26 czerwca 2018 r.

EXIDE TECHNOLOGIES
(„Exide” lub „Firma”)

Polityka w zakresie ochrony danych osobowych („Polityka”)

Należy zapoznać się z treścią niniejszej polityki, ponieważ zawiera ona ważne informacje dotyczące:

- przepisów w zakresie ochrony danych, którym podlega Exide;
- definicji danych osobowych i wrażliwych danych osobowych;
- sposobu gromadzenia, wykorzystywania oraz usuwania danych osobowych i wrażliwych danych osobowych przez Exide zgodnie z niniejszą polityką;
- miejsca, gdzie można znaleźć dodatkowe informacje dotyczące danych, np. zakresu gromadzonych i wykorzystywanych danych osobowych, sposobu ich wykorzystywania, przechowywania i przekazywania; celów, na które są wykonywane te czynności, kroków podejmowanych w celu zapewnienia bezpieczeństwa danych i okresu przechowywania;
- obowiązków jako pracownika Exide w związku z ochroną danych osobowych; i
- konsekwencji w przypadku niestosowania się do tej polityki.

1 Wprowadzenie

1.1 Exide zbiera, przechowuje i wykorzystuje dane osobowe (w dalszej części zwane „danymi osobowymi”) osób trzecich na określone, zgodne z prawem cele, wymienione w *informacjach o ochronie danych osobowych* Exide.

1.2 Niniejsza polityka określa, w jaki sposób wypełniane są obowiązki w zakresie ochrony danych osobowych. Celem tej polityki jest również zapewnienie, że osoby zatrudnione przez firmę, w tym pracownicy i osoby zatrudnione tymczasowo lub przez biuro pośrednictwa rozumieją zasady w zakresie gromadzenia, wykorzystywania i usuwania danych osobowych, do których mogą mieć dostęp podczas wykonywania swojej pracy, i stosują się do nich.

1.3 Exide dokonuje wszelkich starań, aby spełniać obowiązki w zakresie ochrony danych osobowych i do zachowania transparentności w zakresie czynności związanych z uzyskiwaniem i używaniem danych osobowych oraz sposobu i terminu usuwania tych danych, kiedy ich przechowywanie nie jest konieczne.

1.4 W przypadku pytań, komentarzy lub wątpliwości dotyczących treści tej polityki należy skontaktować się miejscowym przedstawicielem ds. RODO lub działem prawnym.

2 Zakres

2.1 Osoby zatrudnione przez firmę powinny zapoznać się z informacjami o ochronie danych osobowych Exide oraz innymi mającymi zastosowanie politykami w tym tymi dotyczącymi *bezpieczeństwa informacji i przechowywania danych w rejestrach,* które zawierają dodatkowe informacje dotyczące ochrony danych osobowych w danych kontekstach.

2.2 Exide będzie sprawdzać i aktualizować tę politykę zgodnie z obowiązkami firmy w zakresie ochrony danych osobowych. Ta polityka nie stanowi części żadnej umowy o pracę z zatrudnionym pracownikiem i Exide zastrzega sobie prawo do wprowadzania do niej zmian, aktualizacji czy dodatków od czasu do czasu. Exide przekaże swoim pracownikom nową lub zmienioną politykę w momencie jej przyjęcia.

3 Definicje

wpisy o karalności oznacza dane osobowe dotyczące popełnionych przestępstw i wyroków skazujących,

informacje dotyczące oświadczeń, procedur i powiązanych środków bezpieczeństwa;

naruszenie danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub nieprawnego zniszczenia, zagubienia, zmiany, nieautoryzowanego ujawnienia lub dostępu do danych osobowych;

podmiot danych osobowych oznacza osobę, której te dane dotyczą;

dane osobowe oznaczają informacje dotyczące podmiotu danych,

którego tożsamość można określić (bezpośrednio lub niebezpośrednio) na podstawie tych danych;

przetwarzanie informacji oznacza uzyskiwanie, nagrywanie, organizowanie, gromadzenie, wprowadzanie zmian, odzyskiwanie, ujawnianie lub/i usuwanie takich informacji lub w bardziej ogólny sposób używanie ich lub wykonywanie na nich dowolnych czynności;

dane opatrzone pseudonimem oznacza proces, w którym dane osobowe są przetwarzane w takich sposób, że nie można ich użyć w celu określenia tożsamości podmiotu danych bez dodatkowych informacji, które są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym, które zapewniają niemożliwość przypisania danych osobowych do osoby o możliwej do określenia tożsamości;

