ORGANIZACYJNE ŚRODKI OCHRONY

L.p.	Nazwa	Opis	Koszt	Ochrona	Praca
1.	Zasady zarządzania projektami	Firma stosuje jasne i czytelne zasady egzekwowania czynności wykonywanych w celu osiągnięcia wyznaczonych celów głównych i pośrednich w skończonym czasie. Obejmuje między innymi planowanie, harmonogramowanie, realizację, kontrolę i rozliczanie zadań składających się na realizację celów projektu	1	1	2
2.	Regulamin obsługi incydentów	Lista kontrolna co ma zrobić kierownictwo firmy, w sytuacji kiedy Pracownik zgłasza podejrzenie naruszenia zasad ochrony danych. Celem jest to, aby tak szybko jak to możliwe zminimalizować wpływ na prawa i wolności podmiotów danych lub na poziom ochrony danych, przez przywrócenie poufności lub dostępności lub integralności danych osobowych.	2	4	2
3.	Regulamin zgłaszania naruszeń	Lista kontrolna dla Pracowników z max. 5 punktami opisującymi, co należy zrobić w sytuacji podejrzenia naruszenia ochrony danych. Celem jest jak najszybsze przekazanie przez Pracownika odpowiedzialności za obsługę incydentu do kierownictwa firmy.	2	5	1
4.	Pisemne upoważnienie do przetwarzania danych	Wymaganie wynikające w art. 29 RODO, ponieważ każda osoba mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie Administratora. Celem jest posiadanie udokumentowanego zbioru upoważnień do przetwarzania danych dla Pracowników	1	3	2
5.	Umowy z podmiotami przetwarzającymi	Wymaganie wynikające z art. 28 RODO. Celem jest posiadanie wzoru umowy powierzenia, zbioru podpisanych umów i ewidencji umów powierzenia	3	3	3
6.	Dokumentacja konfiguracji sprzętu, oprogramowania i usług IT	Dokument głównie w formacie .xls używany przez organizację do przechowywania informacji o zasobach sprzętowych i programowych. Dokumentacja działa jak repozytorium wiedzy nt. systemu informatycznego w firmie, a także przechowuje informacje dotyczące relacji między zasobami, np. ten przełącznik obsługuje 12 urządzeń: x, y, z.... Dokumentacja zapewnia sposoby zrozumienia kluczowych zasobów organizacji i relacji pomiędzy nimi, takich jak systemy informacyjne, źródła danych, usługi, lub zależności na zasobach (np. działanie serwera zależy od poprawnej konfiguracji ustawień sieciowych), ale również cele określane dla zasobów (np. backup dla serwera głównego).	1	3	2
7.	Cykliczne raporty dot. stanu ochrony danych	Sformalizowany sposób zapewniania rozliczalności stosowania RODO. Celem jest informowanie Kierownictwa i Pracowników o ich obowiązkach i doradzanie im w zakresie stosowania RODO, monitorowanie przestrzegania RODO przez firmę, wsparcie w realizacji oceny skutków dla ochrony danych. Realizowane przez wyznaczonego Pracownika lub przez specjalistę z firmy zewnętrznej. Przy spełnieniu warunków opisanych w art. 37 RODO powołanie IOD-a jest obowiązkowe	2	4	2
8.	Zasady realizacji praw podmiotów danych	Lista kontrolna czynności, jakie należy podjąć, żeby zrealizować wymagania RODO wynikające z art. 15 - 22. Chodzi m. in. prawo do dostępu do danych, prawo do zapomnienia, prawo do przenoszenia danych etc.	1	2	1
9.	Regulamin zabezpieczenia dokumentacji papierowej	Lista kontrolna opisująca, jak należy przechowywać (kłaść, przenosić, przekazywać, drukować) papierowe dokumenty	1	3	1
10.	Regulamin korzystania z komputerów służbowych	Lista kontrolna opisująca, jak należy korzystać z komputera służbowego, tj. jak rozpoczynać pracę z komputerem, jak przerywać pracę z komputerem, jak kończyć pracę z komputerem, jak przenosić i przechowywać komputer, jeśli laptop, jak dbać o sprzęt i system operacyjny.	1	3	2
11.	Szkolenia	Człowiek nie jest najsłabszym ogniwem w systemie ochrony, człowiek jest po prostu na pierwszej linii ataku cyber-przestępców, dlatego szkolenia dają świadomość zagrożeń i narzędzia do ich zwalczania lub ograniczania. Poza tym zgodnie z art. 32 ust. 1 lit. d) RODO Administratora powinien regularnie testować, mierzyć i oceniać skuteczność środków ochrony danych, a to można osiągnąć m. in. przez szkolenie Pracowników i ocenianie wyników szkoleń.	1	4	3
12.	Zasada częstego zmieniania haseł	Hasło powinno być często zmieniane, a dostęp do usług i danych blokowany, jeśli Pracownik tego nie zrobi.	1	1	5
13.	Procedura "Ocena skutków dla ochrony danych"	Obowiązek wynikający z art. 35, który należy realizować tylko i wyłącznie po spełnieniu warunków określonych w tym przepisie.	2	2	4
14.	Regulamin monitoringu wizyjnego	Obowiązek wynikający z art. 22 (2) Kodeksu Pracy	1	1	2
15.	Zasady realizacji obowiązku informacyjnego wobec podmiotów danych	Obowiązek wynikający z art. 12 - 14 RODO. Celem jest poinformowanie osoby, której dane dotyczą, w jakim celu, na jakiej podstawie i w jaki sposób będziemy przetwarzać jej dane.	1	3	2