

Temat	I.p.	Pytanie
Wstęp	1	Nazwa podmiotu
	2	Forma prawna
	3	Rok założenia spółki
	4	Czy współpracowali Państwo/ współpracują obecnie z LMPL? (jeśli tak, to proszę opisać w komentarzu).
	5	Czy u Państwa na stanowiskach kierowniczych lub na stanowiskach obsługujących współpracę z LMPL, są zatrudnione osoby będące uprzednio pracownikami LMPL?
	6	Czy byli lub obecni pracownicy LMPL są udziałowcami, współwłaścicielami lub pełnią funkcje nadzorcze w Państwa firmie?
	7	Czy posiadają Państwo wiedzę o jakimkolwiek konflikcie interesów w związku z podjęciem współpracy z LMPL?
	8	Potwierdzam, że powyższe dane są prawdziwe i na żądanie mogę być zobowiązany do przedłożenia stosownych dokumentów na potwierdzenie prawidłowości powyższych danych.
Governance	9	Proszę podać jaki rodzaj usługi ma być realizowany na rzecz LMPL
	10	Czy wyznaczyli Państwo Inspektora Ochrony Danych - prosba o podanie danych Inspektora
	11	Czy wdrożyli Państwo politykę prywatności? Proszę podać link do strony www lub przesłać poniżej załącznik z polityką prywatności
	12	Czy polityka prywatności i zasady ochrony danych osobowych zostały zaakceptowane przez pracowników?
	13	Czy posiadają Państwo politykę zarządzania bezpieczeństwem systemu informatycznego?
	14	Czy Państwa pracownicy przechodzą regularnie szkolenia z zakresu ochrony danych osobowych?
	15	Czy zapoznali się Państwo z zapisami regulacji odnośnie bezpieczeństwa zakupów i zobowiązują się do jego przestrzegania? <a href="https://media.leroymerlin.pl/-has/dla-dostawcy">https://media.leroymerlin.pl/-has/dla-dostawcy</a>
	16	Czy współpracują Państwo z podmiotami objętymi sankcjami (nałożonymi przez MSWiA, sankcjami międzynarodowymi)?
	17	Czy przestrzegają Państwo przepisów regulacji międzynarodowych dotyczących sankcji gospodarczych lub embargó uchwalonych, ogłoszonych lub nałożonych przez ONZ i UE oraz Stany Zjednoczone i Francję, o ile takowe Państwa dotyczą?
	18	Czy została nałożona na Państwa firmę kara administracyjna / sankcja (np. przez Urząd Ochrony Konkurencji i Konsumentów, Urząd Ochrony Danych Osobowych i inne organy polskie lub EU)?
Zarządzanie incydentami	19	Czy mają Państwo wdrożoną procedurę zarządzania incydentami / naruszeniami danych (m.in. wykrywanie incydentów/naruszeń, powiadamianie pracowników, powiadomienie osób, których naruszenie dotyczy, przeprowadzanie analizy, zawiadamianie Prezesa UODO itp.)
	20	Czy przeprowadzają Państwo okresowe testy naruszenia danych dotyczących danych osobowych?
Kontrole wewnętrzne / Audyty	21	Czy wdrożyli Państwo wewnętrzne kontrole i/lub okresowe audyty w celu przestrzegania przepisów prawa oraz wewnętrznych procedur, w tym ochrony danych osobowych i bezpieczeństwa IT na odpowiednim poziomie?
	22	Czy Państwa firma ma certyfikat zintegrowanego systemu zarządzania (np. ISO), raporty z audytu, inne certyfikaty? Prośba o załączenie.
Usługi / produkty/ rozwiązania IT	23	Czy umowa dotyczy dostarczenia produktu informatycznego? (Jeśli tak, to aktywują się poniższe pytania)
	24	Jak nazywa się ta usługa/ produkt/ rozwiązanie?
	25	Proszę opisać podstawową funkcjonalność produktu / rozwiązania
	26	Jakie są procedury potwierdzające mechanizmy zapewnienia ciągłości działania systemu w przypadku awarii (procedury backupu i przeprowadzane testy DRP) (proszę o przedstawienie dokumentacji)
	27	Czy produkt jest oparty o rozwiązanie SaaS, aplikację/ inne?
	28	Jaka jest forma wymiany danych?
	29	Czy są aktualne testy penetracyjne potwierdzające bezpieczeństwo aplikacji webowej (w przypadku aplikacji dostępnej przez www)?
	30	Proszę zaznaczyć które z poniższych elementów bezpieczeństwa IT zostały wdrożone w Państwa organizacji.
	31	Czy do aplikacji logować się będą pracownicy LMPL? Jaka jest forma logowania?
	32	Czy wdrożono zarządzanie poziomem uprawnień użytkowników (jeżeli w aplikacji są zdefiniowane dostępy do różnych obszarów i danych)? Polityka haseł?
Ochrona danych osobowych	33	Czy niniejsza usługa wymaga podpisania umowy powierzenia danych osobowych? (Jeśli tak, to aktywują się poniższe pytania)
	34	Czy mają Państwo podpisane umowy o powierzenie przetwarzania danych osobowych z subprocesorami (dostawcami usług IT)?
	35	Czy przeprowadzają Państwo regularnie (co najmniej raz na 2 lata) przeglądy z podwykonawcami w zakresie przestrzegania uzgodnionych środków ochrony danych osobowych?
	36	Prośba o wskazanie miejsca przetwarzania danych osobowych
	37	Jakie środki bezpieczeństwa mają Państwo wdrożone dla zapewnienia bezpiecznego hostingu?