Informacje | TOM na temat przetwarzania zleconego v1.0.3

Ujawnienie informacji na temat technicznych i organizacyjnych środków przetwarzania danych na zlecenie | Status: 20.10.2021

Zgodnie z przepisami Ogólnego Rozporządzenia o Ochronie Danych Osobowych UE (Art. 28 GDPR), klient musi sprawdzić przed rozpoczęciem przetwarzania danych, czy u zleceniobiorcy zostały zastosowane i są przestrzegane odpowiednie środki techniczne i organizacyjne w celu ochrony poufności, integralności, dostępności, odporności i możliwości odzyskania danych. Wynik tej kontroli należy udokumentować. Aby uprościć tę weryfikację, przedstawia się następujące oświadczenie własne. Dla szybkiej czytelności i przejrzystej prezentacji działań, samoujawnienie jest zaprojektowane jako lista kontrolna. Poszczególne środki wspierają kilka celów GDPR w zakresie ochrony danych. W celu uniknięcia powtórzeń, środki są zatem uporządkowane według ich celów. Ogólnie rzecz biorąc, środki te obejmują cele GDPR w zakresie ochrony danych.

Pytania dotyczą wyłącznie pracowników oraz systemów, procedur i urządzeń, którym powierzono wykonanie zleconych usług lub operacji przetwarzania danych lub które są wykorzystywane do ich wykonania.

W celu zapewnienia bezpiecznego i zgodnego z wymogami ochrony danych przetwarzania zleceń, wprowadzono opisane poniżej środki techniczne i organizacyjne.

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
1. informacje ogólne			
Czy został powołany inspektor ochrony danych?	☑	☐	Thorsten Schröers SAFE-PORT Consulting GmbH datenschutz@trilux.com | privacy@safe-port.de
Czy inspektor ochrony danych przechodzi regularne szkolenia?	☑	☐	IHK Arnsberg / Sauerland ITKservice GmbH IQ-Zert GmbH & Co KG
Jakie inne stanowisko(-a) oprócz tego zadania zajmuje inspektor ochrony danych?			Brak dalszych działań, jako zewnętrzny inspektor ochrony danych
Czy pracownicy są zobowiązani do zachowania poufności zgodnie z przepisami GDPR?	☑	☐	Wszyscy pracownicy Grupy TRILUX są zobowiązani do zachowania poufności i przestrzegania ochrony danych zgodnie z GDPR i BDSG.
Czy zobowiązanie jest weryfikowalnie udokumentowane?	☑	☐	Na piśmie w aktach osobowych
Czy pracownicy są stale instruowani w zakresie wymogów ochrony danych, jeśli tak, to w jaki sposób?	☑	☐	Rodzaj szkolenia ☑ Szkolenie online ☑ Instrukcje pisemne ☑ Regularne spotkania zespołu
Czy istnieje koncepcja usuwania danych z regulacją okresów zatrzymywania lub przechowywania oraz terminowego i bezpiecznego usuwania lub niszczenia danych?	☑	☐	
Czy istnieje systematyczne zarządzanie ochroną i bezpieczeństwem danych z uregulowaną procedurą przeglądu i oceny?	☑	☐	

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
Czy istnieje certyfikat bezpieczeństwa IT lub zarządzania bezpieczeństwem IT lub inny certyfikat dotyczący zgodnego z prawem wdrożenia ochrony danych w firmie?	☑	☐	Przetwarzanie danych odbywa się w centrum danych dostawcy usług w chmurze z siedzibą w UE. Jest on certyfikowany zgodnie z normą DIN EN/ISO IEC 2700x i podlega regularnym kontrolom.
Czy istnieje koncepcja ochrony danych lub podręcznik ochrony danych, który reguluje i wdraża ochronę danych w przedsiębiorstwie?	☑	☐	
Czy istnieje instrukcja bezpieczeństwa IT lub czy istnieją inne regulacje dotyczące technicznych i organizacyjnych środków ochrony danych?	☑	☐	
Czy korzysta się z usług podwykonawców?	☒	☐	
Jeżeli ma to zastosowanie, czy na podwykonawców nałożone są takie same obowiązki jak te, które zostały ustalone między instytucją zamawiającą a wykonawcą?	☑	☐	
Czy niezbędne umowy lub zobowiązania w zakresie ochrony danych istnieją również z dostawcami usług serwisowych i innych usług, a jeśli tak, to jakiego rodzaju?	☑	☐	Wszyscy usługodawcy są pisemnie - zobowiązani do przestrzegania obowiązujących przepisów o ochronie danych.
Czy przetwarzanie danych odbywa się na terytorium Republiki Federalnej Niemiec, czy też na terenie Unii Europejskiej lub państw Europejskiego Obszaru Gospodarczego?	☑	☐	

