Procedura ochrony danych w grupie ArcelorMittal

Przetwarzanie informacji dotyczących poszczególnych osób jest przedmiotem uregulowań prawnych w wielu krajach, w których grupa ArcelorMittal prowadzi działalność. Grupa ArcelorMittal potwierdza, że dane osobowe należy traktować z należytą uwagą, bez względu na to, czy są to dane pracowników czy kontrahentów. Z tego względu grupa ArcelorMittal pragnie przyjąć środki praktyczne i prawne mające na celu ochronę danych osobowych przetwarzanych w ramach jej działalności.

Celem niniejszej procedury jest stworzenie jednolitych, adekwatnych i ogólnie obowiązujących standardów ochrony danych oraz spełnienie wymogów prawnych związanych z ochroną danych przy przekazywaniu danych osobowych w ramach Grupy.

Definicje

Definicje

Podmiot zależny

„Podmiot zależy" oznacza każdą spółkę lub podmiot prawny w pełni skonsolidowany i kontrolowany przez spółkę ArcelorMittal S.A. zarejestrowaną w rejestrze handlowym Luksemburga pod numerem B. 82 454.

Pojęcie „kontroli" oznacza posiadanie, bezpośrednio i pośrednio przez jednego lub więcej pośredników, upoważnienie do kierowania lub wytyczania kierunków zarządzania i polityk spółki lub podmiotu prawnego, zarówno w drodze posiadania papierów wartościowych dających prawo głosu, kontraktu czy w inny sposób.

Dane osobowe

"Dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe czy społeczne.

Podmiot danych"Podmiot danych" oznacza każdą osobę fizyczną, której dane osobowe są przetwarzane przez podmiot zależny w kontekście procesu podlegającego zakresowi tej procedury.

Przetwarzanie

"Przetwarzanie" danych osobowych oznacza każdą operację lub zespół operacji wykonywanych na danych osobowych, bez względu na to, czy są to operacje automatyczne, czy

nie, takie jak gromadzenie, zapisywanie, organizowanie, przechowywanie, dostosowanie lub zmiana, odzyskiwanie, konsultacje, wykorzystanie, ujawnienie w drodze przekazu, rozpowszechniania lub innego udostępniania, dostosowanie lub łączenie, blokowanie, usuwanie lub niszczenie;

Specjalne kategorie danych („Dane specjalne")

"Dane specjalne" oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznaniowe lub filozoficzne, przynależność do związków zawodowych i dane dotyczące zdrowia oraz życia seksualnego.

Dane personalne

"Dane personalne" oznaczają wszelkie dane osobowe dotyczące pracowników, kandydatów, stażystów, pracowników tymczasowych i osób, które odeszły z każdego podmiotu zależnego ArcelorMittal.

Globalne narzędzia/bazy danych

"Globalne narzędzia / bazy danych" oznaczają każde narzędzie informatyczne (i) obejmujące dane osobowe (ii) nieograniczone do oddziału, jednostki biznesowej czy segmentu.

Przykład:

One HRIS

Kontroler danych

"Kontroler danych" lub „kontroler" oznacza osobę fizyczną lub prawną, która samodzielnie lub wraz z innymi określa cele i sposoby przetwarzania danych osobowych.

Podmiot przetwarzający

"Podmiot przetwarzający" oznacza podmiot prawny przetwarzający dane osobowe w imieniu kontrolera danych. Pojęcie „podmiot przetwarzający" ma to samo znaczenie jak pojęcie „usługodawca" stosowane powszechnie w ramach grupy ArcelorMittal.

Podmiot ArcelorMittal przetwarzający dane

"Podmiot ArcelorMittal przetwarzający dane" oznacza podmiot przetwarzający będący podmiotem zależnym ArcelorMittal.

Europa („UE")

Europa oznacza 27 państw członkowskich Unii Europejskiej według stanu na listopad 2010 r. plus 3 członków Europejskiego Obszaru Ekonomicznego:

Islandia
Liechtenstein
Norwegia
Austria
Belgia
Bułgaria
Cypr
Czechy
Dania
Estonia
Finlandia
Francja
Niemcy
Grecja
Węgry
Irlandia
Włochy
Łotwa
Litwa
Luksemburg
Malta
Holandia
Polska
Portugalia
Rumunia
Słowacja
Słowenia
Hiszpania
Szwecja
Wielka Brytania

Eksporter danych

"Eksporter danych" oznacza każdy podmiot zależny zlokalizowany w Europie przetwarzający dane osobowe w Europie, przy czym dane osobowe są dalej przekazywane lub udostępnianie podmiotowi zależnemu spoza Europy.

Importer danych

"Importer danych" oznacza każdy podmiot zależny zlokalizowany poza Europą przetwarzający dane osobowe przekazywane lub udostępnianie przez podmiot zależny w Europie.

Warunki niniejszej procedury należy interpretować zgodnie z zapisami Dyrektyw UE 95/46/WE i 2002/58/WE.

Artykuł 1 – Status procedury

Za wdrożenie niniejszej procedury ogólną odpowiedzialność ponosi Zarząd Grupy ArcelorMittal.

Do przestrzegania tej procedury zobowiązani są wszyscy członkowie zarządów, kadra kierownicza i pracownicy ArcelorMittal i podmiotów zależnych ArcelorMittal przetwarzających dane osobowe na całym świecie.

Względem osób naruszających niniejszą procedurę zostaną podjęte kroki dyscyplinarne zgodnie z obowiązującym lokalnie prawem i politykami.

Grupa ArcelorMittal jest świadoma tego, że niektóre przepisy mogą nakładać ostrzejsze regulacje niż te opisane w niniejszej procedurze. W takim przypadku podmioty zależne ArcelorMittal będą postępować z danymi osobowymi zgodnie z prawem lokalnym obowiązującym w miejscu przetwarzania danych osobowych. W przypadku gdy poziom ochrony danych osobowych według prawa lokalnego jest niższy niż opisano w tej procedurze, wówczas obowiązują wymogi określone w tej procedurze.

W celu wykorzystania określonych narzędzi/baz danych zostały i zostaną wypracowane szczegółowe procedury dotyczące prywatności. W przypadku rozbieżności między niniejszą procedurą a daną polityką prywatności, obowiązuje dana polityka prywatności. Narzędzia i bazy danych nieobjęte odrębną polityką prywatności będą podlegać wyłącznie niniejszej procedurze.

Niniejsza procedura została przyjęta w kontekście dyrektywy europejskiej 95/46 jako wiążące reguły korporacyjne ArcelorMittal.