Wrażliwe dane osobowe (czasami nazywane „specjalnymi kategoriami danych osobowych" lub „poufnymi danymi osobowymi") oznaczają informacje dotyczące rasy, pochodzenia

etnicznego, opinii politycznych, przekonań religijnych lub filozoficznych, przynależności związkowej (lub niezwiązkowej), informacje genetyczne, biometryczne (używane do określenia tożsamości podmiotu danych) oraz informacje dotyczące zdrowia, życia seksualnego lub orientacji seksualnej danej osoby.

4 Zasady ochrony danych

4.1 Exide będzie postępował zgodnie z nas zasadami ochronny danych osobowych podczas ich przetwarzania:

4.1.1 będziemy przetwarzać wszelkie dane w sposób zgodny z przepisami prawa, jasny i transparenty;

4.1.2 będziemy gromadzić dane osobowe jedynie na konkretne, jasno określone i legalne cele i nie będziemy ich przetwarzać w sposób niezgodny z legalnymi celami;

4.1.3 będziemy przetwarzać dane osobowe, które są niezbędne, stosowne i konieczne na określone cele;

4.1.4 będziemy przechowywać dokładne i aktualne dane osobowe oraz podejmiemy racjonalne kroki w celu usunięcia lub poprawienia niedokładnych danych bez zwłoki;

4.1.5 będziemy przechowywać dane osobowe w sposób, który pozwala na identyfikacje podmiotów danych przez okres czasu nie dłuższy od okresu koniecznego w celu realizacji celów, na które dane są przetwarzane; i

4.1.6 podejmiemy odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych i zabezpieczenia ich przed nieautoryzowanym przetwarzaniem i przypadkową utratą, zniszczeniem lub uszkodzeniem.

5 Podstawy do przetwarzania danych osobowych

5.1 Exide, przed wykonaniem jakiejkolwiek czynności związanej z przetwarzaniem po raz pierwszy i następnie regularnie, będzie:

5.1.1 sprawdzać cele danej czynności z zakresu przetwarzania danych i wybierać najbardziej odpowiednią podstawę prawną (lub podstawy) dla tej czynności, tj.:

(a) czy podmiot danych wyraził zgodę na przetwarzanie;

(b) czy przetwarzanie jest konieczne w celu wykonania umowy, w której podmiot danych jest stroną lub w celu wykonania kroków na żądanie podmiotu danych przed zawarciem umowy;

(c) czy przetwarzanie jest konieczne w celu spełnienia prawnego obowiązku, któremu

podlega Firma;

(d) czy przetwarzanie jest konieczne w celu ochrony uzasadnionych interesów podmiotu danych lub interesów innej osoby fizycznej; lub

(e) że przetwarzanie jest konieczne w celu ochrony prawnych interesów Exide lub firmy lub osoby trzeciej, za wyjątkiem, gdy są one sprzeczne z interesami lub podstawowymi prawami czy wolnościami podmiotu danych — patrz punkt 5.2 poniżej.

5.1.2 za wyjątkiem, gdy podstawą do przetwarzania danych jest zgoda wyrażona przez podmiot danych, sprawdzać, czy przetwarzanie jest konieczne na cel określonej podstawy prawnej, tj. brak jest żadnego innego racjonalnego sposobu pozwalającego osiągnąć ten cel);

5.1.3 odpowiednio dokumentować decyzję odnoszącą się do mającej zastosowanie podstawy prawnej, aby wykazać zgodność z przepisami w zakresie ochrony danych osobowych;

5.1.4 uwzględniać informacje dotyczące zarówno celu przetwarzanie, jak i podstawy prawnej w odpowiedniej informacji o polityce prywatności;

5.1.5 w przypadku przetwarzania wrażliwych danych osobowych, również wskazywać specjalne warunki prawne w celu przetwarzania tego typu informacji (patrz punkt 6.2.2 poniżej) i dokumentować ten fakt (tylko dla Wielkiej Brytanii); i

5.1.6 w przypadku przetwarzania informacji dotyczących wpisów o karalności zgodnie z prawem unijnym lub państwa członkowskiego, również wskazać warunki prawne w celu przetwarzania tego typu informacji i dokumentować ten fakt.

