarys architektury pokazujący wykorzystane komponenty IT, miejsca przechowywania i stosowane protokoły (proszę podać wykorzystywane usługi chmurowe): _____

☐ Nie korzystam z usług cloudowych w celu realizacji umowy.

Komentarz [A4]: Jeśli zasadne, wypełnia Procesor

4.2. Sprawy różne

4.2.1. Opis dodatkowych środków technicznych i organizacyjnych wprowadzonych przez Procesora, jeśli występują

.....
.....

Komentarz [A5]: Jeśli zasadne, wypełnia Procesor (np. systemy alarmowe, systemy monitoringu)

5. Podpis

Potwierdzamy, że dostarczone informacje odzwierciedlają bieżące techniczne i organizacyjne środki, które stosujemy w celu zapewnienia poziomu ochrony i bezpieczeństwa danych. O wszelkich odstępstwach od podanych tu informacji należy bezzwłocznie powiadomić Administratora.

_____	_____
Nazwisko i imię osoby odpowiedzialnej, która dokonała merytorycznej weryfikacji załącznika i jego uzupełnień (wypełnić czytelnie)	podpis tej osoby

Administrator	**Procesor**
Data:	Data: .....
Imię i nazwisko:	Imię i nazwisko: .....
Podpis	Podpis .....
Imię i nazwisko:	Imię i nazwisko: .....
Podpis	Podpis .....