

**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań  
w celu zapewniania przestrzegania przepisów o ochronie danych osobowych.**

Lp.	Zgłoszona uwaga do paragrafu rozporządzenia	Zgłaszający	Stanowisko
<b>§ 2.</b>			
<b>Ad. § 2 pkt 3</b>			
1.	W par. 2 pkt 3 – nie jest do końca jasne, kto komu zleca czynności sprawdzenia: ABI GIODO czy GIODO ABI? Po słowie „zwrócenia się” dodać sformułowanie „do ABI”.	<b>SABI</b>	
<b>§ 3.</b>			
<b>Ad. § 3. ust. 2 pkt. 1 i 2</b>			
2.	W § 3 ust. 2 pkt 1 i 2 należy dokonać korekty redakcyjnej:  W § 3 ust. 2 pkt 1 zamienić treść na: <i>"1) sprawdzenia planowego - według planu sprawdzeń, o którym mowa w ust. 3, przygotowanego przez administratora bezpieczeństwa informacji;"</i>  W § 3 ust. 2 pkt 2 po słowach: <i>"przez administratora bezpieczeństwa informacji"</i> dodać słowo: <i>"informacji"</i> .	<b>SABI</b>	
<b>Ad. § 3. ust. 4</b>			
3.	Przepis w obecnym brzmieniu powoduje, że każde sprawdzenie musi obejmować <u>w szczególności</u> całą inwentaryzację przetwarzanych zbiorów oraz całościowe sprawdzenie realizacji wszystkich obowiązków ustawowych, co w przypadku dużych organizacji jest długotrwałe. Proponujemy przereformowanie zapisów w taki sposób, aby ABI mający niezależność w wykonywaniu sprawdzenia ustalał jego zakres w zależności od potrzeb w odniesieniu do weryfikacji poszczególnych obowiązków ustawowych. Proponujemy następujące brzmienie pierwszego zdania w ust. 4:	<b>SABI</b>	

**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań  
w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych.**

	<p>„Administrator bezpieczeństwa informacji w planie sprawdzeń ustala ich zakres, w zależności od potrzeb, w odniesieniu do konieczności inwentaryzacji zbiorów danych osobowych przetwarzanych przez administratora danych oraz weryfikacji zgodności przetwarzania danych osobowych, w tym:.....</p> <p>Natomiast należy też wziąć pod uwagę, że delegacja do rozporządzenia w art. 36a ust. 9 pkt 1 odnosi się do trybu i sposobu realizacji zadań wynikających z art. 36a ust. 2 pkt. 1 lit. a i b. Natomiast nie odnosi się do zakresu zadań jakie ma obowiązek wykonywać ABI, dlatego podawanie co ma w szczególności uwzględnić w sprawdzeniu ABI jest niezgodne z delegacją ustawową. Pojawia się zatem pytanie: czy takie zapisy w par. 3 ust. 4 są zgodnie z delegacją ustawową?</p>		
<b>Ad. § 3 ust. 7</b>			
4.	<p>Przy sprawdzeniu dokonywanym przez ABI dla GIODO nie ma zapisów dotyczących trybu powiadamiania ADO przez ABI. Przy sprawdzeniu planowym i pozaplanowym wymóg takiego powiadomienia jest zapisany w par. 3 ust 7.</p> <p>Proponujemy uzupełnienie w tym zakresie ust. 7:</p> <p>„Administrator danych przyjmuje od administratora bezpieczeństwa informacji do wiadomości:</p> <ol style="list-style-type: none"> <li>1. plan sprawdzeń,</li> <li>2. zawiadomienie o sprawdzeniu pozaplanowym,</li> <li>3. zawiadomienie o otrzymaniu wystąpienia GIODO o dokonanie sprawdzenia, o którym mowa w art. 19b ust. 1 ustawy.”</li> </ol>	<b>SABI</b>	

**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań  
w celu zapewniania przestrzegania przepisów o ochronie danych osobowych.**