5.2 Podczas określania, czy prawny interes Firmy jest najwłaściwszą podstawą do legalnego przetwarzania danych, Exide:

5.2.1 przeprowadzi ocenę interesów prawnych (LIA, z ang. legitimate interests assessment) i zachowa jej dokumentację, aby zapewnić, że może uzasadnić swoją decyzję;

5.2.2 w przypadku, gdy LIA wykaże znaczące skutki dla prywatności osób, rozważy, czy jest również konieczne przeprowadzenie oceny skutków w zakresie ochrony danych (DPIA, ang. data protection impact assessment); i

5.2.3 zawrze informacje o prawnych interesach w stosownej(ych) informacji(ach) o polityce prywatności.

6 Wrażliwe dane osobowe

6.1 Wrażliwe dane osobowe są czasami nazywane „specjalnymi kategoriami danych osobowych” lub „poufnymi danymi osobowymi” .

6.2 Firma może od czasu do czasu przetwarzać wrażliwe dane osobowe. Exide będzie przetwarzać tego typu dane, jeśli:

6.2.1 będzie miała do tego prawną podstawę, tak jak określono w punkcie 5.1.1 powyżej, np. będzie to konieczne w celu wykonania umowy o pracę, w celu spełnienia obowiązków prawnych Exide lub prawnych interesów firmy; i

6.2.2 będzie miał zastosowanie jeden ze specjalnych warunków w celu przetwarzania wrażliwych danych osobowych, np.

(a) podmiot danych wyrazi na to wyraźną zgodę;

(b) przetwarzanie będzie konieczne w celu egzekwowania praw wynikających z prawa pracy lub obowiązków Exide lub podmiotu danych;

(c) przetwarzanie będzie konieczne w celu ochrony prawnych interesów podmiotu danych i podmiot danych jest fizycznie niezdolny do udzielenia zgody;

(d) przetwarzanie będzie odnosić się do danych osobowych, które zostały upublicznione przez podmiot danych;

(e) przetwarzanie jest konieczne w celu ustanowienia roszczeń prawnych, ich realizacji lub bronienia ich. lub

(f) przetwarzanie jest konieczne ze względu na istotny interes publiczny.

6.3 Wrażliwe dane osobowe nie będą przetwarzane przez Exide, chyba, że:

6.3.1 podmiot danych został odpowiednio poinformowany (za pomocą informacji o polityce prywatności lub w inny sposób) o czynności przetwarzania, celach na które jest ona wykonywana i o jej prawnej podstawie.

6.4 Firma nie będzie podejmować decyzji automatycznych (w tym profilowanie) w oparciu o wrażliwe dane osobowe.

6.5 *Informacja o polityce prywatności* Firmy obejmuje rodzaje wrażliwych danych osobowych, które przetwarza Exide, cele ich przetwarzania oraz podstawę prawną przetwarzania.

6.6 Firma będzie postępować zgodnie z procedurami opisanymi w punktach 6.7 i 6.8 poniżej w kwestiach związanych z wrażliwymi danymi osobowymi, aby upewnić się, że są one zgodne z zasadami w zakresie ochrony danych osobowych wymienionymi w punkcie 4 powyżej.

6.7 **Podczas procesu rekrutacyjnego**: Dział zasobów ludzkich Exide upewni się, że (chyba że przepisy prawa stanowią inaczej):

6.7.1 podczas wstępnego wyboru kandydatów, rozmów kwalifikacyjnych i podejmowania ostatecznej decyzji nie będą zadawane żadne pytania dotyczące wrażliwych danych osobowych, np. rasy czy pochodzenia etnicznego, przynależności związkowej lub zdrowia;

6.7.2 wszelkie wypełnione formularze dotyczące nadzoru nad równymi szansami są przechowywane oddzielnie od zgłoszenia podmiotu danych i nie są dostępne osobie dokonującej wstępnego wyboru kandydatów, przeprowadzającej rozmowę kwalifikacyjną i podejmującą ostateczną decyzję;

6.7.3 czynności kontrolne w zakresie prawa do pracy są wykonywane przed przedstawieniem bezwarunkowej oferty pracy, a nie w fazach wstępnego wyboru kandydatów, rozmów kwalifikacyjnych i podejmowania ostatecznej decyzji;

