KNORR-BREMSE

POLITYKA

BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W KNORR BREMSE SYSTEMY POJAZDÓW SZYNOWYCH SP. Z O.O.

Autor	Ilość stron	Data wprowadzenia
adw. Jan Prasałek	16	2 lutego 2023 r.

Wersja	Zakres modyfikacji	Autor modyfikacji	Data wprowadzenia
2.0.	Dodanie nowej lokalizacji w § 4 ust. 6	r.pr. Daniel Rybarczyk zatwierdzone przez IODa - Sylwię Kilińską-Łokieć	14.01.2025 r.

DO UŻYTKU WEWNĘTRZNEGO

§1 DEFINICJE

Na potrzeby niniejszego dokumentu, przez użyte określenia należy rozumieć:

1. „RODO" oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
2. „Polityka Bezpieczeństwa" oznacza niniejszą Politykę Bezpieczeństwa Przetwarzania Danych Osobowych;
3. „Organizacja" oznacza Knorr Bremse Systemy Pojazdów Szynowych Sp. z o.o. z siedzibą w Rzeszowie, ul. Innowacyjna 2, 30-396 Rzeszów, NIP 6762592516; KRS 0000883472,
4. „Inspektor Ochrony Danych" oznacza Inspektora Ochrony Danych (IOD) w rozumieniu art. 37 RODO, wyznaczonego przez Organizację i formalnie zgłoszonego Prezesowi Urzędu Ochrony Danych Osobowych;
5. „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio

zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

6. „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

7. „usuwanie danych" oznacza zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą;

8. „system informatyczny" oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

9. „administrator" oznacza administratora danych osobowych, to jest osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

10. „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

11. „odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców;

12. „strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

13. „zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

14. „naruszenie bezpieczeństwa danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

15. „szczególne kategorie danych osobowych" oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne lub biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;

16. „organ nadzorczy" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie Unii Europejskiej, w Polsce Prezesa Urzędu Ochrony Danych Osobowych;
17. „pracownik" oznacza każdą osobę upoważnioną przez Organizację do przetwarzania danych osobowych w imieniu Organizacji, niezależnie od formy zatrudnienia lub współpracy między pracownikiem a Organizacją.

§2 CEL POLITYKI

1. Celem Polityki Bezpieczeństwa Przetwarzania Danych Osobowych (zwanej dalej Polityką Bezpieczeństwa) w Organizacji jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe.
2. Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwanego dalej RODO. Polityka Bezpieczeństwa wdraża także obowiązki i wytyczne, wynikające z ustawodawstwa polskiego, w szczególności ustawy z 10 maja 2018 r. o ochronie danych osobowych.

§3 BEZPIECZEŃSTWO TELEINFORMATYCZNE

1. Środki techniczne i organizacyjne, zapewniające bezpieczeństwo danych osobowych w kontekście przetwarzania danych osobowych w systemach informatycznych określa Polityka Bezpieczeństwa Teleinformatycznego w Organizacji.
2. Polityka Bezpieczeństwa Teleinformatycznego określa w szczególności:
    a) zasady zabezpieczenia lokalizacji fizycznych, w których przetwarzane są dane osobowe;
    b) zasady bezpieczeństwa serwerów i stacji roboczych;
    c) procedury tworzenia kopii zapasowych i sposób ich przechowywania;
    d) obowiązki użytkownika systemu teleinformatycznego;
    e) zasady ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony danych.

§4 ZAKRES ZASTOSOWANIA POLITYKI BEZPIECZEŃSTWA

1. W Organizacji dane osobowe elektronicznej są przetwarzane i przechowane zarówno w postaci dokumentacji tradycyjnej jak i.
2. Zasady określone w Polityce Bezpieczeństwa stosuje się do:
    a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz systemów papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
    b) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

c) wszystkich pracowników w rozumieniu przepisów ustawy Kodeks Pracy, stażystów, współpracowników i innych osób mających dostęp do informacji podlegających ochronie w Organizacji.