<b>§ 4.</b>		
<b>Ad. § 4. ust. 2</b>		
5.	<p>W przypadku sprawdzenia planowego sporządzenie programu będzie powielać przygotowany plan sprawdzeń. Zapisy dotyczące zakresu czynności oraz sposób i zakres ich dokumentowania mogą być zawarte w planie sprawdzeń.</p> <p>Proponujemy wykreślenie pkt 2 lub rozważenie pozostawienia zapisu o wymogu przygotowywania programu jedynie dla sprawdzenia pozaplanowego.</p>	<b>SABI</b>
<b>Ad. § 4. ust. 3</b>		
6.	<p>W par. 4 ust. 3 pkt 3 jest mowa o dokumentach dotyczących przetwarzania danych. Natomiast nie zawsze będą to dokumenty papierowe. Mogą być to również zapisy elektroniczne lub np. nagrania rozmów telefonicznych.</p> <p>Proponujemy zmianę zapisów w pkt 3 na:</p> <p><i>„Wgląd do dokumentów i danych mających związek z przedmiotem sprawdzenia i przeprowadzenie ich analizy„</i></p>	<b>SABI</b>
<b>Ad. § 4. ust. 6</b>		
7.	<p>W par. 4 ust. 6 wprowadzono obowiązek asysty osób upoważnionych do przetwarzania danych, w tym w szczególności administratora systemu. Wyklucza to wykonywanie tych czynności przez ABI samodzielnie. Natomiast w praktyce ABI ma dostęp do systemu informatycznego, i jako uprawniony i upoważniony użytkownik może wykonywać takie czynności w zakresie swoich uprawnień dostępowych. Jeśli natomiast dostęp ten przekracza uprawnienia ABI i będzie on potrzebował pomocy ze strony innych osób, to i tak się do nich zwróci.</p> <p>Rozumiemy, że intencją tego zapisu jest ryzyko żądania przez ABI nadania mu szczególnych uprawnień</p>	<b>SABI</b>

**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań  
w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych.**

	<p>dostępowych do system w ramach przeprowadzenia sprawdzenia (np. uprawnień administratora systemu). W praktyce wykonywania zadań ABI nie spotyka się takich sytuacji. Dlatego proponujemy usunięcie zapisu lub jego przerehabilitowanie:</p> <p><i>“W systemie informatycznym służącym do przetwarzania danych osobowych czynności, o których mowa w ust. 3, wykonywane są przez administratora bezpieczeństwa informacji w zakresie przyznanych mu uprawnień dostępowych lub przy udziale osób upoważnionych do przetwarzania danych, w szczególności administratora systemu.”</i></p>		
<b>Ad. § 4. ust. 7</b>			
8.	<p>W par. 4 ust 7 mamy wątpliwość czy zastosowanie słowa "albo" jest tu właściwe. Dokumenty, o których mowa w ust. 4 mogą być zarówno elektroniczne, jak i papierowe. Proponujemy zmianę zapisów na:</p> <p><i>“Dokumenty, o których mowa w ust. 4, mogą być sporządzane w postaci papierowej lub elektronicznej”.</i></p>	<b>SABI</b>	
<b>Ad. § 4. ust. 8</b>			
9.	<p>Nie można zabronić ABI aby zwracał się o opinie prawne lub techniczne i organizacyjne do specjalistów posiadających wiedzę dotycząca przepisów o ochronie danych osobowych. Jest to zbyt daleko idące ograniczanie swobody działalności gospodarczej; jest to wewnętrzna sprawa organizacji i nie powinno się tego regulować. Wymóg posiadania odpowiedniej wiedzy przez ABI, który wynika obecnie z przepisów ustawy nie oznacza, że ABI musi posiadać wiedzę interdyscyplinarną z dziedziny prawa, zarządzania czy technologii informatycznych i nie znaczy, że nie może zasięgać opinii ekspertów. Nie można zatem ograniczać jego prawa do konsultacji z fachowcami w zakresie ochrony danych, dotyczących skomplikowanych i zawitych stanów faktycznych przetwarzania danych osobowych. Orzecznictwo GIODO i WSA pokazują jak trudne i długie jest nieraz rozwikłanie takich stanów faktycznych w zgodzie z obowiązującymi przepisami o ochronie danych osobowych. Przepis ten, w proponowanym brzmieniu, odbiera ABI możliwość wnioskowania do ADO o wydanie opinii</p>	<b>SABI</b>	