6.8 **Podczas stosunku pracy**: Dział zasobów ludzkich przetworzy:

6.8.1 dane dotyczące zdrowia na cele związane z ustaleniem możliwości dopuszczenia do pracy, wypłatą zasiłku chorobowego, utrzymaniem rejestru dni na zwolnieniu lekarskim, nadzorem nad obecnością pracowników i udzielaniem świadczeń związanych ze zdrowiem i z tytułu choroby;

6.8.2 wrażliwe dane osobowe na cele związane z nadzorem nad równymi szansami. Dane te będą anonimizowane, jeśli będzie to możliwe; i

6.8.3 informacje dotyczące przynależności związkowej na cele związane z zażądaniem pracownikami i wypisami.

7 Informacje o wpisach o karalności

Informacje o wpisach o karalności będą przetwarza zgodnie z obowiązującymi przepisami unijnymi lub danego kraju członkowskiego.

8 Oceny skutków w zakresie ochrony danych

8.1 W przypadku, gdy czynność przetwarzania może stanowić wysokie zagrożenie dla praw do ochrony danych osobowych podmiotu danych (np. kiedy Exide planuje wdrożyć nową technologię), przed przystąpieniem do realizacji tej czynności, dokona oceny skutków w zakresie ochrony danych:

8.1.1 czy czynność przetwarzania jest konieczna i proporcjonalna w stosunku do jej celu;

8.1.2 zagrożeń dla podmiotów danych; i

8.1.3 określi jakie środki należy podjąć w celu ochrony przed tymi zagrożeniami i ochrony danych osobowych.

8.2 Przed wdrożeniem dowolnej nowej technologii właściwy kierownik powinien skontaktować się z Działem IT w celu wykonania oceny skutków w zakresie ochrony danych.

8.3 Podczas realizacji oceny Firma zwróci się o opinię i poglądy innych ważnych akcjonariuszy.

9 Dokumentacja i rejestry

9.1 Exide będzie prowadzić pisemny rejestr czynności przetwarzania, w tym:

9.1.1 nazwę i inne dane osoby prawej Exide (i jeśli dotyczy innych administratorów danych);

9.1.2 cele przetwarzania;

9.1.3 opis kategorii danych osobowych podmiotów danych i kategorii danych osobowych;

9.1.4 kategorii odbiorców danych osobowych;

9.1.5 jeśli dotyczy, szczegółowych informacji dotyczących przekazywania do krajów trzecich, w tym dokumentacji dot. stosowanych zabezpieczeń zapewniających odpowiedni poziom ochrony transferu.

9.1.6 jeśli jest to możliwe, czasów przechowywania; i

9.1.7 jeśli jest to możliwe, opisu technicznych i organizacyjnych środków bezpieczeństwa.

9.2 W ramach prowadzonego rejestru czynności przetwarzania przechowujemy następującą dokumentację lub zamieszczamy do niej linki:

9.2.1 informacje o polityce prywatności;

9.2.2 udzielone zgody;

9.2.3 umowy z administratorami danych;

9.2.4 informacje o lokalizacji danych osobowych;

9.2.5 oceny skutków w zakresie ochrony danych; i

9.2.6 zapisy naruszeń danych.

9.3 W przypadku przetwarzania wrażliwych danych osobowych lub informacji o wpisach o karalności Exide będzie prowadzić pisemny rejestr:

9.3.1 celów, na które przetwarzane są dane, w tym informacji, dlaczego realizacja danej czynności przetwarzania jest konieczna na ten cel (jeśli takowa jest wymagana);

9.3.2 podstaw prawnych przetwarzania; i

9.3.3 informacji, czy dane osobowe są przechowywane czy też usuwane zgodnie z polityką prywatności i, jeśli tak się nie dzieje, informacji o przyczynach niepostępowania zgodnie z polityką.

9.4 Exide będzie regularnie dokonywać przeglądu przetwarzanych danych osobowych i aktualizować

prowadzoną dokumentację i rejestry.