Wniosek	Spełnia wymagania		Komentarz / Wyjaśnienie
	J	N	
2. środki techniczne i organizacyjne			
2.1 Poufność (Art. 32 ust. 1 lit. b GDPR)			
2.1.1 Dostęp do przedsiębiorstwa			
Czy pomieszczenia i budynki są - zabezpieczone przed dostępem osób nieupoważnionych poza godzinami pracy?	☑	☐	☑ Ochroniarze ☑ Czujnik ruchu/system alarmowy ☑ System kontroli dostępu ☑ Centralny zamek, zamki bezpieczeństwa
Czy wejścia i wyjścia są zabezpieczone?	☑	☐	Drzwi wejściowe do budynku ☑ Tak☐ Nie Drzwi ewakuacyjne/ wyjścia awaryjne ☑ Tak☐ Nie☐ Nie dotyczy Klatki schodowe i schody przeciwpożarowe ☑ Tak☐ Nie☐ Nie dotyczy Dostawa i obszary dostawy ☑ Tak☐ Nie☐ Nie dotyczy
Czy prowadzenie i nadzór nad zwiedzającymi jest uregulowany?	☑	☐	☑ Recepcja ☑ Księga gości ☑ Odznaka gościa ☑ Indywidualne doradztwo dla zwiedzających
Czy nadzorowany jest personel zewnętrzny, np. personel konserwacyjny i serwisowy?	☑	☐	Personel konserwacyjny i serwisowy jest przez cały czas nadzorowany przez członka personelu odpowiedzialnego za dany obszar.

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
Czy wprowadzono kontrolę dostępu?	☑	☐	☑ System kontroli dostępu ☑ z ☐ bez stref bezpieczeństwa ☑ Centralny zamek z kluczem sterującym Uprawnienia dostępu są przyznawane pracownikowi tylko wtedy, gdy wystąpił o to odpowiedni przełożony i/lub dział kadr. Przy wydawaniu zezwoleń uwzględnia się zasadę konieczności.
Czy zdefiniowano obszary bezpieczeństwa, np. serwerownia, centrala, archiwum, rozdzielacze sieciowe i oddzielnie zabezpieczono je przed dostępem osób niepowołanych?	☑	☐	
Czy te strefy bezpieczeństwa są specjalnie chronione przed dostępem osób nieupoważnionych, jeśli tak, to w jaki sposób?	☑	☐	Rodzaj ochrony ☑ System kontroli dostępu ☑ Centralny zamek z Kluczowe regulacje
Czy upoważnienia dostępu do tych stref bezpieczeństwa są uregulowane i udokumentowane w koncepcji upoważnienia dostępu?	☑	☐	Przydzielanie kluczy i zarządzanie kluczami odbywa się zgodnie ze zdefiniowanym procesem, który reguluje nadawanie i odbieranie upoważnień dostępu do pomieszczeń zarówno na początku stosunku pracy, jak i po jego zakończeniu.
Czy w tych pomieszczeniach obowiązują inne środki ochrony?	☑	☐	☑ Porter ☑ System alarmowy ☑ Karta firmowa

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
2.1.2 Dostęp do systemów przetwarzania danych			
Czy istnieją środki kontroli dostępu do - pulpitu i systemów sieciowych?	☑	☐	Bezpieczny identyfikator użytkownika ☑ Bezpieczne hasło Powtórzenie☑ blokady hasła po 3 nieudanych próbach Aby uzyskać dostęp do systemów informatycznych, użytkownicy muszą posiadać odpowiednie uprawnienia dostępu. W tym celu administratorzy wydają odpowiednie upoważnienia dla użytkowników. Odbywa się to jednak tylko na życzenie odpowiedniego przełożonego. Wniosek można również złożyć za pośrednictwem działu kadr.
Czy istnieją zasady dotyczące haseł dla wszystkich poziomów dostępu (sieć, serwer, aplikacje), aby zapewnić bezpieczne i poufne hasła?	☑	☐	Użytkownik otrzymuje nazwę użytkownika i hasło początkowe, które musi zostać zmienione przy pierwszym logowaniu. Specyfikacja hasła obejmuje minimalną długość hasła wynoszącą 8 znaków, przy czym hasło musi spełniać wymagania dotyczące złożoności.
Czy zgodność z tymi zasadami jest sprawdzana automatycznie na wszystkich poziomach podczas wprowadzania danych?	☑	☐	Hasła są regularnie zmieniane. Zostanie - zasygnalizowana automatyczna zmiana hasła. Zapisywana jest historia haseł. Dzięki temu 10 poprzednich haseł nie będzie mogło być ponownie użyte. Hasła są zawsze przechowywane w postaci zaszyfrowanej.
Czy jest ustawiony czasowo kontrolowany, chroniony hasłem obwód pauzy (wygaszacz ekranu)?	☑	☐	