Pytania dotyczące przestrzegania tej procedury i/lub poszczególnych polityk prywatności można kierować do odpowiedniego koordynatora ochrony danych (zob. załącznik VI).

Data wejścia w życie niniejszej procedury dla każdego z podmiotów zależnych jest uzależniona od podpisania formularza procedury o ochronie danych przez ten podmiot zależny.

Artykuł 2 – Zakres procedury

Niniejsza procedura obejmuje:

(i) wszelkie dane osobowe przetwarzane w UE przez lub w imieniu ArcelorMittal, w tym dane osobowe dotyczące pracowników, klientów i dostawców

oraz

(i) wszelkie dane osobowe przetwarzane w UE przez lub w imieniu ArcelorMittal i przekazywane lub udostępniane dalej poza UE, w tym dane osobowe dotyczące pracowników, klientów i dostawców

Niniejsza procedura obejmuje wszystkie osoby, których dane są przetwarzane, bez względu na ich narodowość.

Niniejsza procedura nie obejmuje danych przetwarzanych anonimowo. Dane są traktowane jako anonimowe, jeśli tożsamości osób nie da się już zidentyfikować, ani bezpośrednio, ani pośrednio.

Niniejsza procedura nie obejmuje danych przetwarzanych ab initio lokalnie poza UE przez podmiot zależny i nieprzekazywanych dalej, ani w całości ani w części do kraju członkowskiego UE. Tego typu dane osobowe są przetwarzane zgodnie z prawem lokalnym obowiązującym w miejscu przetwarzania danych osobowych.

Bieżące procesy objęte zakresem są opisane szczegółowo w załączniku VIII do niniejszej procedury.

Artykuł 3 – Zasady przetwarzania danych osobowych

3.1. Kryteria legalności

Dane osobowe będą przetwarzane w oparciu o poniższe przesłanki:

- Podmiot danych w sposób jednoznaczny wyraził na to zgodę; lub
- Przetwarzanie jest niezbędne dla celów realizacji umowy, której stroną jest podmiot danych lub w celu podjęcia kroków na wniosek podmiotu danych przed zawarciem umowy; lub
- Przetwarzanie jest konieczne dla celów spełnienia zobowiązań prawnych kontrolera; lub
- Przetwarzanie jest niezbędne dla ochrony życia lub zdrowia podmiotu danych; lub
- Przetwarzanie jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla realizacji urzędowych uprawnień kontrolera lub strony trzeciej, na rzecz których ujawniane są dane

Dane osobowe można również przetwarzać (i) jeśli któryś z podmiotów zależnych ArcelorMittal jest do tego zobowiązany prawem bądź procesem prawnym (ii) na rzecz organów ścigania lub innych przedstawicieli władzy wykonawczej na podstawie prawomocnego wniosku organów państwowych lub w związku z dochodzeniem dotyczącym domniemanej lub stwierdzonej działalności niezgodnej z prawem (iii) kiedy ujawnienie danych jest konieczne lub stosowne albo ze względu na potencjalny wpływ na interesy życiowe ArcelorMittal lub na dobre imię lub zdrowie fizyczne i psychiczne pracowników.

lub

- Przetwarzanie jest niezbędne dla realizacji prawomocnych celów kontrolera lub strony trzeciej lub stron, którym ujawniane są dane, z wyjątkiem sytuacji, gdy interesy te są podrzędne względem interesów związanych z fundamentalnymi prawami i swobodami podmiotu danych.

3.2. Zasady przetwarzania danych osobowych

Dane osobowe będą przetwarzane w sposób uczciwy i zgodnie z prawem.

Dane osobowe będą zbierane w konkretnych i zgodnych z prawem celach i nie będą dalej przetwarzane w innych celach.

Dane osobowe będą stosowne do celu, a ich zakres nie będzie wykraczać poza cel zbierania i wykorzystywania.

Dane osobowe będą precyzyjne potrzeby aktualizowane. W przypadku niedokładnych lub niepełnych danych osobowych, zostaną podjęte stosowne działania mające na celu ich korektę lub usunięcie.

Dane osobowe będą przechowywane tylko w okresie niezbędnym do celów, jakim służyło ich zbieranie i przetwarzanie, z uwzględnieniem prawnego obowiązku ich zabezpieczania.

Specjalne kategorie danych będą posiadały dodatkowe zabezpieczenia określone w artykule 9 niniejszej procedury.

Do danych osobowych dostęp mogą mieć jedynie te osoby, których funkcja wymaga tego dostępu, z dostępem do danych wymaganych.

Załącznik I zawiera listę pytań ilustrujących powyższe zasady.

Załącznik II zawiera precyzyjne procedury, których należy przestrzegać przy tworzeniu nowego systemu informacyjnego, których celem jest zadbanie o spełnienie tychże zasad.

3.3. Specjalne kategorie danych

Przetwarzanie danych specjalnych jest zabronione z wyjątkiem następujących sytuacji:

- Podmiot danych udzielił jednoznacznej zgodny na przetwarzanie tych danych specjalnych, z wyjątkiem sytuacji, kiedy zabrania tego obowiązujące prawo; lub
- Przetwarzanie jest niezbędne w celu realizacji obowiązków i praw kontrolera w obszarze prawa pracy (np. prawa przeciwdziałającego dyskryminacji) na ile jest to dozwolone prawem krajowym zapewniającym adekwatne zabezpieczenia; lub
- Przetwarzanie jest konieczne w celu ochrony życia lub zdrowia podmiotu danych lub innej osoby, w przypadku gdy podmiot danych nie posiada zdolności fizycznej bądź prawnej do wyrażenia zgody; lub
- Przetwarzanie jest prowadzone w toku działań uprawnionych za odpowiednimi gwarancjami fundacji (takiej jak Fundacja ArcelorMittal), stowarzyszenia lub innej organizacji non-profit, której celem jest promowanie zdrowia i bezpieczeństwa lub odpowiedzialności społecznej i pod warunkiem, że przetwarzanie dotyczy wyłącznie

członków tej organizacji lub osób będących w regularnym kontakcie z organizacją w związku z jej celami i że dane nie będą ujawniane stronom trzecim bez zgody podmiotów danych; lub

- Przetwarzanie dotyczy danych specjalnych ewidentnie upublicznionych przed podmiot danych; lub
- Przetwarzanie danych wrażliwych jest niezbędne dla ustanowienia, wykonania lub obrony roszczeń prawnych; lub
- Przetwarzanie danych wrażliwych jest wymagane dla celów profilaktyki medycznej, diagnostyki medycznej, opieki lub leczenia lub zapewniania opieki zdrowotnej, i w sytuacji gdy te dane wrażliwe są przetwarzane przez pracownika opieki zdrowotnej zgodnie z prawem krajowym lub zasadami ustanowionymi przez kompetentne organy państwowe dotyczącymi obowiązku zachowania tajemnicy zawodowej lub przez inną osobę podlegającą odpowiedniemu obowiązkowi zachowania tajemnicy.

