

# TECHNICZNE (LOGICZNE) ŚRODKI OCHRONY

Lp.	Nazwa	Opis	Koszt	Ochrona	Praca
1.	Anonimizacja i pseudonimizacja	Umiejętność wykorzystania możliwości, jakie dają systemy CRM do anonimizowania (nieodwracalny proces, nikt nie rozpozna danych) lub pseudonimizowania (proces odwracalny, Administrator rozpozna dane) danych osobowych Gości. Celem jest spełnienie wymogu art 32 RODO dot. zachowania poufności danych oraz zapewnienie przestrzegania zasady ograniczania czasu przetwarzania i minimalizacji zakresu przetwarzanych danych.	1	5	4
2.	Kryptografia - "hasłowanie"	Wykorzystanie bezpłatnego oprogramowania typu VeraCrypt do szyfrowania plików, folderów, dysków lub pendrive'ów. Druga opcja polega na "hasłowaniu" plików w bezpłatnym oprogramowaniu do kompresowania danych. Celem jest spełnienie wymogu art 32 RODO dot. zachowania poufności danych	1	5	2
3.	Tworzenie backup	Sformalizowany i udokumentowany sposób tworzenia kopii zapasowych, w tym kopii trzymanyh w trybie "off-line". Celem jest zapewnienie dostępności i integralności danych	2	5	1
4.	Odtwarzanie backup	Sformalizowany i udokumentowany sposób odtwarzania kopii zapasowych, w tym testowanie poprawności odtwarzanych danych. Celem jest zapewnienie dostępności i integralności danych	4	5	2
5.	Segmentacja sieci WiFi	Oddzielenie sieci WiFi, z której mogą korzystać Goście od sieci WiFi do celów służbowych	3	5	2
6.	Monitorowanie systemu IT i jego użytkowników	Sformalizowany i udokumentowany sposób powiadamiania osób odpowiedzialnych o próbach nieuprawnionego dostępu na poziomie okablowania, sieci, serwerów i innych zasobów (które mogą dotyczyć wartości materialnych i niematerialnych) oraz na poziomie aplikacji.	3	5	3
7.	Antywirus/Antymalware na komputerze	Oprogramowanie antywirusowe zainstalowane, stale aktualizowane na komputerze Pracownika	1	3	1
8.	Ochrona sieci komputerowej "na wejściu i wyjściu"	Żeby ograniczyć ryzyko naruszenia zasad ochrony danych "na wejściu" do sieci komputerowej Hotelu stosujemy takie zabezpieczenia jak: Antywirus Antyspam Filtrowanie treści Wykrywanie "intruzów" w sieci komputerowej Zautomatyzowane raportowanie zagrożeń "sieciowych". Taka ochrona sieci komputerowej, to zmniejszenie do minimum prawdopodobieństwa i skutków ryzyka naruszenia praw i wolności.	3	5	2
9.	Menadżer haseł	Bezpłatne oprogramowanie typu KeePass pozwalające użytkownikowi zarządzać ważnymi danymi uwierzytelniającymi takimi jak konta, hasła, kody PIN, itd.	1	5	1
10.	Strona Internetowa do pozyskiwania zgód na przetwarzanie z tytułu RODO	Zgoda, zgodnie z art. 6 RODO jest jedną z 5 podstaw przetwarzania RODO. Zasady wyrażania zgód zostały opisane w art. 7 i 8 RODO. Strona internetowa stanowi interfejs dla Klientów do wyrażania zgody, jednocześnie wraz ze stroną działa baza danych, która przechowuje te zgody. Na razie mechanizm wycofywania zgody jest obsługiwany ręcznie.	4	1	4
11.	Sensory ruchu i rozpoznawania twarzy	Czujniki ruchu wykorzystuje się głównie do włączania oświetlenia lub inicjowania alarmu (np. włamaniowego), czy też np. do uruchamiania przepływu wody w toaletach. Rozpoznawanie twarzy nazuje na technologii, która pozwala na rozpoznawanie obiektów przedstawianych na cyfrowych obrazach o charakterze rastrowym, czyli w specjalnym formacie graficznym.	5	1	4