3. Do przetwarzania danych osobowych w Organizacji dopuszczeni zostają wyłącznie pracownicy i współpracownicy, którym Organizacja udzieliła pisemnego upoważnienia do przetwarzania danych osobowych.
4. Obszarem przetwarzania danych osobowych w Organizacji są wydzielone pomieszczenia znajdujące się w lokalizacji rejestrowej Spółki oraz w lokalizacji: ul. Leona Henryka Sternbacha 1, 30-394 Kraków.

§5 PODSTAWOWE ZASADY PRZETWARZANIA DANYCH

1. Bezpieczeństwo danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.
2. Polityka Bezpieczeństwa zapewnia, że dane osobowe są przetwarzane przez Organizację zgodnie z zasadami:
    a) rozliczalności, rozumianej jako możliwość wykazania przez Organizację, że przetwarzanie danych następuje zgodnie z przepisami prawa;
    b) zgodności z prawem, rzetelności i przejrzystości dla osoby, której dane dotyczą;
    c) ograniczenia celu, rozumianego jako zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
    d) minimalizacji danych, rozumianej jako przetwarzanie wyłącznie takich danych, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
    e) prawidłowości, co oznacza, że przetwarzane dane są prawidłowe i w razie potrzeby uaktualniane, Organizacja podejmuje zaś wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
    f) ograniczenia przechowywania, co oznacza, że przetwarzane dane osobowe przechowywane są w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane
    g) integralności i poufności, co oznacza przetwarzanie danych osobowych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
3. Każdy pracownik i współpracownik Organizacji jest zobowiązany do zachowania zasad bezpiecznej pracy z danymi osobowymi i innymi danymi poufnymi, zgodnie z następującymi zasadami:
    a) zasada indywidualnych kont w systemie - każdy pracownik zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych mu indywidualnie kontach. Zabronione jest udostępnianie kont osobom trzecim;

b) zasada poufności haseł i kodów dostępu - każdy pracownik zobowiązany jest do zachowania poufności i nie przekazywania osobom nieuprawnionym udostępnionych haseł, w tym do systemów teleinformatycznych;
c) zasada zamkniętego pomieszczenia - niedopuszczalne jest pozostawianie niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu, jeśli nie pozostaje w nim inna osoba upoważniona do przetwarzania danych. Zasada nie dotyczy pomieszczeń ogólnie dostępnych. Po zakończeniu dnia pracy, ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna i drzwi oraz zgodnie z obowiązującymi ustaleniami, zabezpieczyć klucze do pomieszczenia. W przypadku pracy zdalnej zasada ta oznacza wyznaczenie stanowiska pracy umożliwiającego zachowanie przetwarzanych danych w poufności;
d) zasada nadzorowania dokumentów - po godzinach pracy wszystkie dokumenty zawierające informacje, które mogą być objęte ochroną (w tym zawierające dane klientów lub dłużników) powinny być przechowywane w zamkniętych szafach lub szufladach, zabezpieczonych przed dostępem do osób nieuprawnionych. W przypadku pracy zdalnej zasada ta oznacza wyznaczenie stanowiska pracy umożliwiającego zachowanie przetwarzanych danych w poufności;
e) zasada czystego biurka - należy unikać pozostawionych bez nadzoru dokumentów, a po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz innych nośników informacji;
f) zasada czystego ekranu - każdy komputer musi mieć ustawiony wygaszasz ekranu włączający się automatycznie po określonym czasie bezczynności użytkownika. Dodatkowo przed pozostawieniem włączonego komputera bez opieki użytkownicy mają obowiązek zablokować go (włączając wygaszasz ekranu) lub w przypadku dłuższej nieobecności wylogować się z systemu.
g) zasada czystego pulpitu - na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty folderów pod warunkiem, że w nazwie nie zawierają informacji o realizowanych projektach lub klientach.
h) zasada czystego kosza - dokumenty papierowe powinny być niszczone wyłącznie w niszczarce, w przypadku pracy zdalnej dokumenty powinny być zniszczone w inny sposób uniemożliwiający odtworzenie ich treści;
i) przebywanie osób nieupoważnionych do przetwarzania danych osobowych - osoby nieupoważnione do przetwarzania danych osobowych (np. goście, klienci, pracownicy serwisowi, osoby sprzątające) mogą przebywać w strefach, w których przetwarzane są dane osobowe wyłącznie pod nadzorem wyznaczonego pracownika Organizacji. W przypadku pracy zdalnej zasada ta oznacza wyznaczenie stanowiska pracy umożliwiającego zachowanie przetwarzanych danych w poufności.