Artykuł 4 – Bezpieczeństwo i poufność

4.1. Podstawowe kontrole bezpieczeństwa informatycznego w ArcelorMittal

Aby zapobiec nieuprawnionemu przetwarzaniu i nieuprawnionej lub przypadkowej utracie, zniszczeniu lub uszkodzeniu danych, jak szczegółowo opisano w załączniku III do tej procedury (podstawowe kontrole bezpieczeństwa informatycznego w ArcelorMittal) zostaną podjęte stosowne kroki techniczne, fizyczne i organizacyjne.

Z uwzględnieniem stanu wiedzy i kosztu wdrożenia, kroki takie powinny zapewnić poziom bezpieczeństwa odpowiedni do zagrożeń wiążących się z przetwarzaniem i rodzajem danych podlegających ochronie.

Wszystkie narzędzia globalne, procesy typowe dla danego segmentu czy aplikacje lokalne podlegające zakresowi niniejszej procedury muszą spełniać wymogi podstawowych kontroli bezpieczeństwa informatycznego w ArcelorMittal.

Aby zapewnić zgodność każdego z przyszłych narzędzi lub procesów z niniejszym standardem, podstawowe kontrole bezpieczeństwa informatycznego w ArcelorMittal będą stanowić część specyfikacji (zob. załącznik II). Każdy konsultant zewnętrzny posiadający dostęp do systemów i narzędzi ArcelorMittal musi się zobowiązać do przestrzegania podstawowych kontroli bezpieczeństwa informatycznego ArcelorMittal.

W razie potrzeby podstawowe kontrole bezpieczeństwa informatycznego ArcelorMittal będą aktualizowane przez komitet ochrony danych.

Stopień ochrony i bezpieczeństwa tak zdefiniowany jest minimalnym standardem, który musi być wdrożony we wszystkich podmiotach zależnych ArcelorMittal. Spółki grupy ArcelorMittal, tam gdzie to stosowne, zachęca się do wprowadzania dodatkowych środków bezpieczeństwa.

Pytania dotyczące przestrzegania podstawowych kontroli bezpieczeństwa informatycznego ArcelorMittal (załącznik III) można kierować do odpowiedniego koordynatora ds. zgodności procedur informatycznych i bezpieczeństwa (“ITCS”, zob. załącznik VI).

4.2. Przypadki naruszenia procedur bezpieczeństwa

Korespondent ds. ochrony danych i/lub ITCS (koordynator ds. zgodności procedur informatycznych i bezpieczeństwa) niezwłocznie poinformują komitet ochrony danych o każdym podejrzeniu lub faktycznym przypadku naruszenia zabezpieczeń lub podobnym zdarzeniu, które zagroziło lub mogło zagrozić poufności lub bezpieczeństwu jakichkolwiek danych osobowych.

Dany podmiot zależny ArcelorMittal podejmie wszelkie działania w celu usunięcia znanego przypadku naruszenia lub jego próby i spowoduje pełną współpracę usługodawców zewnętrznych zgodnie z wytycznymi komitetu ds. ochrony danych. W przypadku wniosku ze strony komitetu ds. ochrony danych, koordynator ochrony danych będzie uczestniczyć w wykrywaniu i identyfikacji przypadków naruszenia zasad bezpieczeństwa.

Dana spółka grupy ArcelorMittal i odpowiedni korespondent ds. ochrony danych będą współpracować w pełni z władzami cywilnymi bądź karnymi podczas dochodzenia lub działań związanych z takim naruszeniem lub jego próbą.

Przypadek naruszenia bezpieczeństwa zostanie następnie udokumentowany przez komitet ochrony danych w celu wyciągnięcia wniosków i stosownej modyfikacji podstawowych kontroli bezpieczeństwa informatycznego (w razie konieczności).

Artykuł 5 – Prawa podmiotów danych

5.1. Kontroler danych

Każdy podmiot zależny ArcelorMittal będzie odpowiadać za przestrzeganie tej procedury.

Każdy podmiot zależny ArcelorMittal jest uznawany za kontrolera swoich danych personalnych, chyba że jest to inaczej określone w danej polityce prywatności lub zatwierdzone przez komitet ochrony danych.

(Jedynie dla informacji: w przypadku systemów informatycznych innych niż systemy kadrowe, za kontrolera uznaje się podmiot prawny działający w charakterze „właściciela biznesowego” zgodnie ze znaczeniem przyjmowanym zwykle przez ArcelorMittal.

5.2. Jawność i prawo do informacji

Niniejsza procedura będzie dostępna do wglądu każdemu podmiotowi danych. Na prośbę zostanie udostępniona jej kopia, w formie elektronicznej lub papierowej.

Podmiot danych otrzyma informację o przekazywaniu i przetwarzaniu jego danych osobowych.

Przed przetwarzaniem danych, podmioty danych otrzymają następujące informacje:

- Dane identyfikacyjne kontrolera (kontrolerów) i osoby go (ich) reprezentującej, jeśli taka istnieje
- Cel, jakiemu ma służyć przetwarzanie danych,
- Inne dodatkowe informacje, takie jak:

i) odbiorców lub kategorie odbiorców danych,

ii) możliwość wglądu w dane i informacja o prawie do modyfikacji danych dotyczących danej osoby.

W przypadku gdy dane nie zostały uzyskane od podmiotu danych, obowiązek informowania podmiotu danych nie ma zastosowania, jeśli przekazanie takiej informacji okaże się niemożliwe lub byłoby związane z nieproporcjonalnym wysiłkiem lub jeśli zapis lub ujawnienie są wyraźnie określone prawem.

5.3. Prawo wglądu do danych, ich modyfikacji, usunięcia lub zablokowania

Każdy podmiot danych ma prawo do otrzymywania bez ograniczeń w rozsądnych odstępach czasu i bez zbędnej zwłoki ani kosztów kopii wszystkich danych dotyczących podmiotu i będących przedmiotem przetwarzania.