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
Czy systemy są zabezpieczone przed nieuprawnionym włamaniem i przed dostępem do Internetu?	☑	☐	☑ Firewall ☑ Skaner antywirusowy ☑ Rozdzielenie sieci zasilających Wszystkie systemy serwerowe i klienckie są - wyposażone w oprogramowanie antywirusowe, które gwarantuje codzienną aktualizację sygnatur. Wszystkie serwery są chronione przez zapory ogniowe, które są zawsze utrzymywane i dostarczane z aktualizacjami i łatami. Dostęp serwerów i klientów do Internetu oraz dostęp do tych systemów przez Internet jest również zabezpieczony przez zapory sieciowe. W ten sposób można wykorzystać tylko te porty, które są wymagane do danej komunikacji. Wszystkie inne porty są odpowiednio blokowane.
Czy wprowadzono środki rejestrowania/monitorowania, jeśli tak, to jakie?	☑	☐	☑ Konfigurowanie użytkowników i uprawnień ☑ Zmiany w systemie ☑ Błędne próby dostępu ☑ Monitorowanie systemu ☑ Logowanie i wylogowywanie się do procedur przetwarzania danych
Czy dane dziennika są przechowywane w sposób odporny na audyt i zabezpieczony przed dostępem?	☑	☐	
Czy dane dziennika są sprawdzane szybko i regularnie pod kątem działań i procesów istotnych z punktu widzenia bezpieczeństwa?	☑	☐	☑ Ręczne i okolicznościowe
Czy dostęp do systemów przetwarzania danych jest ograniczony przez system uprawnień do wymaganej grupy użytkowników?	☑	☐	☐ Profile praw i zarządzanie prawami ☐ Ograniczenia funkcjonalne terminali Uprawnienia do systemów informatycznych i aplikacji są nadawane wyłącznie przez administratorów.
Czy dostęp z instytucji zewnętrznych jest zabezpieczony, jeśli tak, to w jaki sposób?	☑	☐	☑ Połączenie VPN ☑ Szyfrowanie ☑ Specjalne oprogramowanie do zdalnej konserwacji/zdalnego wsparcia

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
2.1.3 Ochrona danych przed nieuprawnionym dostępem			
Czy istnieje udokumentowany profil autoryzacji, który zapewnia, że każdy pracownik ma tylko te uprawnienia dostępu, które są mu potrzebne do wykonania swoich zadań?	☑	☐	W jakiej formie? Jeśli to konieczne, również zróżnicowane według: ☑ Odczytać upoważnienie ☑ Napisz pozwolenie Upoważnienia są zawsze udzielane zgodnie z zasadą ograniczonego dostępu. W związku z tym prawa dostępu do danych, baz danych lub aplikacji otrzymują tylko te osoby, które - utrzymują i obsługują te dane, aplikacje lub bazy danych lub są zaangażowane w ich rozwój. Istnieje koncepcja autoryzacji opartej na rolach z możliwością zróżnicowanego przydzielania uprawnień dostępu, co zapewnia, że pracownicy otrzymują prawa dostępu do aplikacji i danych w zależności od zakresu odpowiedzialności, a w razie potrzeby na podstawie projektu.
Czy wprowadzono środki ograniczające przechowywanie, w szczególności pseudonimizację lub anonimizację?	☑	☐	
Czy zdefiniowane uprawnienia i ich zmiany są udokumentowane w zrozumiały sposób?	☑	☐	
Czy ustanowiono system zarządzania uprawnieniami w celu udokumentowanego przydzielania uprawnień, który zapewnia również, że uprawnienia, które nie są już potrzebne, są niezwłocznie anulowane w przypadku zmiany obszaru odpowiedzialności?	☑	☐	Warunkiem wstępnym jest odpowiedni wniosek o udzielenie upoważnienia dla pracownika przez przełożonego. Utworzony został odpowiedni proces wymeldowania.
Czy istnieją inne środki kontroli dostępu, jeśli mają zastosowanie?	☑	☐	☑ Proces przeglądu i zatwierdzania programu ☑ Rejestrowanie i ocena zdarzeń o istotnym znaczeniu dla bezpieczeństwa