**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań  
w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych.**

	<p>dotyczącej złożonych stanów faktycznych przetwarzania danych osobowych. ABI powinien posiadać taką możliwość. Po za tym w organizacjach działają różnego rodzaju specjaliści (np. radca prawny, księgowy, kadrowiec), którzy powinni również posiadać należytą wiedzę na temat swojego zakresu obowiązków, a mimo to nie ma przepisu, który zabraniałby im korzystać ze wsparcia zewnętrznych konsultantów. Wprowadzenia takiego ograniczenia w stosunku do ABI jest bezpodstawne.</p> <p>Pojawia się również wątpliwość czy zapis ten nie przekracza delegacji ustawowej do tego rozporządzenia.</p> <p><b><u>Należy zatem usunąć w całości ust. 8 .</u></b></p>		
<b>§ 5.</b>			
<b><u>Ad. § 5. ust. 2 i 3</u></b>			
10.	<p>Pojawiają się wątpliwości czy zapis ten nie jest zbędnym formalizmem oraz czy nie niesie za sobą niepotrzebnego wydłużenia czasu sprawdzenia. W wielu przypadkach sprawdzenie będzie dotyczyło różnych procesów przetwarzania danych osobowych, w które zaangażowane są różne osoby z wielu komórek organizacyjnych ADO. W toku sprawdzenia może pojawić się konieczność objęcia nim również innych osób, których wcześniej nie przewidziano. Przy takim zapisie każda osoba niepowiadomiona ma prawo odmówić poddania się czynnościom sprawdzającym (bo niebyła zawiadomiona w terminie), co uniemożliwi realizację sprawdzenia przez ABI, a przynajmniej znacznie ją opóźni. W szczególności gdy ABI będzie przeprowadzać sprawdzenie w terenie (co wiąże się z dodatkowymi kosztami).</p> <p>Proponujemy zatem usunięcie par. 5 ust. 2 i 3.</p>	<b>SABI</b>	
<b>§ 6.</b>			
<b><u>Ad. § 6. ust. 2</u></b>			
11.	<p>W organizacjach pozarządowych stosowanie tego typu rozwiązań jest śladowe i wymóg ten uniemożliwiłby</p>	<b>SABI</b>	

**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych.**

	<p>większości przedsiębiorcom sporządzanie elektronicznych sprawozdań do własnych organizacyjnych potrzeb, gdzie istnieją wdrożone elektroniczne systemy obiegu dokumentów, a wszystkie dokumenty są przechowywane i udostępniane do wglądu jedynie w formie elektronicznej (bez konieczności stosowania kwalifikowanych certyfikatów).</p> <p>Proponujemy rozważenie pozostawienia konieczności podpisywania sprawozdania kwalifikowanym certyfikatem lub podpisem potwierdzonym profilem zaufanym jedynie w przypadku sprawozdania dla Generalnego Inspektora.</p>		
<b>§ 8.</b>			
<b>Ad. § 8 pkt 4</b>			
12.	<p>Zapis o spełnieniu wymogu "<i>weryfikacji skuteczności zabezpieczeń</i>" oznacza konieczność przeprowadzenia przez ABI m. in. testów bezpieczeństwa systemu np. testów penetracyjnych związanych z ryzykiem nieautoryzowanego dostępu do danych. Nie wydaje się, żeby to było zadanie dla ABI. ABI, na podstawie posiadanej wiedzy powinien ocenić, czy zastosowane środki zabezpieczeń są adekwatne do ryzyk.</p> <p>Proponujemy zmianę zapisu w pkt. 4:  <i>§ 8. Nadzór, o którym mowa w § 1 pkt 2, polega na weryfikacji:</i>          (...)          4) <del>skuteczności</del> <b>adekwatności</b> przewidzianych w dokumentacji przetwarzania danych, środków technicznych i organizacyjnych <del>zabezpieczenia rozwiązań dla</del> <u>służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;</u></p>	<b>SABI</b>	
<b>Ad. § 8 pkt 5</b>			
13.	<p>W par. 8 pkt 5 – przed słowem „<i>obowiązków</i>” dodać „<i>zasad i</i>” – ponieważ ABI ma nadzorować zgodnie z art. 36a ust. 2 pkt. 1 lit b przestrzeganie zasad określonych w dokumentacji przetwarzania danych.</p>	<b>SABI</b>	