§6 ZASADY DOSTĘPU DO DANYCH OSOBOWYCH

1. Wszyscy pracownicy Organizacji, niezależnie od prawnej formy współpracy z Organizacją, przed przystąpieniem do wykonywania obowiązków:

a) uzyskują od Organizacji upoważnienie do przetwarzania danych osobowych w celu zapewnienia, że do przetwarzania danych dopuszczono wyłącznie osoby pisemnie upoważnione przez Organizację do przetwarzania danych osobowych;
b) podlegają obowiązkowemu szkoleniu oraz są zaznajamiane w adekwatnym do rodzaju wykonywanych zadań zakresie z przepisami prawa oraz wewnętrznymi regulacjami chroniącymi dane osobowe w Organizacji;
c) są zobowiązani złożyć w formie pisemnej oświadczenie o zachowaniu poufności danych pozyskanych w toku współpracy z Organizacją.

2. Osoba odpowiedzialna w Organizacji za obszar HR lub osoba odpowiedzialna za ten obszar w podmiocie, któremu Organizacja powierzyła przetwarzanie danych osobowych:

a) jest uprawniona do udzielania upoważnień do przetwarzania danych osobowych o których mowa w § 6 ust. 1 lit. a Polityki;
b) odpowiada za prawidłowe udzielenie upoważnień i oświadczeń o zachowaniu poufności;
c) prowadzi i aktualizuje prowadzony w formie elektronicznej rejestr osób upoważnionych do przetwarzania danych osobowych.

3. Zakończenie współpracy z osobą upoważnioną jest równoznaczne z wygaśnięciem upoważnienia do przetwarzania danych osobowych. Organizacja może podjąć decyzję o cofnięciu upoważnienia do przetwarzania danych osobowych przed zakończeniem okresu wypowiedzenia umowy łączącej Organizację z osobą upoważnioną.

4. Udzielenie upoważnienia do przetwarzania danych osobowych oraz jego wygaśnięcie są podstawą do przyznania oraz odpowiednio odebrania dostępu do lokalizacji oraz systemów teleinformatycznych Organizacji, zgodnie z zasadami określonymi w Polityce Bezpieczeństwa Teleinformatycznego.

§7 KSZTAŁTOWANIE ŚWIADOMOŚCI PRACOWNIKÓW

1. Każdy pracownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej jest poddany szkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

2. Poza szkoleniami dla nowych pracowników prowadzonymi przez osoby odpowiedzialne w Organizacji za obszar HR, Organizacja przeprowadza szkolenia prowadzone przez Inspektora Ochrony Danych dla wszystkich pracowników Organizacji nie rzadziej, niż co sześć miesięcy;

3. Pracownicy mają obowiązek uczestniczenia w szkoleniach.

4. Zakres szkolenia obejmuje zaznajomienie z przepisami prawa dotyczącymi ochrony danych osobowych oraz politykami, procedurami i instrukcjami obowiązującymi w Organizacji. Szkolenie zostaje udokumentowane oraz zakończone podpisaniem przez pracownika lub współpracownika oświadczenia o odbyciu szkolenia.