10 Prawa podmiotów danych

10.1 Podmioty danych mają względem swoich danych osobowych następujące prawa:

10.1.1 do uzyskania informacji dotyczących sposobu, przyczyny i podstawy przetwarzania danych osobowych — patrz *[informacja o polityce prywatności] Exide;*

10.1.2 do uzyskania potwierdzenia o fakcie, że ich dane są przetwarzane oraz do wglądu do nich i uzyskania innych informacji poprzez wysłanie stosownego wniosku o dostęp do informacji;

10.1.3 do wprowadzania poprawek do danych, jeśli są one nieprawidłowe lub niepełne;

10.1.4 do żądania ich usunięcia, jeśli nie są one niezbędne na cel, na który zostały pierwotnie zebrane/przetworzone lub jeśli brak jest prawnej podstawy do ich przetwarzania (to prawo jest czasem nazywane „prawem do bycia zapomnianym”);

10.1.5 do ograniczenia przetwarzania danych osobowych, w przypadku gdy ich dokładność jest kwestionowana lub samo przetwarzanie jest niezgodne z prawem; i

10.1.6 do tymczasowego ograniczenia przetwarzania danych osobowych, w przypadku

gdy uważają, że są one nieprawidłowe lub nie zgadzają się na przetwarzanie danych.

10.1.7 w przypadkach uregulowanych przepisami prawa, do ustalenia zasad, na podstawie których dane będą przechowywane, usuwane i przekazywane po ich śmierci.

11 Obowiązki podmiotów danych

11.1 Pracownicy mają obowiązek dbać, aby dane przechowywane przez Exide były aktualne. Poszczególne osoby mogą mieć dostęp do danych osobowych innych pracowników, dostawców czy klientów podczas trwania umowy lub zatrudnienia. Firma wymaga od takich osób, aby spełniały obowiązki w zakresie ochrony danych osobowych takich podmiotów danych. W przypadku dostępu do takich danych dana osoba ma obowiązek:

11.1.1 do uzyskiwania dostępu do danych osobowych jedynie w przypadku posiadania odpowiednich uprawnień i jedynie na dozwolone cele;

11.1.2 do zezwalania na dostęp do danych osobowych innym pracownikom Exide, jeśli mają odpowiednie uprawnienia;

11.1.3 do zezwalania osobom niezatrudnionym przez Firmę na dostęp do danych osobowych jedynie w przypadku stosownego upoważnienia udzielonego przez Dział zasobów ludzkich lub prawny;

11.1.4 do dbania o bezpieczeństwa danych, np. poprzez przestrzeganie zasad dostępu do siedziby firmy, dostępu do komputera, ochrony hasłem oraz bezpiecznego przechowywania plików i ich usuwania, jak również innych przestrzeganie innych środki ostrożności wymienionych w Globalnej polityce bezpieczeństwa informacji firmy);

11.1.5 do wynoszenia danych osobowych lub urządzeń zawierających dane osobowe (lub urządzeń umożliwiających do nich dostęp) z siedziby firmy, jeśli nie zostały podjęte odpowiednie środki bezpieczeństwa (takie jak pseudonimizacja, szyfrowanie lub ochrona hasłem) w celu zabezpieczenia danych i urządzeń; i

11.1.6 do nieprzechowywania danych osobowych na dyskach lub innych urządzeniach prywatnych wykorzystywanych na cele robocze.

11.2 W przypadku podejrzeń, że miało miejsce jedno z następujących naruszeń (lub ma bądź będzie mieć miejsce), należy skontaktować się z działem zasobów ludzkich lub działem prawnym:

11.2.1 przetwarzanie danych osobowych bez odpowiedniej ku temu podstawy prawnej lub też w przetwarzanie wrażliwych danych osobowych;

11.2.2 dowolne naruszenie bezpieczeństwa z tych wymienionych w punkcie 15.1 poniżej;

11.2.3 dostęp do danych osobowych bez stosownego upoważnienia;

11.2.4 dane osobowe nie były przechowywane lub usuwane w bezpieczny sposób;

11.2.5 wynoszenie danych osobowych lub urządzeń zawierających dane osobowe (lub urządzeń umożliwiających do nich dostęp) z siedziby firmy, jeśli nie zostały podjęte odpowiednie środki bezpieczeństwa

11.2.6 dowolne naruszenie bezpieczeństwa wymienione w tej polityce lub którekolwiek z tych wymienionych w punkcie 4.1 powyżej;

12 Dostęp podmiotu danych

12.1 Podmiot danych może w dowolnym momencie zażądać, aby firma udzieliła mu informacji o przetwarzanych przez nią danych. Firma ma obowiązek odpowiedzieć na takie żądanie w terminie miesiąca, licząc od dnia otrzymania (termin ten można przedłużyć do dwóch miesięcy w przypadku skomplikowanych lub/i licznych żądań, jednak w takim przypadku należy poinformować i tym fakcie podmiot danych).

