

L.P.	NAZWA ZBIORU DANYCH OSOBOWYCH	NAZWA I SIEDZIBA ADMINISTRATORA DANYCH	NAZWA KOMÓRKI ORGANIZACYJNEJ	DATA ZGŁOSZENIA ZBIORU DO REJESTRACJI	DATA DOKONANIA OSTATNIEJ ZMIANY	RODZAJ ZMIANY (nowy wpis, wykreślenie, aktualizacja)	ZAKRES ZMIANY	DATA WYKREŚLENIA ZBIORU	NAZWA PODMIOTU KTÓREMU POWIERZONO PRZETWARZANIE DANYCH	PODSTAWA PRAWNA UPOWAŻNIAJĄCA DO PROWADZENIA ZBIORU DANYCH	CEL PRZETWARZANIA DANYCH W ZBIORZE	OPIS KATEGORII OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE W ZBIORZE	ZAKRES DANYCH OSOBOWYCH PRZETWARZANYCH W ZBIORZE	SPOSÓB ZBIERANIA DANYCH DO ZBIORU	SPOSÓB UDOSTĘPNIANIA DANYCH ZE ZBIORU	OZNACZENIE ODBIORCY DANYCH LUB KATEGORII ODBIORCÓW, KTÓRYM DANE MOGĄ BYĆ PRZEKAZYWANE	INFORMACJA O PRZEKAZYWANIU DANYCH DO PAŃSTWA TRZECIEGO	FORMA ZBIORU (elektroniczny/papierowy)	LOKALIZACJA ZBIORU (budynek, numer pomieszczenia)	APLIKACJA (INF. PRZETWARZAJĄCA ZBIÓR DANYCH)	OPIS ŚRODKÓW TECHNICZNYCH ORG.
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	W	Z
1.	Dane klientów	Stefczyk Leasing Towarzystwo Zarządzające SKOK Sp. z o.o. S.K.A.	Pion Sprzedaży, Pion Wspierania Sprzedaży	1.07.2015	11.01.2017	aktualizacja	1. Dotarcie nazwy komórki org (kolumna D) 2. Zmiana lokalizacji i zbioru (kolumna U)	---	Aplitt S.A. z siedzibą w Gdańsku, Towarzystwo Zarządzające SKOK Sp. z o.o. S.K.A. z siedzibą w Gdyni	Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych art. 23.1.1)	Rozpatrzenie wniosku leasingowego i wykonywanie umowy, marketing usług przesyłany drogą elektroniczną	Klienci Stefczyk Leasing	imię, nazwisko, seria i nr dowodu, adres, nr Pesel, data urodzenia, nr telefonu, Nip, adres mailowy, informacje dot. podatku PIT	Od właścicieli danych	Nie dotyczy	nie dotyczy	nie dotyczy	elektroniczna i papierowa	Sopot, ul. T. Kościuszki 43 Gdynia, Al. Zwycięstwa 266	Greensoft, serwer, DGA Workflow	zgodnie z arkuszem "Opis środków"

f) inne środki, oprócz wymienionych w ppkt a - e, zastosowane w celu zabezpieczenia danych:

L.P.	RODZAJ ŚRODKÓW
Środki ochrony fizycznej danych:	
1	Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej ≥ 30 min.
2	Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
3	Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
4	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych objęte są systemem kontroli dostępu.
5	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
6	Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
7	Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:	
1	Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
2	Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
3	Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
4	Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
5	Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
6	Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.
7	Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
8	Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
9	Użyto system Firewall do ochrony dostępu do sieci komputerowej.
10	Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.
Środki ochrony w ramach narzędzi programowych i baz danych:	
1	Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
2	Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
3	Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
4	Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
5	Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
Środki organizacyjne:	
1	Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
2	Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
3	Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
4	Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.