Dla wyjaśnienia – podmiot danych nie ma prawa do wglądu w dane osobowe, które go nie dotyczą.

Każdy podmiot danych ma prawo do modyfikacji, usunięcia lub zablokowania danych w szczególności w przypadku gdy dane są niekompletne lub niedokładne.

Każdy podmiot danych może w dowolnym momencie sprzeciwić się przetwarzaniu swoich danych osobowych, gdy jest to uzasadnione jego szczególną sytuacją, chyba że przetwarzanie danych jest wymagane prawem. W przypadku uzasadnionego sprzeciwu, przetwarzanie danych musi się zakończyć.

Każdy podmiot danych ma prawo do nieodpłatnego sprzeciwienia się przetwarzaniu swoich danych personalnych do celów marketingu bezpośredniego.

Podmiot danych może uzyskać wgląd w swoje dane osobowe składając wniosek do odpowiedniego kontrolera danych. Kontroler może odrzucić te wnioski, które w sposób ewidentny są nieuzasadnione.

5.4. Automatyczne podejmowanie decyzji dotyczących osób

Żadna ocena ani decyzja dotycząca podmiotu danych, a mająca nań znaczący wpływ nie będzie opierać się wyłącznie na automatycznym przetwarzaniu danych podmiotu, chyba że decyzja ta:

- będzie podejmowana w toku zawierania lub realizacji umowy, pod warunkiem że wniosek o zawarcie lub realizację umowy, złożony przez podmiot danych, zostanie spełniony lub że będą istniały odpowiednie środki służące ochronie interesu prawnego podmiotu, takie jak ustalenia umożliwiające podmiotowi ujęcie swojego punktu widzenia, lub
- będzie ważna mocą prawa określającego również kroki służące ochronie interesu prawnego podmiotu danych.

Artykuł 6 – Przekazywanie danych

Dane osobowe mogą być przetwarzane przez systemy informatyczne znajdujące się w posiadaniu i pod kontrolą zewnętrznego podmiotu przetwarzającego.

Przed przekazaniem danych osobowych każdemu takiemu usługodawcy, podmiot zależny ArcelorMittal musi wybrać usługodawcę zapewniającego dostateczne gwarancje dotyczące technicznych środków ochrony oraz środków organizacyjnych dla prowadzenia procesu i musi zadbać o przestrzeganie tych środków.

6.1. Przekazywanie danych do zewnętrznego podmiotu przetwarzającego („dostawcy") w UE lub poza UE

Złota zasada nr 1: Żadne dane osobowe podmiotów ArcelorMittal nie będą przekazywane/udostępniane zewnętrznemu podmiotowi przetwarzającemu bez podpisania umowy między podmiotem zależnym ArcelorMittal a zewnętrznym podmiotem przetwarzającym. Umowa taka powinna zawierać standardową klauzulę umowną ujętą w tej procedurze (zob. załącznik V).

Złota zasada nr 2: Żadne dane osobowe podmiotu ArcelorMittal nie będą przekazywane/udostępnianie zewnętrznemu podmiotowi przetwarzającemu, chyba że zapewni on poziom ochrony odpowiadający poziomowi zgodnemu z podstawowymi kontrolami bezpieczeństwa informatycznego ArcelorMittal.

Złota zasada nr 3: W przypadku transferu transgranicznego z Europy do dowolnego kraju spoza Europy, najnowsze standardowe klauzule umowne wymagane legislacją europejską (zestaw standardowych klauzul umownych dla transgranicznego transferu danych osobowych od kontrolera do podmiotu przetwarzającego) lub dowolnym prawem krajowym należy również ująć w umowie podpisanej między danym podmiotem ArcelorMittal a podmiotem przetwarzającym, w przypadku gdy ma to miejsce.

Ocenę bezpieczeństwa opisaną w tej części należy przeprowadzić przed podpisaniem umowy (lub jej przedłużeniem) we wszystkich scenariuszach, w których zewnętrzny podmiot przetwarzający będzie mieć dostęp do jakichkolwiek danych osobowych.

Cel oceny bezpieczeństwa jest następujący: zewnętrzny podmiot przetwarzający musi zapewnić taki sam poziom ochrony danych osobowych ArcelorMittal, jaki został określony w podstawowych kontrolach bezpieczeństwa informatycznego ArcelorMittal.

Przed przekazaniem danych osobowych usługodawcy niebędącego podmiotem ArcelorMittal, podmiot zależny ArcelorMittal jako kontroler danych powinien przedsięwziąć następujące kroki:

→ **Krok 1 : Ocena bezpieczeństwa**

Zainteresowany podmiot zależny ArcelorMittal przedstawi załączony kwestionariusz oceny bezpieczeństwa (załącznik IV) dostawcy pragnącemu świadczyć usługi na rzecz ArcelorMittal.

Odpowiedź dostawcy zostanie oceniona przez koordynatora ds. zgodności z procedurami informatycznymi i bezpieczeństwa dla celów oceny, czy sposób ochrony tak udzielonej odpowiada poziomowi zapewnianemu przez podstawowe kontrole bezpieczeństwa informatycznego ArcelorMittal (załącznik III).

Podczas tej oceny koordynator ds. zgodności z procedurami informatycznymi i bezpieczeństwa powinien otrzymać od podmiotu zależnego ArcelorMittal możliwość rozmowy z dostawcą, zasugerowania usprawnień w środkach bezpieczeństwa dostawcy oraz kontroli jego systemów w celu sprawdzenia, czy dostawca faktycznie zapewnia równoważny poziom ochrony.

W przypadku gdy wynik oceny będzie negatywny ze względu na istnienie krytycznego problemu w politykach dostawcy, proces negocjacyjny zostanie zablokowany a umowa nie zostanie podpisana, chyba że dostawca zobowiąże się do rozwiązania w krótkim okresie problemu (problemów) poruszonego (poruszonych) przez ITCS (koordynatora ds. zgodności z procedurami informatycznymi i bezpieczeństwa).

→ **Krok 2 : Umowa**

W przypadku gdy odpowiedź dostawcy na kwestionariusz oceny bezpieczeństwa zostanie uznana za zadowalającą przez ITCS, odpowiedź ta zostanie ujęta w umowie podpisanej między podmiotem ArcelorMittal a dostawcą. Odpowiedź będzie integralną częścią umowy.