**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań  
w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych.**

§ 10.		
<u>Ad. § 10 ust. 1</u>		
14.	<p>W zapisach ust. 1 pkt 1 i 2 pojawia się wymóg przedstawienia ADO przez ABI do wdrożenia dokumentów aktualizacyjnych. Zapis ten jest sprzeczny z zadaniami ABI określonymi w art. 36a ust. 2 pkt 1 lit. b - nie ma tam mowy, że ABI ma obowiązek opracowywać dokumentację dotyczącą ochrony danych. Natomiast ADO może mu to zlecić jako dodatkowe zadanie zgodnie z art. 36a ust. 4.</p> <p>Dlatego w pkt 1 i 2 ust. 10 należy zmienić zapisy:</p> <p><i>W przypadku wykrycia podczas weryfikacji nieprawidłowości administrator bezpieczeństwa informacji:</i></p> <p>1) zawiadamia administratora danych o nieopracowaniu lub brakach w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności <b>może przedstawić</b> mu do wdrożenia dokumenty usuwające stan niezgodności;</p> <p>2) zawiadamia administratora danych o nieaktualności dokumentacji przetwarzania danych oraz <b>może przedstawić</b> administratorowi danych do wdrożenia dokumenty aktualizujące;</p>	<b>SABI</b>
15.	W par. 10 ust. 1 pkt 3 – po słowach „zasad” dodać „i obowiązków”.	<b>SABI</b>
§ 11.		
16.	<p>Proponujemy wykreślenie zapisu: „a w przypadku administratora bezpieczeństwa informacji, o którym mowa w art. 35 ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. poz. 1662) – w terminie do dnia 30 kwietnia 2015 r.”.</p> <p>Zmiana ustawy miała w swych założeniach wprowadzić okres przejściowy, w którym ADO miałyby czas na podjęcie decyzji czy powołać ABI na nowych zasadach i zarejestrować go w GIODO do 30 czerwca 2015 r. Niefortunnie zapis</p>	<b>SABI</b>

**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań  
w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych.**

	<p>przejściowy w ustawie deregulacyjnej (art. 35) wprowadził obowiązek wykonywania wszystkich nowych zadań już od 1 stycznia przez dotychczasowych ABI, bez względu czy spełniają oni kryteria dla nowego ABI oraz czy będą oni powołani wg nowych przepisów. Aby nie wprowadzać zbędnego zamieszania organizacyjnego u ADO, którzy będą podejmować decyzję organizacyjne o tym czy powołać ABI na nowych zasadach lub nie, proponujemy rozważenie zrezygnowania z przepisu przejściowego dotyczącego podania terminu dla przedstawienia planu sprawdzeń przez dotychczasowych ABI. Jeżeli nie zostaną oni wyznaczeni do 30 czerwca, to i tak nie będą musieli wykonywać sprawdzeń zgodnie z wytycznymi tego rozporządzenia, a jeżeli zostaną powołani 30 czerwca, to przedstawią plan do 30 lipca. Sytuacja ta nie będzie wpływać na wykonywanie bieżącego nadzoru nad przetwarzaniem danych.</p>		
<b>§ 13.</b>			
17.	W par. 13 zamienić zapis: "oraz nadzór na dokumentacją" na: "oraz nadzór <b>nad</b> dokumentacją".	<b>SABI</b>	
<b>§ 15.</b>			
18.	<p>Wyłączenie odpowiedniego stosowania przepisów rozporządzenia do ADO, o którym mowa w art. 36b powinno obejmować:</p> <ol style="list-style-type: none"> <li>1) sprawdzenie, o którym mowa w par. 3 ust. 1 pkt 2 rozporządzenia, oraz</li> <li>2) sprawozdanie, o którym mowa w par. 6 ust. 3 pkt 3 rozporządzenia.</li> </ol> <p>Brak takiego wyłączenia oznaczałby, że ten ADO ma dokonywać sprawdzenia samego siebie na zlecenie GIODO. Nie ma takiego rodzaju sprawdzenia w ustawie i nie można go wprowadzać w drodze rozporządzenia. Sprawdzenie, o którego dokonanie zwrócił się GIODO na podstawie art. 19b ust. 1 ustawy, może przeprowadzić tylko ABI. GIODO może mu powierzyć wykonanie takiego zadania "ze względu na niezależną kompetencję kontrolną" jaką posiada ABI. Taką intencję ustawodawcy znajdujemy na str. 18 uzasadnienia rządowego projektu ustawy o ułatwieniu wykonywania działalności gospodarczej.</p>	<b>SABI</b>	



**TABELA UWAG Stowarzyszenia ABI do projektu rozporządzenia MAiC w sprawie trybu i sposobu realizacji zadań  
w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych.**

<p>Proponujemy nowe brzmienie: § 15. Do administratora danych, o którym mowa w art. 36b ustawy, stosuje się odpowiednio przepisy rozporządzenia, z wyłączeniem obowiązków:</p> <ol style="list-style-type: none"><li><b><u>1.</u> dokonania sprawdzenia dla GIODO w przypadku, o którym mowa w § 3 ust. 1 pkt 2,</b></li><li><b><u>2.</u> sporządzenia sprawozdania, o którym mowa w § 6,</b></li><li><b><u>3.</u> zawiadomień, o których mowa w § 10 ust. 1.</b></li></ol> <p>Administrator danych nie będący osobą fizyczną wskazuje osoby wykonujące czynności lub opracowujące dokumenty określone w rozporządzeniu.</p>		
--	--	--