§8 STATUS ORGANIZACJI W KONTEKŚCIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Organizacja pełni funkcję administratora danych osobowych w zakresie:
    a) danych osobowych pracowników Organizacji;
    b) danych osobowych osób rekrutowanych;
    c) danych osobowych klientów i potencjalnych klientów Organizacji;
    d) danych osobowych kontrahentów i dostawców produktów i usług dla Organizacji;
    e) danych osobowych personelu klientów, kontrahentów i dostawców.
2. Szczegółowy wykaz danych osobowych przetwarzanych przez Organizację znajduje się w Rejestrze Przetwarzania Danych Osobowych oraz w Rejestrze Kategorii Czynności Przetwarzania Danych Osobowych.
3. Inspektor Ochrony Danych na bieżąco uaktualnia rejestry, o których mowa w ust. 3.

§9 PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH

1. Organizacja przetwarza dane osobowe wyłącznie w przypadku spełnienia minimum jednej z przesłanek określonych w art. 6 RODO, to jest w szczególności jeżeli:
    a) osoba, której dane dotyczą wyraziła dobrowolną i wyraźną zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (przykładowo dla celów rekrutacji),
    b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (przykładowo w celu wykonania umowy łączącej Organizację z pracownikami, współpracownikami, klientami, kontrahentami);
    c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, wynikającego z prawa Unii Europejskiej lub z prawa polskiego (przykładowo w zakresie realizacji obowiązków podatkowych, rachunkowych, sprawozdawczych lub wynikających z przepisów prawa pracy);
    d) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Organizację lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem (przykładowo w zakresie kontaktu i relacji z personelem i reprezentantami klientów, kontrahentów lub kooperantów Organizacji).
2. Jeżeli przetwarzanie danych osobowych w Organizacji odbywa się na podstawie zgody, Organizacja jest w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Osoba, której dane dotyczą ma prawo w każdym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego na podstawie zgody przed jej wycofaniem. Wycofanie zgody jest równie łatwe jak jej wyrażenie.

3. Jeżeli przetwarzanie danych osobowych w Organizacji odbywa się na podstawie celów wynikających z prawnie uzasadnionych interesów realizowanych przez Organizację lub przez stronę trzecią Organizacja jest w stanie wykazać, że prawa i wolności osób, których dane dotyczą nie mają charakteru nadrzędnego wobec prawnie uzasadnionych interesów realizowanych przez Organizację.

§10 PODSTAWY PRZETWARZANIA DANYCH „WRAŻLIWYCH" I DANYCH O WYROKACH

1. Zasady przetwarzania danych osobowych, określone w § 9 Polityki Bezpieczeństwa nie dotyczą przetwarzania przez Organizację szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO oraz danych dotyczących wyroków skazujących i naruszeń prawa w rozumieniu art. 10 RODO, których przetwarzanie odbywa się na zasadach określonych we właściwych przepisach prawa.

2. Organizacja przetwarza szczególne kategorie danych osobowych wyłącznie w przypadku spełnienia minimum jednej z przesłanek określonych w art. 9 RODO, to jest w szczególności jeżeli:

   a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że przepisy prawa przewidują, iż osoba, której dane dotyczą, nie może wyrazić zgody na przetwarzanie szczególnych kategorii danych osobowych;
   b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone przepisami prawa;
   c) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
   d) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
   e) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego;
   f) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych.

3. Organizacja nie przetwarza danych osobowych dotyczących wyroków skazujących i naruszeń prawa w rozumieniu art. 10 RODO.

§11 REALIZACJA OBOWIĄZKÓW INFORMACYJNYCH

1. W przypadku zbierania przez Organizację danych osobowych od osoby, której dane dotyczą, Organizacja podczas pozyskiwania danych osobowych informuje tę osobę o

zasadach przetwarzania jej danych osobowych i przysługujących uprawnieniach, w zakresie określonym w art. 13 RODO.

2. W przypadku pozyskiwania przez Organizację danych osobowych w inny sposób niż od osoby, której dane dotyczą, Organizacja podczas pozyskiwania danych osobowych informuje tę osobę o zasadach przetwarzania jej danych osobowych i przysługujących uprawnieniach, w zakresie określonym w art. 14 RODO.