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
2.2 Integralność (Art. 32 ust. 1 lit. b GDPR)			
2.2.1 Ochrona danych podczas przesyłania i przekazywania			
Czy dane są chronione przed nieuprawnionym dostępem podczas transmisji?	☑	☐	☑ Szyfrowanie ☑ Bezpieczne połączenia, VPN
Czy zagwarantowane jest bezpieczne usuwanie, niszczenie i utylizacja nośników danych?	☑	☐	Wszyscy pracownicy są poinstruowani, aby umieszczać informacje zawierające dane osobowe i/lub informacje o projektach w wyznaczonych pojemnikach na zniszczenie.
Czy usuwanie/niszczenie nośników danych zleca się firmie usługowej?	☑	☐	Niszczenie nośników danych i papieru jest przeprowadzane przez usługodawcę, który gwarantuje niszczenie zgodnie z normą DIN 66399.
Czy istnieje umowa/zlecenie zgodnie z wymogami art. 28 GDPR?	☑	☐	
Czy uregulowana jest bezpieczna i poufna likwidacja urządzeń z nośnikami danych (np. serwerów, urządzeń wielofunkcyjnych itp.)?	☑	☐	
Czy w przypadku zdalnej konserwacji dostęp do danych i systemów klienta odbywa się wyłącznie za pośrednictwem bezpiecznych łączy?	☑	☐	Zabezpieczanie linii: ☑☑ Szyfrowanie VPN Zdalny dostęp do systemów informatycznych odbywa się zawsze poprzez szyfrowane połączenia.
Czy zagwarantowano bezpieczną identyfikację/uwierzytelnianie w przypadku zdalnej konserwacji?	☑	☐	
Czy w przypadku zdalnej konserwacji linie są monitorowane przez odpowiednie urządzenia zabezpieczające, np. rejestrację i ocenę dzienników?	☑	☐	

Wniosek	Spełnia wymagania		Komentarz / Wyjaśnienie
	J	N	
2.2.2 Kontrola wprowadzania danych			
Czy procesy łączenia się z systemami klienta są rejestrowane i monitorowane w sposób możliwy do prześledzenia?	☑	☐	Wprowadzanie, modyfikacja i usuwanie danych osobowych przetwarzanych w imieniu klienta jest zawsze rejestrowane. Pracownicy są zobowiązani do pracy na własnych kontach przez cały czas. Konta użytkowników nie mogą być współdzielone lub wykorzystywane wspólnie z innymi osobami.
Czy korzystanie z systemów przetwarzania danych i wprowadzanie danych jest rejestrowane?	☑	☐	Rejestrowanie użycia plików: ☑ Tak☐ Nie Rejestrowanie wpisów i zmian: ☑ Dane związane z dziedziną ☑ Powiązane z zapisami
Czy ustawiono uprawnienia użytkowników o zróżnicowanych profilach uprawnień?	☑	☐	Prawa: ☑ Odczyt, zmiana, usuwanie ☑ Częściowy dostęp do danych i funkcji
Czy ustanowiono procedurę zrozumiałego przyznawania praw oraz zmiany lub anulowania praw?	☑	☐	Upoważnienia są zawsze udzielane zgodnie z zasadą ograniczonego dostępu. W związku z tym prawa dostępu do danych, baz danych lub aplikacji otrzymują tylko te osoby, które - utrzymują i obsługują te dane, aplikacje lub bazy danych lub są zaangażowane w ich rozwój. Warunkiem wstępnym jest odpowiedni wniosek o udzielenie upoważnienia dla pracownika przez przełożonego. Utworzono odpowiedni proces wymeldowania.
Czy przy przyznawaniu praw przestrzegana jest zasada minimum?	☑	☐	
Czy organy odpowiedzialne za przyznawanie/udzielanie zezwoleń i ustanawianie praw są odrębne?	☑	☐	

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
2.2.3 Kontrola operacji przetwarzania			
Czy realizacja zamówienia klienta/działania usługowego jest - monitorowana w sposób możliwy do prześledzenia, aby zapewnić realizację zgodnie z zamówieniem?	☑	☐	Odpowiednie regulacje znajdują się w umowie o zlecone przetwarzanie danych.
Czy istnieją odpowiednie mechanizmy logowania i oceny w celu monitorowania nieuprawnionego dostępu do systemów klienta i danych klienta?	☑	☐	Odpowiednie regulacje znajdują się w umowie o zlecone przetwarzanie danych.
Czy istnieją przepisy dotyczące postępowania w przypadku incydentów oraz wypełniania obowiązków sprawozdawczych wobec klienta?	☑	☐	Odpowiednie regulacje znajdują się w umowie o zlecone przetwarzanie danych.
Czy przy udzielaniu zamówień na usługi (np. usługi IT, konserwacja itp.) przestrzegane są wymogi art. 28 GDPR?	☑	☐	☑ Wybór wykonawcy ☑ Przegląd środków technicznych i organizacyjnych stosowanych przez wykonawcę ☑ Zawarcie umowy zgodnie z art. 28 GDPR ☑ Regularny przegląd wykonawcy
Czy czynności konserwacyjne w zleconych systemach przetwarzania są rzetelnie monitorowane i rejestrowane?	☑	☐	