Umowa podpisana między danym podmiotem ArcelorMittal a zewnętrznym podmiotem przetwarzającym będzie również zawierać standardowe klauzule ujęte w tej procedurze (zob. załącznik V). Niemniej jednak w przypadku i w zakresie w jakim prawo ochrony danych nakłada ostrzejsze zobowiązania w kwestii takich umowy, obowiązywać będzie prawo ochrony danych, tak że standardowe klauzule ujęte w załączniku V a sprzeczne z prawem ochrony danych zostaną zastąpione nowymi klauzulami zgodnymi z prawem ochrony danych.

W przypadku transferu transgranicznego z Europy do dowolnego kraju spoza Europy, najnowsze standardowe klauzule umowne wymagane legislacją europejską (zestaw standardowych klauzul umownych dla transgranicznego transferu danych osobowych od kontrolera do podmiotu przetwarzającego) lub dowolnym prawem krajowym należy również ująć w umowie podpisanej między danym podmiotem zależnym ArcelorMittal a podmiotem przetwarzającym, w przypadku gdy ma to miejsce.

6.2. Przekazanie danych do podmiotu przetwarzającego ArcelorMittal

Każdy podmiot przetwarzający ArcelorMittal musi spełniać wymogi podstawowych kontroli bezpieczeństwa informatycznego ArcelorMittal.

Podstawowe kontrole bezpieczeństwa informatycznego ArcelorMittal są automatycznie ujmowane w każdej umowie podpisanej przez jakikolwiek podmiot ArcelorMittal przetwarzający dane i jego klientów (tj. kontrolerów danych).

Cel przetwarzania danych przez podmiot przetwarzający ArcelorMittal w imieniu klienta zostanie ustalony wspólnie na piśmie między podmiotem ArcelorMittal przetwarzającym dane a klientem ArcelorMittal. Podmiot ArcelorMittal przetwarzający dane nie będzie przetwarzać danych osobowych w żadnym innym celu. Podmiot ArcelorMittal przetwarzający dane przekaże dane osobowe jedynie zgodnie z wytycznymi pisemnymi otrzymanymi od klienta.

Podczas podzlecania części wszystkich usług zewnętrznemu podmiotowi przetwarzającemu, podmiot ArcelorMittal przetwarzający dane spełni wymogi procesu opisane w części 6. powyżej.

6.3. Przekazywanie danych zewnętrznemu kontrolerowi danych

Każde przekazanie danych osobowych z Europy zewnętrznemu kontrolerowi danych spoza UE musi być zgodne z europejskimi zasadami dotyczącymi transgranicznego przepływu danych (artykuły 25-26 dyrektywy 95/46/WE: na przykład z wykorzystaniem standardowych klauzul umownych UE zatwierdzonych przez Komisję Europejską 2001/497/WE lub 2004/915/WE lub innych odpowiednich środków umownych zgodnie z artykułami 25 i 26 dyrektywy UE).

6.4. Przekazywanie danych nowemu podmiotowi zależnemu ArcelorMittal

Przekazanie danych osobowych nowemu podmiotowi zależnemu ArcelorMittal nie może nastąpić przed (i) podpisaniem tej procedury przez taki nowy podmiot i (ii) wyznaczeniem koordynatora ochrony danych, jeśli nie ma takiego w danym kraju/segmencie.

Artykuł 7 – Wdrożenie niniejszej procedury i mechanizmy jej egzekwowania

- Zachowanie zgodności z przepisami na poziomie lokalnym/regionalnym (koordynator ochrony danych i ITCS)
- Komitet ochrony danych ArcelorMittal
- Program szkoleniowy
- Wewnętrzny mechanizm składania zażaleń
- Program audytów
- Wzajemna pomoc i współpraca z organami ochrony danych
- Działania w przypadku prawa krajowego uniemożliwiającego przestrzeganie niniejszej procedury

7.1. Zachowanie zgodności z przepisami na poziomie lokalnym/regionalnym (koordynator ochrony danych i ITCS)

Koordynator ochrony danych

Każda osoba na stanowisku Country Manager lub Segment Manager wyznaczy jednego lub kilku koordynatorów ochrony danych. Każdemu koordynatorowi ochrony danych zostanie przypisany konkretny obszar geograficzny i/lub organizacyjny.

Koordynator ochrony danych będzie zajmować się koordynacją wszelkich działań mających na celu spełnienie przez podmioty zależne zobowiązań w ramach niniejszej procedury w odpowiadającym im zakresie.

Koordynator ochrony danych będzie również podstawową osobą do kontaktu w przypadku zażaleń zgłaszanych w jego zakresie zgodnie z częścią 7/4 niniejszej procedury (Wewnętrzny mechanizm składania zażaleń) i w przypadku wszelkich naruszeń bezpieczeństwa opisanych w części 4.2 niniejszej procedury (naruszenie bezpieczeństwa).

Koordynator ochrony danych jest zobowiązany do pełnej współpracy z osobami na równoważnych stanowiskach w kwestiach dotyczących właściwej realizacji niniejszej procedury, w szczególności w kwestiach dotyczących lub wpływających na kilku kontrolerów danych w różnych krajach/regionach.

Koordynator ochrony danych będzie na bieżąco informować komitet ds. ochrony danych o wszelkich zażaleniach lub innych kwestiach/problemach objętych zakresem tej procedury.

W przypadku gdy koordynator ochrony danych nie wypełni swoich zobowiązań może zostać usunięty przez komitet ochrony danych. W takim przypadku nowego koordynatora ochrony danych wyznaczy Country Manager lub zarząd lokalny.

Zespół zgodności z procedurami informatycznymi i bezpieczeństwa (ITCS)

Misją koordynatorów ds. zgodności z procedurami informatycznymi i bezpieczeństwa jest określenie, wprowadzenie i monitorowanie wdrożenie wewnętrznego systemu kontroli w ramach pionu informatyki ArcelorMittal, wymaganego dla osiągnięcia celów tego obszaru w dziedzinie zgodności z przepisami i bezpieczeństwa.

Koordynatorzy ds. zgodności z procedurami informatycznymi i bezpieczeństwa w szczególności będą wprowadzać i monitorować wdrożenie podstawowych kontroli bezpieczeństwa ArcelorMittal zarówno wewnętrznie jak i w odniesieniu do zewnętrznych podmiotów przetwarzających dane sprawdzając równoważny minimalny poziom bezpieczeństwa określony w części 6.1 niniejszej procedury.

7.2. - Komitet ochrony danych ArcelorMittal

Komitet ochrony danych będzie funkcjonować w okresie obowiązywania tej procedury.

