



PKP POLSKIE LINIE KOLEJOWE S.A.

System Zarządzania Bezpieczeństwem Informacji w PKP Polskie Linie Kolejowe S.A.		<i>Data wdrożenia SZBI:</i> 2013-01-02
Wyciąg z Polityki Bezpieczeństwa Danych Osobowych w PKP Polskie Linie Kolejowe S.A.	Załącznik Nr 18 do SZBI-lbi-3	<i>Data wdrożenia:</i> 2010-08-16
	<i>Numer wersji:</i> 26	<i>Data obowiązywania wersji:</i> 2023-07-07

**Procedura weryfikacji podmiotu przetwarzającego
dane osobowe w PKP Polskie Linie Kolejowe S.A.**

Właściciel: PKP Polskie Linie Kolejowe S.A.

Wydawca: PKP Polskie Linie Kolejowe S.A. Centrala
Biuro Bezpieczeństwa Informacji i Spraw Obronnych
ul. Targowa 74, 03-734 Warszawa
tel. 22 47 324 00
www.plk-sa.pl, e-mail: ioi@plk-sa.pl

Wszelkie prawa zastrzeżone.
Modyfikacja, wprowadzanie do obrotu, publikacja, kopiowanie
i dystrybucja w celach komercyjnych, całości lub części dokumentu,
bez uprzedniej zgody PKP Polskie Linie Kolejowe S.A. – są
zabronione

§ 1.

Zakres stosowania

Niniejszy dokument obowiązuje we wszystkich jednostkach organizacyjnych i komórkach Centrali Spółki, które zamierzają powierzyć przetwarzanie danych osobowych ze zbiorów prowadzonych przez Spółkę podmiotom zewnętrznym (podmiotom przetwarzającym) na podstawie umowy powierzenia przetwarzania danych osobowych, zwanej dalej: „*Umową*”.

§ 2.

Cel

Celem dokumentu „*Procedura weryfikacji podmiotu przetwarzającego dane osobowe*”, zwana dalej: „*Procedurą*”, jest weryfikacja podmiotu przetwarzającego, któremu Spółka zamierza powierzyć przetwarzanie danych osobowych w określonym celu i zakresie przetwarzania.

§ 3.

Role i odpowiedzialności

1. Inspektor Ochrony Danych odpowiada za:
 - 1) nadzór oraz koordynację działań w zakresie realizacji niniejszej Procedury;
 - 2) analizę wyników przeprowadzonej weryfikacji podmiotu przetwarzającego;
 - 3) ostateczne zatwierdzenie wyniku przeprowadzonej weryfikacji podmiotu przetwarzającego.
2. Pracownik koordynujący proces zawierania Umowy odpowiada za:
 - 1) przedłożenie do wypełnienia podmiotowi zewnętrznemu (podmiotowi przetwarzającemu) „*Ankiety oceny podmiotu przetwarzającego dane osobowe*” stanowiącej Załącznik Nr 1 do niniejszej Procedury;
 - 2) zapewnienie sprawnej współpracy z osobą wyznaczoną do weryfikacji podmiotu przetwarzającego ze strony IOD w tym zakresie.
3. Osoba wyznaczona do weryfikacji podmiotu przetwarzającego ze strony IOD odpowiada za:
 - 1) bieżące monitorowanie stanu weryfikacji podmiotu przetwarzającego i wsparcie pracownika koordynującego proces zawierania Umowy w tym zakresie;

- 2) przeprowadzenie oceny podmiotu przetwarzającego oraz jego podsumowanie dla IOD.
4. Wymóg sprawnej realizacji Procedury dotyczy wszystkich osób wskazanych w ust. 1-3.

§ 4.

Metodyka weryfikacji podmiotu przetwarzającego

1. Zgodnie z art. 28 ust. 1 RODO Spółka może korzystać wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.
2. W Spółce przyjmuje się metodykę weryfikacji podmiotu przetwarzającego, która realizowana jest zgodnie z poniższym schematem działania:
 - 1) **Etap I** – Przesłanie podmiotowi przetwarzającemu przed zawarciem Umowy do wypełnienia „*Ankiety oceny podmiotu przetwarzającego dane osobowe*”, weryfikującej podmiot przetwarzający pod względem wiedzy fachowej, wiarygodności oraz posiadania adekwatnych zasobów służących bezpieczeństwu przetwarzania danych.
 - 2) **Etap II** – Weryfikacja podmiotu przetwarzającego na podstawie udzielonych przez podmiot przetwarzający odpowiedzi w „*Ankiecie oceny podmiotu przetwarzającego dane osobowe*”, przeprowadzana jest za pomocą „*Karty weryfikacji podmiotu przetwarzającego dane osobowe*”, zgodnie z poniższymi zasadami:
 - a) wpływ udzielonych odpowiedzi na wynik weryfikacji podmiotu przetwarzającego pod względem oceny poszczególnych środków zapewniających bezpieczeństwo przetwarzania danych osobowych według ustalonych wymagań należy określić jako: Zgodność/Niezgodność;
 - b) spełnienie przyjętych wymagań na poziomie powyżej 75% - podmiot daje gwarancje wdrożenia odpowiednich środków zapewniających spełnienie wymogów RODO i bezpieczeństwa praw, osób, których dane dotyczą;
 - c) spełnienie przyjętych wymagań na poziomie poniżej 75% - podmiot przetwarzający nie daje wystarczającej gwarancji stosowania środków

zapewniających spełnienie wymogów RODO i bezpieczeństwo praw, osób, których dane dotyczą.

- 3) **Etap III** – Podsumowanie weryfikacji podmiotu przetwarzającego pod względem zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.

§ 5.

Postępowanie z podmiotem przetwarzającym

1. W przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, Pracownik koordynujący proces zawierania Umowy we współpracy z osobą wyznaczoną do weryfikacji podmiotu przetwarzającego po stronie IOD, przed zawarciem Umowy, przekazuje do wypełnienia podmiotowi przetwarzającemu „*Ankieta oceny podmiotu przetwarzającego dane osobowe*”.
2. Podmiot przetwarzający jest zobowiązany wypełnić „*Ankieta oceny podmiotu przetwarzającego dane osobowe*” oraz odesłać jej podpisaną treść do Pracownika koordynującego proces zawierania Umowy.
3. Pracownik koordynujący proces zawierania Umowy przekazuje wypełnioną przez podmiot przetwarzający „*Ankieta oceny podmiotu przetwarzającego dane osobowe*”, osobie wyznaczonej do weryfikacji podmiotu przetwarzającego ze strony IOD.
4. Osoba wyznaczona do weryfikacji podmiotu przetwarzającego ze strony IOD, dokonuje oceny udzielonych przez podmiot przetwarzający odpowiedzi w „*Ankiecie oceny podmiotu przetwarzającego dane osobowe*”, poprzez adnotację poziomu zgodności w „*Karcie weryfikacji podmiotu przetwarzającego dane osobowe*”, stwierdzającej czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą, czy też nie.
5. IOD po zakończeniu działań przez osobę wyznaczoną do weryfikacji podmiotu przetwarzającego ze strony IOD analizuje wynik przeprowadzonej weryfikacji podmiotu przetwarzającego oraz dokonuje jego zatwierdzenia (*lub nie*).
6. Osoba wyznaczona do weryfikacji podmiotu przetwarzającego ze strony IOD dokumentuje w BPM przeprowadzenie weryfikacji podmiotu przetwarzającego.

§ 6.

Załączniki

1. Ankieta oceny podmiotu przetwarzającego dane osobowe.
2. Karta weryfikacji podmiotu przetwarzającego dane osobowe.