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
2.3 Dostępność i niezawodność systemów (art. 32 ust. 1 lit. b) GDPR)			
2.3.1 Zapewnienie dostępności danych			
Czy dane klientów są chronione przed zniszczeniem i utratą dzięki odpowiednim procedurom tworzenia kopii zapasowych?	☑	☐	☑ Magazyn danych lustrzanych ☑ Regularne tworzenie kopii zapasowych/rozwiązanie do tworzenia kopii zapasowych Czy istnieje koncepcja backupu, która określa sposób wykonywania regularnego backupu i odtwarzania danych? ☑ Tak☐ Nie
Czy podjęto środki zabezpieczające serwerownię i infrastrukturę IT?	☑	☐	Dane klientów są przechowywane w centrum danych certyfikowanym zgodnie z normą DIN EN/ISO IEC 2700x.

Wniosek	Spełnia wymagania		Komentarz / Wyjaśnienie
	J	N	
2.3.2 Rozdzielenie różnych klientów			
Czy dane różnych klientów są odpowiednio oddzielone od siebie, aby zapewnić ich oddzielne przetwarzanie?	☑	☐	Rodzaj separacji: ☑ Oddzielenie klienta

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
2.4 Procedury regularnego przeglądu, oceny i ewaluacji			
Czy funkcjonuje system zarządzania bezpieczeństwem IT?	☑	☐	Dane klientów są przechowywane w centrum danych certyfikowanym zgodnie z normą DIN EN/ISO IEC 2700x.
Czy skuteczność środków technicznych i organizacyjnych w przedsiębiorstwie jest regularnie sprawdzana również w inny sposób?	☑	☐	Wdrożone jest zarządzanie ochroną danych. Istnieje wytyczna w sprawie ochrony i bezpieczeństwa danych oraz wytyczne zapewniające realizację celów tej wytycznej. Zespół ds. ochrony danych i bezpieczeństwa informacji (DST) został powołany w celu planowania, wdrażania, oceny i dostosowywania środków ochrony danych i bezpieczeństwa danych. Wytyczne są regularnie oceniane i dostosowywane pod kątem ich skuteczności. W szczególności zapewnia się, że incydenty związane z ochroną danych są rozpoznawane przez wszystkich pracowników i niezwłocznie zgłaszane do DST. DST niezwłocznie przeprowadzi dochodzenie w sprawie tego zdarzenia. Jeżeli dotyczy to danych przetwarzanych w imieniu klientów, należy zadbać o to, aby zostali oni niezwłocznie poinformowani o charakterze i zakresie incydentu. W przypadku przetwarzania danych na potrzeby własne, jeśli spełnione są wymogi art. 33 GDPR, powiadomienie organu nadzorczego nastąpi w ciągu 72 godzin od momentu powzięcia informacji o incydencie.

Wniosek	**Spełnia wymagania**		**Komentarz / Wyjaśnienie**
	J	N	
2.5 Procedury regularnego przeglądu, oceny i ewaluacji			
Czy przestrzegane są wymogi "ochrony danych za pomocą technologii" i "-ustawień domyślnych sprzyjających ochronie danych"? ("Prywatność w fazie projektowania" i "Prywatność domyślna")	☑	☐	Już podczas tworzenia oprogramowania zwraca się uwagę na to, aby przy interfejsach użytkownika uwzględniana była zasada konieczności. Na przykład, pola formularzy i maski ekranów mogą być zaprojektowane w sposób elastyczny. Można podać pola obowiązkowe lub je dezaktywować. Oprogramowanie wspiera zarówno kontrolę danych wejściowych poprzez elastyczną i konfigurowalną ścieżkę audytu, która zapewnia niezmienny zapis zmian w danych i uprawnieniach użytkowników. Uprawnienia do danych lub aplikacji mogą być ustawiane elastycznie i granularnie.

Arnsberg | 20.10.2021

Miejsce | Data

Podpis

Thorsten Schröers
Datenschutzbeauftragter