3. W przypadku, gdy osoba, której dane dotyczą tego zażąda, Organizacja udziela takiej osobie potwierdzenia, że jej dane są przetwarzane i na żądanie tej osoby, udziela jej informacji określonych w art. 15 RODO. Na żądanie osoby, której dane są przetwarzane, Organizacja dostarcza takiej osobie kopię danych osobowych podlegających przetwarzaniu.

4. W przypadku zbierania danych osobowych, w przypadku których Organizacja działa jako podmiot przetwarzający, za wypełnienie obowiązków informacyjnych odpowiedzialny jest klient Organizacji, będący administratorem danych powierzanych Organizacji w trybie art. 28 RODO.

5. Organizacja realizuje obowiązki informacyjne w szczególności poprzez politykę prywatności na stronie internetowej, komunikat znajdujący się w stopce email oraz klauzule informacyjne dołączane do umów zawieranych w pracownikami, klientami i kontrahentami.

§ 12 REALIZACJA UPRAWNIEŃ OSÓB, KTÓRYCH DANE PRZETWARZA ORGANIZACJA

1. Osobom, których dane osobowe przetwarza Organizacja, przysługuje prawo złożenia żądań określonych w art. 15-21 RODO. Żądanie może zostać wniesione w dowolnej formie, chociaż Organizacja zachęca do zgłaszania adresowanych żądań poprzez adres email rodo@knorr-bremse.com.

2. W przypadku, w którym Organizacja pełni funkcję administratora danych osobowych, odpowiedź na żądanie określone w art. 15-21 RODO udzielana jest w terminie 30 dni od jego wpłynięcia przez Inspektora Ochrony Danych Organizacji.

3. W przypadku, w którym Organizacja pełni funkcję podmiotu przetwarzającego, żądanie jest niezwłocznie przekazywane do administratora danych, a Organizacja udziela wsparcia informacyjnego i merytorycznego w zakresie udzielenia odpowiedzi, na zasadach określonych w umowie powierzenia przetwarzania danych.

4. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych. Osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

5. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe jeżeli występuje jedna z następujących okoliczności:

    a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego.
f) Osoba, której dane dotyczą, ma prawo żądania od Organizacji ograniczenia przetwarzania w przypadkach i na zasadach określonych w art. 18 RODO.
g) W przypadku, w którym Organizacja pełni funkcję administratora danych osobowych, informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonała zgodnie z art. 16-18 RODO każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Organizacja informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
h) Osoba, której dane dotyczą, na jej żądanie, otrzymuje od Organizacji w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Organizacji oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Organizacji w przypadkach i na zasadach określonych w art. 20 RODO.
i) Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, na zasadach i w trybie określonym w art. 21 RODO. W takiej sytuacji Organizacji nie wolno już przetwarzać tych danych osobowych, chyba że Organizacja wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
j) Jeżeli dane osobowe są przetwarzane przez Organizację na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. W takim przypadku Organizacja zaprzestaje przetwarzania takich danych osobowych i niezwłocznie je trwale i nieodwracalnie usuwa.
k) Pracownik lub współpracownik, który uzyskał od jakiejkolwiek osoby fizycznej żądanie określone w art. 15-21 RODO, jest bezwzględnie zobowiązany do powiadomienia o tym fakcie przełożonego oraz przesłanie wiadomości na adres rodo@knorr-bremse.com.

§ 13 POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie przez Organizację przetwarzania danych osobowych innemu podmiotowi przetwarzającemu może nastąpić wyłącznie na rzecz podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą, przy spełnieniu wymogów wynikających z przepisów prawa, zwłaszcza w art. 28 RODO, po zawarciu pisemnej umowy powierzenia przetwarzania danych osobowych.
2. Dalsze powierzenie (podpowierzenie) przez Organizację działającą jako podmiot przetwarzający danych osobowych innemu podmiotowi przetwarzającemu dane osobowe w imieniu Organizacji może nastąpić wyłącznie po uzyskaniu zgody podmiotu, który powierzył przetwarzanie danych osobowych Organizacji, w sposób określony w stosownej umowie powierzenia przetwarzania danych.
3. Umowy powierzenia przetwarzania danych osobowych określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora i wypełniają pozostałe obowiązki wynikające z art. 28 RODO.