Komitet ochrony danych będzie obejmował trzech (3) podstawowych członków,

- Jednego (1) wyznaczonego przez dyrektora informatyki Grupy ArcelorMittal,
- Jednego (1) wyznaczonego przez wiceprezesa wykonawczego Grupy (EVP) ds. personalnych i
- sekretarza, wyznaczonego przez radcę prawnego Grupy ArcelorMittal.

Pierwsi członkowie komitetu ochrony danych są wymienieni w załączniku IX.

Komitet ochrony danych będzie również obejmować wszystkich lub niektórych koordynatorów ochrony danych, zgodnie z decyzją członków podstawowych, dla efektywnego omawiania punktów porządku obrad.

Ponadto w posiedzeniach komitetu ochrony danych może wedle własnego uznania brać udział szef audytu wewnętrznego ArcelorMittal lub osoba przez niego wyznaczona.

Każdy członek wedle własnego uznania może zapraszać innych członków lub konsultantów do udziału w posiedzeniach komitetu ochrony danych. Dla jasności żaden zaproszony konsultant nie będzie podejmować decyzji i nie będzie uznawany za członka komitetu ochrony danych ArcelorMittal.

Dyrektor informatyki Grupy, wiceprezes wykonawczy Grupy ds. personalnych i radca prawny Grupy mogą wycofać mianowanie dla każdego z członków przez siebie wyznaczonych i mianować zastępstwo (ze skutkiem natychmiastowym) w dowolnym momencie, informując o wycofaniu i zastępstwie pozostałych członków.

Komitet ochrony danych będzie spotykać się w takich terminach i miejscach jakie okresowo ustalą jego członkowie, ale nie rzadziej niż raz na trzy (3) miesiące.

Porządek obrad każdego posiedzenia będzie ustalany przez sekretarza i przekazywany członkom komitetu ochrony danych oraz koordynatorom ochrony danych.

W ciągu trzech (3) dni roboczych od każdego posiedzenia komitetu ochrony danych jego sekretarz przygotuje i roześle członkom komitetu szczegółową notatkę pisemną na temat decyzji podjętych podczas posiedzenia.

Notatka ta zostanie również przekazana koordynatorom ochrony danych.

Komitet ochrony danych będzie:

(i) prowadzić i aktualizować listę podmiotów zależnych ArcelorMittal podlegających niniejszej procedurze,

(ii) prowadzić i aktualizować listę koordynatorów ochrony danych zgodnie z wnioskami składanymi przez menedżerów ArcelorMittal na poziomie lokalnym/ regionalnym (zob. pierwszą listę w załączniku VI),

(iii) nadzorować wdrożenie tej procedury i jej realizacji przez podmioty zależne, w tym przyszłe podmioty zależne ArcelorMittal,

(iv) rozwiązywać wszelkie ważniejsze kwestie / problemy, jakie się pojawią,

(v) inicjować, zatwierdzać i aktualizować poszczególne polityki dotyczące narzędzi globalnych (żadna polityka tego typu nie wejdzie w życie bez wcześniejszej zgody komitetu ochrony danych),

(vi) mieć pełne prawo do aktualizacji załącznika II i załączników III, IV, V, VI, VII i VIII. O zmianach zostaną powiadomieni koordynatorzy ochrony danych i ITCS (koordynator ds. zgodności z procedurami informatycznymi i bezpieczeństwa), a zaczną one obowiązywać w dniu określonym w powiadomieniu. Przykładowo, przewiduje się, że pojawi się konieczność zmiany standardowej klauzuli dotyczącej usługodawców zewnętrznych w załączniku V dostosowującej klauzulę do prawa krajowego i jego zmian w poszczególnych krajach.

(vii) modyfikować procedurę w zależności od potrzeb, na przykład w celu dostosowania do zmian w prawie, przepisach, praktykach i procedurach ArcelorMittal, strukturze korporacyjnej ArcelorMittal lub wymogów nałożonych przez organy ochrony danych. O zmianach w tym podstawowym dokumencie zostaną powiadomione podmioty zależne ArcelorMittal; jeśli podmiot zależny nie odrzuci tych zmian wyraźnie na piśmie, przyjmuje się, że zostały zaakceptowane przez każdy z podmiotów po upływie dwóch (2) miesięcy.

(viii) dbać o to, by zmiany w tym dokumencie podstawowym i zmiany w wykazie podmiotów zależnych ArcelorMittal podlegających tej procedurze zostały przekazane organom ochrony danych udzielającym pozwoleń z krótkim wyjaśnieniem powodów zmian.

(ix) prowadzić rejestr wszystkich wersji tej procedury

7.3 Szkolenia

Pracownikom mającym stały bądź regularny dostęp do danych osobowych, zaangażowanych w gromadzenie danych osobowych lub w tworzenie narzędzi stosowanych do przetwarzania danych osobowych zostanie zapewnione odpowiednie szkolenie z niniejszej procedury.

Za szkolenie będzie odpowiadać koordynator ochrony danych; szkolenie może mieć formę szkolenia online.

7.4 Wewnętrzny mechanizm składania zażaleń

Każdy podmiot danych może złożyć zażalenie związane z nieprzestrzeganiem niniejszej procedury przez któregoś kontrolera danych ArcelorMittal.

Koordynator ochrony danych danego kontrolera danych ArcelorMittal będzie odpowiadać za terminową obsługę takiego zażalenia. Pierwsza odpowiedź zostanie przekazana wnoszącemu zażalenie w ciągu jednego (1) miesiąca od jej złożenia. Następnie koordynator ochrony danych dołoży wszelkich starań w celu terminowego rozpatrzenia zażalenie z uwzględnieniem jego złożoności i zakresu. Zakłada się, że okres rozpatrywania wyniesie od jednego (1) do sześciu (6) miesięcy z wyjątkiem okoliczności niezwykłych i wyjątkowych.

W przypadku gdy koordynator ochrony danych nie będzie w stanie rozwiązać problemu, kwestia taka zostanie przez niego przekazana komitetowi ochrony danych ArcelorMittal.

Podmiot danych może w dowolnym terminie złożyć zażalenie odpowiednim organom ochrony danych lub wnieść sprawę sądową przed sądem właściwym dla eksportera danych znajdującego się w UE.

7.5 Plan audytów

Przestrzeganie tej procedury przez Grupę będzie podlegać regularnej kontroli przez dział audytu wewnętrznego. Audyty będą odbywać się nie rzadziej niż dwa razy w roku. Dział audytu wewnętrznego może korzystać ze wsparcia członka komitetu ochrony danych. Można również wyznaczyć zespół zewnętrzny.