12.2 Wszystkie żądania podmiotów danych należy przekazać do miejscowego przedstawiciela ds. RODO.

12.3 Firma nie pobiera żadnych opłat za obsługę zwykłych żądań podmiotów danych. Exide

zastrzega sobie prawo do pobierania racjonalnych opłat za dodatkowe kopie danych, które zostały wcześniej przekazane do podmiotu danych lub w przypadku, gdy żądania są ewidentnie bezpodstawne lub nadmierne, a zwłaszcza, gdy takie żądania powtarzają się.

13 Bezpieczeństwo informacji

13.1 Firma podejmie odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych, a zwłaszcza w celu zabezpieczenia ich przed nieautoryzowanym przetwarzaniem i przypadkową utratą, zniszczeniem lub uszkodzeniem. Mogą one obejmować:

13.1.1 upewnienie się, jeśli jest to możliwe, że dane osobowe zostały opatrzone pseudonimem lub zaszyfrowane;

13.1.2 zapewnienie bieżącej poufności, bezpieczeństwa, dostępności i odporności systemów przetwarzania i usług;

13.1.3 zapewnienie, że w przypadku jakiejkolwiek awarii technicznej lub fizycznej, będzie możliwe odzyskanie dostępu do danych w sposób terminowy; i

13.1.4 procedury regularnego testowania, analizy i oceny wydajności środków technicznych i organizacyjnych stosowanych w celu zabezpieczenia przetwarzanych danych.

13.2 W przypadku, gdy Firma korzysta z usług osób trzecich w celu przetwarzania danych osobowych w jej imieniu, należy w umowach z tymi osobami trzecimi uwzględnić dodatkowe środki bezpieczeństwa, aby zapewnić ochronę danych osobowych. W szczególności umowy z osobami trzecimi powinny zawierać następujące wzmianki:

13.2.1 że osoba trzecia lub zewnętrza organizacja może działać jedynie zgodnie z pisemną instrukcją Exide;

13.2.2 że przetwarzane dane są poufne;

13.2.3 że należy zapewnić odpowiednie środki w celu zagwarantowania bezpieczeństwa przetwarzanych danych

13.2.4 podwykonawcy mogą być zatrudniani jedynie po uzyskaniu wcześniejszej zgody Exide i należy z nimi obowiązkowo podpisać umowę;

13.2.5 że osoba trzecia lub zewnętrzna organizacja będzie pomagać Exide w udzielaniu dostęp do danych podmiotowi do tych danych oraz zezwoli podmiotowi danych na egzekwowanie swoich praw w zakresie ochrony danych osobowych;

13.2.6 że osoba trzecia lub zewnętrza organizacja będzie pomagać Exide w spełnianiu obowiązków w zakresie bezpieczeństwa przetwarzania, powiadamiania o naruszeniach bezpieczeństwa i ocenie skutków w zakresie ochrony danych;

13.2.7 że osoba trzecia lub zewnętrza organizacja usunie lub zwróci wszystkie dane osobowe Exide, zgodnie z żądaniem firmy, na koniec okresu obowiązywania umowy;

13.2.8 że osoba trzecia lub zewnętrza organizacja będzie podlegać audytom i kontrolom oraz przekaże Exide wszelkie informacje, których firma będzie potrzebować w celu zapewnienia, że zarówno Exide, jak i osoba trzecia spełniają obowiązki w zakresie ochrony danych osobowych; i

13.2.9 że osoba trzecia lub zewnętrza organizacja powiadomi Exide w sposób natychmiastowy w przypadku wystąpienia podejrzeń co do wystąpienia naruszenia w zakresie ochrony danych osobowych.

13.3 Przed podpisaniem umowy obejmującej przetwarzanie danych osobowych przez osobę trzecią lub zewnętrzną organizację lub wprowadzeniem zmian do istniejącej umowy, pracownicy za to odpowiadający powinni uzyskać zatwierdzenie od działu prawnego Exide.

14 Przechowywanie danych osobowych i okres tego przechowywania

14.1 Dane osobowe (oraz wrażliwe dane osobowe) należy przechowywać w sposób bezpieczny zgodnie z Globalną polityką bezpieczeństwa informacji firmy.