§14 OBOWIĄZKI ZWIĄZANE Z ZAGROŻENIEM LUB NARUSZENIEM OCHRONY DANYCH

1. Każdy pracownik Organizacji, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest do poinformowania swojego bezpośredniego przełożonego oraz zawiadomienia Inspektora Ochrony Danych poprzez adres rodo@knorr-bremse.com.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    b) niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem danych, kradzieżą i utratą danych osobowych;
    c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników/współpracowników.
3. Do typowych naruszeń bezpieczeństwa danych osobowych należą:
    a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
    b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);
    c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)

4. W przypadku stwierdzenia wystąpienia zagrożenia Organizacja, działając poprzez osoby odpowiedzialne za przestrzeganie danych osobowych, prowadzi postępowanie wyjaśniające w czasie którego ustalany jest zakres i przyczyny zagrożenia oraz jego ewentualne skutki, inicjowane są ewentualne działania dyscyplinarne, rekomendowane są działania prewencyjne oraz dokonywane są odpowiednie działania wynikające z przepisów prawa.

§15 NARUSZENIE OCHRONY DANYCH ADMINISTROWANYCH PRZEZ ORGANIZACJĘ

1. W przypadku gdy Organizacja działa jako administrator danych osobowych, w przypadku jakiegokolwiek naruszenia bezpieczeństwa danych osobowych, zastosowanie znajduje procedura określona w niniejszym paragrafie Polityki Bezpieczeństwa.
2. Naruszenie bezpieczeństwa danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
3. Organizacja dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w rejestrze naruszeń ochrony danych osobowych.
4. Rejestr naruszeń umożliwia organowi nadzorczemu weryfikowanie przestrzegania obowiązków wynikających z przepisów prawa i Polityki Bezpieczeństwa. Rejestr jest na bieżąco aktualizowany i weryfikowany przez Inspektora Ochrony Danych.
5. W przypadku, gdy Organizacja działa jako administrator danych osobowych, jeżeli wskutek naruszenia istnieje większe niż pomijalne ryzyko naruszenia praw osób, których dane osobowe podlegały naruszeniu, Organizacja bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je na przewidzianym formularzu organowi nadzorczemu.
6. W przypadku zgłoszenia naruszenia ochrony danych osobowych następującego po upływie 72 godzin od stwierdzenia naruszenia, Organizacja do zgłoszenia przesłanego Prezesowi Urzędu Ochrony Danych Osobowych załącza także wyjaśnienie przyczyn opóźnienia. Jeżeli zgłoszenia naruszenia ochrony danych osobowych nie można w całości dokonać w tym samym czasie, Organizacja dokonuje częściowych zgłoszeń sukcesywnie.
7. W przypadku, gdy Organizacja działa jako administrator danych osobowych, w przypadku naruszenia ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Organizacja niezwłocznie zawiadamia osobę, której dane dotyczą, o naruszeniu.

§16 NARUSZENIE OCHRONY DANYCH POWIERZONYCH ORGANIZACJI

1. W przypadku, gdy Organizacja działa jako podmiot przetwarzający dane osobowe, po stwierdzeniu naruszenia ochrony danych osobowych, bez zbędnej zwłoki zgłasza je administratorowi danych, który powierzył Organizacji przetwarzanie danych osobowych w formie zawiadomienia.

2. W przypadku zaistnienia naruszenia ochrony danych osobowych, Organizacja stosuje procedurę określoną w Organizacji oraz w zawartej umowie powierzenia przetwarzania danych osobowych, na mocy której powierzono jej przetwarzanie.
3. Powiadomienie organu nadzorczego lub osób, których danych dotyczy naruszenie następuje wyłącznie w sytuacji, w której stosowne działanie zostanie zlecone w wyraźny sposób przez administratora danych powierzonych Organizacji.