Audyt taki może obejmować wszystkie aspekty tej procedury, zarówno w Europie jak i poza nią.

Z każdego audytu zostanie przygotowany raport obejmujący w razie konieczności szczegółowe działania korygujące (faza 1). Działania te zostaną podjęte przez podmiot(y) ArcelorMittal w określonym terminie określonym w raporcie. Następnie zostanie przeprowadzona ponowna wizyta w celu potwierdzenia, że wszystkie działania korygujące zostały podjęte (faza 2).

Dział audytu wewnętrznego i komitet ochrony danych ustalą roczny plan audytów.

Kopie wszystkich raportów z audytów zostaną przekazane (i) odpowiedniemu koordynatorowi (koordynatorom) ochrony danych, (ii) komitetowi ochrony danych, (iii) wiceprezesowi Grupy ds. personalnych, dyrektorowi informatyki Grupy i radcy prawnemu Grupy (iv) zarządowi danego podmiotu zależnego.

Organy ochrony danych mogą uzyskać dostęp do raportów z audytu po złożeniu o to wniosku.

Raporty z audytów nie będą w żaden sposób przekazywane organom bądź osobom niewymienionym w tej część dokumentu 7.5 (“Plan audytów”).

7.6. Wzajemna pomoc i współpraca z organami ochrony danych

- Podmioty zależne będą ze sobą współpracować i wspierać się nawzajem w rozpatrywaniu wniosków lub zażaleń ze strony podmiotu danych lub w przypadku dochodzenia lub zapytania ze strony organów ochrony danych.
- W przypadku naruszenia niniejszej procedury poza Europą, organy ochrony danych w kraju, w którym znajduje się eksporter danych, mogą poprosić o przeprowadzenie audytu przez dział audytu wewnętrznego ArcelorMittal. Audyt taki zostanie przeprowadzony zgodnie z częścią 7.5 niniejszej procedury.
- Podmioty zależne będą stosować się do zaleceń organów ochrony danych w kwestiach dotyczących interpretacji tej procedury.

7.7 Działania w przypadku przepisów krajowych uniemożliwiających przestrzeganie niniejszej procedury.

W przypadku gdy podmiot zależny ma powody, by sądzić, że obowiązujące go przepisy uniemożliwiają kontrolerowi danych realizację obowiązków w ramach niniejszej procedury i że mają znaczący wpływ na gwarancje określone w tej procedurze, niezwłocznie poinformuje komitet ochrony danych (z wyjątkiem sytuacji, gdy jest to zakazane przez organ ścigania, np. zachowanie w poufności dochodzenia karnego prowadzonego przez organy ścigania).

Ponadto, w przypadku konfliktu między prawem krajowym a zobowiązaniami określonymi w tej procedurze, komitet ochrony danych podejmie odpowiedzialną decyzję dotyczącą działań do podjęcia, a w przypadku wątpliwości skonsultuje się z organami ochrony danych.

Artykuł 8 - Odpowiedzialność

Każdy podmiot danych może domagać się przestrzegania poniższych zasad jako praw przed odpowiednim organem ochrony danych lub sądem dla dochodzenia zadośćuczynienia i uzyskania odszkodowania w przypadku nieprzestrzegania tych zasad przez któryś podmiot zależny:

- Przepisów krajowych uniemożliwiających przestrzeganie niniejszej procedury, zgodnie z zapisami części 7.7 niniejszej procedury,
- Prawa do składania zażaleń w ramach wewnętrznego mechanizmu składania zażaleń opisanego w części 7.4,
- Obowiązków związanych ze współpracą z organem ochrony danych zgodnie z częścią 7.6,
- Zapisów dotyczących odpowiedzialności i właściwości sądu zgodnie z następną częścią i częścią 7.4;
- Ograniczeń dotyczących przeznaczenia danych, zgodnie z częścią 3.2,
- Jakości i proporcjonalności danych, zgodnie z częścią 3.2,
- Kryteriów legalności przetwarzania zgodnie z częścią 3.1,
- Jawności i łatwego dostępu do niniejszej procedury, zgodnie z częścią 5.2,
- Prawa do wglądu, modyfikacji, usuwania lub blokowania danych i sprzeciwu wobec przetwarzania, zgodnie z częścią 5.3,
- Praw w przypadku podejmowania automatycznych decyzji dotyczących poszczególnych osób, zgodnie z częścią 5.4,
- Bezpieczeństwa i poufności, zgodnie z częścią 4,
- Ograniczeń dotyczących dalszego transferu poza grupę spółek, zgodnie z częścią 6.1 i częścią 6.3.

Każdy podmiot ArcelorMittal przyjmuje na siebie odpowiedzialność za każde naruszenie tej procedury niezależnie od mechanizmu odpowiedzialności solidarnej opisanego w art. 8.2.

Podmiot danych może w dowolnym terminie złożyć zażalenie odpowiednim organom ochrony danych lub wnieść sprawę sądową przed sądem właściwym dla eksportera danych znajdującego się w UE.

Prawa te nie obejmują elementów tej procedury dotyczących mechanizmów wewnętrznych wdrożonych przez podmioty zależne, takich jak szczegóły szkoleń, audytów, dane osób odpowiedzialnych za przestrzeganie i mechanizm aktualizacji zasad.

8.1. Obowiązek eliminacji przypadków naruszeń

Jeśli któryś z podmiotów zależnych ArcelorMittal narusza niniejszą procedurę, ma obowiązek eliminacji takiego naruszenia i podjęcia niezbędnych działań mających na cel spełnienie wymogów tej procedury.

Podmioty zależne zgadzają się na konieczność eliminacji naruszenia, zaniedbania czy niezgodności z niniejszą procedurą, tak by do danego problemu nie dochodziło ponownie w przyszłości.

8.2. Obowiązek wypłaty odszkodowania na rzecz podmiotu danych

Ponadto każdy podmiot danych, który doznał szkody w wyniku naruszenia ośmiu (8) wyżej wymienionych praw podmiotu danych ma prawo do otrzymania odszkodowania za doznaną szkodę.