14.2 Dane osobowe (wrażliwe dane osobowe) nie mogą być przechowywane dłużej niż jest to konieczne. Długość okresu przechowywania danych zależy od okoliczności przetwarzania, w

tym od przyczyn, dla których dane zostały zebrane. Pracownicy powinni postępować zgodnie z Polityką przechowywania rejestrów firmy, w której treści ustanowiono okres przechowywania, lub kryteria, które pomagają określić jego długość. W przypadku wątpliwości pracownik powinien skontaktować się z miejscowym przedstawicielem ds. RODO lub działem prawnym.

15 Naruszenia bezpieczeństwa danych

15.1 Naruszenia bezpieczeństwa danych mogą mieć różną formę:

15.1.1 utrata lub kradzież danych lub urządzenia, na którym dane osobowe są przechowywane;

15.1.2 nieautoryzowany dostęp lub wykorzystanie danych osobowych przez pracownika lub osobę trzecią;

15.1.3 utrata danych wynikająca z błędu urządzenia lub systemu (w tym oprogramowania lub sprzętu hardware);

15.1.4 błąd ludzki, taki jak przypadkowe usunięcie czy wprowadzenie zmian;

15.1.5 siły wyższe, takie jak pożar czy powódź;

15.1.6 celowe ataki na systemy IT, takie jak ataki hackerskie, wirusy czy phishing; i

15.1.7 uzyskiwanie danych przez oszustów przechowujących dane.

15.2 Firma zobowiązuje się do:

15.2.1 zgłoszenia naruszenia bezpieczeństwa danych do właściwego organu nadzorującego lub biura ds. danych osobowych (ang. Information Commissioner's Office) w Wielkiej Brytanii bez zbędnej zwłoki i, jeśli jest to możliwe, w przeciągu 72 godzin od uzyskania świadomości na ten temat, określenia, czy to naruszenie może stanowić zagrożenie dla praw i wolności osób, których dane dotyczą; i

15.2.2 powiadomienia podmiotu danych, którego dotyczy naruszenie, jeśli naruszenie może stanowić zagrożenie dla jego praw i wolności osób i obowiązek powiadomienia wynika z obowiązujących przepisów prawa.

16 Międzynarodowe przekazywanie danych

16.1 Firma może przekazywać dane osobowe poza Europejski Obszar Gospodarczy (który obejmuje Unię Europejską, Islandię, Liechtenstein i Norwegię) do swojej spółki dominującej, Exide Technologies, w Stanach Zjednoczonych na takiej podstawie, że Exide Technologies można uznać za przedsiębiorstwo mające standardowe klauzule dotyczące ochrony danych.

17 Szkolenie

Firma zobowiązuje się do zapewnienia, że jej pracownicy będą odpowiedni przeszkoleni w zakresie obowiązków dot. ochrony danych osobowych. Pracownicy, których stanowiska wymagają regularnego dostępu do danych osobowych lub odpowiedzialni za wdrażanie niniejszej Polityki, lub odpowiadający za odpowiadanie na żądania podmiotów danych dotyczące kwestii objętych tą polityką, otrzymają dodatkowe szkolenie dotyczące ich obowiązków i sposobu ich wypełniania.

18 Konsekwencje postępowania niegodnie z zasadami

18.1 Firma uznaje zgodność z niniejszą Polityką za bardzo ważną. Postępowanie niezgodnie z jej treścią:

18.1.1 naraża podmioty danych, których dane osobowe są przetwarzane; i

18.1.2 stanowi zagrożenie sankcji cywilnych lub karnych dla pracownika i Firmy; i

18.1.3 może w niektórych przypadkach stanowić przestępstwo karne popełnione przez pracownika.

18.2 Postępowanie niezgodnie z treścią tej polityki może skutkować podjęciem czynności dyscyplinarnych względem pracownika zgodnie z obowiązującymi zasadami w firmie, co z kolei może prowadzić do zwolnienia pracownika w przypadku poważnego przewinienia. W przypadku naruszenia polityki przez osobę niebędącą pracownikiem może spowodować

rozwiązanie umowy ze skutkiem natychmiastowym.

18.3 W przypadku pytań lub wątpliwości dotyczących tej polityki należy skontaktować się z reprezentantem krajowym ds. RODO lub działem prawnym.