§17 PRZEGLĄD ROCZNY ORAZ RETENCJA DANYCH OSOBOWYCH

1. Corocznie, do dnia 30 grudnia każdego roku, Inspektor Ochrony Danych, Administrator IT oraz inne osoby odpowiedzialne za ochronę bezpieczeństwa danych osobowych w Organizacji przygotowują sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych.
2. Z przeglądu rocznego systemu ochrony danych osobowych sporządzany jest pisemny protokół zawierający ewentualne rekomendacje.
3. W ramach przeglądu rocznego Organizacja dokonuje przeglądu przetwarzanych w formie tradycyjnej oraz poprzez systemy teleinformatyczne danych osobowych pod kątem konieczności usunięcia lub anonimizacji w zakresie danych, co do których upłynął okres ich przechowywania, ustalony zgodnie z Tabelą Retencji Danych obowiązującą w Organizacji.
4. Podmiotem odpowiedzialnym za realizację procesów związanych z retencją danych osobowych są osoby odpowiedzialne w Organizacji za obszar HR i IT. Wszyscy pracownicy mają obowiązek wspierać powyższe osoby w realizacji obowiązków związanych z retencją danych, w szczególności dokonać zniszczenia lub anonimizacji wskazanych danych oraz udzielać informacji oraz odpowiedzi na pytania.

§18 INSPEKTOR OCHRONY DANYCH

1. Organizacja powołała Inspektora Ochrony Danych osobowych, który odpowiedzialny jest za całokształt działań zapewniających adekwatny i odpowiedni poziom ochrony danych osobowych w Organizacji.
2. Inspektor Ochrony Danych osobowych w swoich zadaniach wspierany jest przez dyrektorów i kierowników odpowiednich komórek organizacyjnych Organizacji oraz Administratora IT.
3. Kontakt z Inspektorem Ochrony Danych możliwy jest:
    a) Pisemnie, pod adresem: Knorr Bremse Systemy Pojazdów Szynowych Sp. z o.o. z siedzibą w Rzeszowie, ul. Innowacyjna 2, 30-396 Rzeszów,
    b) Elektronicznie, pod adresem e-mail: rodo@knorr-bremse.com.
4. Do najważniejszych zadań i obowiązków Inspektora Ochrony Danych osobowych w Organizacji należy:

a) działania zmierzające do zapewnienia przetwarzania danych osobowych zgodnie z przepisami prawa oraz obowiązującymi w Organizacji wewnętrznymi regulacjami;
b) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
c) przygotowywanie i udzielanie odpowiedzi na żądania osób, których dane przetwarza Organizacja;
d) wsparcie działów Organizacji pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
e) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
f) współpraca z klientami i kontrahentami w zakresie ochrony danych osobowych;
g) sporządzanie sprawozdań rocznych z ochrony danych osobowych w Organizacji oraz organizowanie i prowadzenie szkoleń z zakresu bezpieczeństwa danych;

5. Inspektor Ochrony Danych osobowych wykonuje swoje zadania z zachowaniem odpowiedniej dozy niezależności. Organizacja zapewnia Inspektorowi Ochrony danych odpowiednie zasoby umożliwiające realizację zadań.

§19 POSTANOWIENIA KOŃCOWE

1. Organizacja ma obowiązek zapoznać z treścią Polityki Bezpieczeństwa każdego pracownika lub współpracownika.
2. Pracownicy i współpracownicy Organizacji zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce Bezpieczeństwa.
3. Polityka Bezpieczeństwa wchodzi w życie z dniem podpisania i zastępuje mające taki sam zakres merytoryczny dokumenty, polityki i procedury regulujące przetwarzanie danych osobowych.
4. Wszelkie zmiany niniejszej Polityki Bezpieczeństwa wymagają zachowania formy pisemnej.

W imieniu Organizacji:

.....

Jacek Biłas

Prezes Zarządu (R/MDL)

.....

Łukasz Zalibowski

HR Director (R/HRL)