W przypadku gdy podmiot naruszający znajduje się poza Europą, zastosowanie mają poniższe zasady:

- podmiot naruszający i eksporter danych ponoszą odpowiedzialność solidarną za szkody wyrządzone podmiotowi danych w wyniku naruszenia zapisów niniejszej procedury.
- podmiot naruszający zwróci eksporterowi wszelkie poniesione koszty, opłaty, odszkodowania, wydatki czy straty.
- jeśli eksporter danych jest w stanie dowieść, że członek spoza Europy nie ponosi odpowiedzialności za naruszenie, może zostać zwolniony z wszelkiej odpowiedzialności.

ZAŁĄCZNIK I

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

LISTA KONTROLNA

Celem niniejszej listy kontrolnej jest zilustrowanie sposobu rozumienia zasad dotyczących ochrony danych.

„Dane osobowe będą przetwarzane w sposób uczciwy i zgodny z prawem."

- Czy istnieje faktyczna przyczyna biznesowa przetwarzania tych informacji?
- Czy osoby, o których informacje posiadam, są tego świadomi i czy zrozumieją, do czego te informacje będą wykorzystywane?
- Czy muszę informować organ ochrony danych, a jeśli tak, czy moje zawiadomienie jest aktualne?

„Dane osobowe będą zbierane w określonych i zgodnych z prawem celach i nie będą dalej przetwarzane w innych celach."

- Czy wiem, w jakim celu będę wykorzystywać te dane osobowe?
- Jeśli ktoś mnie poprosi o przekazanie danych personalnych, czy osoby, których dane posiadam, oczekiwałyby, że to zrobię?

„Dane osobowe będą stosowne do celu i nie będą wykraczać poza cele ich gromadzenia i wykorzystywania."

- Czy rzeczywiście potrzebuję tych informacji na temat danej osoby?

„Dane osobowe będą dokładne i w razie potrzeby aktualizowane. Niedokładne lub niepełne dane osobowe będą poprawiane lub usuwane w rozsądnym zakresie."

- Czy mam pewność, że informacje personalne są dokładne i aktualne?

„Dane osobowe będą przechowywane tylko w okresie niezbędnym do celów, jakim służyło ich zbieranie i przetwarzanie, z uwzględnieniem obowiązku prawnego dotyczącego zachowywania danych."

- Czy usuwam lub niszczę informacje osobowe, gdy tylko nie są mi już dłużej potrzebne?

"Dane wrażliwe będą dodatkowo zabezpieczone zgodnie z wymogami dyrektywy unijnej 95/46/WE"

- Czy moim pracownikom zapewniono szkolenie dotyczące ich obowiązków i zadań zgodnie z procedurą ochrony danych ArcelorMittal i czy wdrażają je w życie?

„Do danych osobowych dostęp mogą mieć jedynie te osoby, których funkcja obejmuje obsługę tych danych, z dostępem do danych wymaganych."

- Czy dostęp do danych osobowych jest ograniczony do tych, którzy mają ścisłą potrzebę ich znajomości?
- Czy satysfakcjonuje mnie bezpieczeństwo przechowywania tych informacji?

ZAŁĄCZNIK II

KONTROLA OCHRONY DANYCH PRZED ZAKOŃCZENIEM FAZY PROJEKTOWEJ ZADANIA

Faza projektowa każdego zadania ma kluczowe znaczenie dla zapewnienia, że powstały proces/aplikacja będę zgodne z niniejszą procedurą. „Faza projektowa" oznacza fazę, w której zespół projektowy w imieniu kontrolera (kontrolerów) definiuje architekturę, specyfikację i funkcjonalności systemu.

Zasady określone w niniejszej procedurze należy zintegrować z każdym nowym systemem informatycznym lub jego znacząca zmianą już na etapie projektowania.

Niniejszy ZAŁĄCZNIK opisuje sposób osiągnięcia tego celu.

Tytułem wstępu warto wspomnieć, że niniejsza procedura jest neutralna z punktu widzenia technologii. W przypadku gdy istniejący system został niedawno zmieniony z wykorzystaniem nowej technologii przy zachowaniu tych samych procesów, danych, środków organizacyjnych i zabezpieczeń, konieczne będzie przestrzeganie zaleceń podanych w momencie projektowania istniejącego systemu, niemniej jednak w przypadku takiej zmiany nie będzie konieczny nowy punkt kontrolny ochrony danych.

Niniejszy ZAŁĄCZNIK dotyczy wszelkich nowych systemów informatycznych mieszczących się w ramach niniejszej procedury i wszelkich ich zmian (pod warunkiem jednak, że sposób przetwarzania danych osobowych się zmieni).

- Nowe narzędzie globalne

Zespół projektowy jest zobowiązany do konsultacji z komitetem ochrony danych przed zatwierdzeniem projektu każdego nowego narzędzia globalnego.

Komitet ochrony danych będzie służyć zespołowi projektowemu radą i pomocą, dbając o to, by projekt systemu był zgodny z niniejszą procedurą.

W każdym przypadku w specyfikacji należy ująć podstawowe kontrole bezpieczeństwa informatycznego (zob. ZAŁĄCZNIK III).

- Procesy typowe dla segmentu

Przed zatwierdzeniem projektu każdego nowego procesu typowego dla segmentu zespół projektowy musi skonsultować się z koordynatorami ochrony danych.

Koordynatorzy ochrony danych będą służyć zespołowi projektowemu radą i pomocą, dbając o to, by projekt systemu był zgodny z niniejszą procedurą.

W każdym przypadku w specyfikacji należy ująć podstawowe kontrole bezpieczeństwa informatycznego (zob. ZAŁĄCZNIK III).

W przypadku gdy nowy system ma wykorzystywać dane osobowe z narzędzia lub procesu już istniejącego, zespół projektowy również skonsultuje się z komitetem ochrony danych.

- Lokalne aplikacje komputerowe

Przed zatwierdzeniem projektu systemu należy skonsultować się z koordynatorem ochrony danych w danym kraju.

Koordynator ochrony danych będzie służyć zespołowi projektowemu radą i pomocą, dbając o to, by projekt systemu był zgodny z niniejszą procedurą.

W każdym przypadku podstawowe kontrole bezpieczeństwa informatycznego (zob. ZAŁĄCZNIK III) zostaną ujęte w specyfikacji.

W przypadku gdy nowa aplikacja ma korzystać z danych osobowych pobranych z systemu istniejącego należy również skonsultować się z komitetem ochrony danych.

Zasada ta może obejmować różne działania w zależności od szczególnego przypadku czy aplikacji. Na przykład w niektórych przypadkach może wymagać eliminacji/redukcji danych osobowych lub uniemożliwienia zbędnego przetwarzania lub poprawy zabezpieczeń w celu spełnienia wymogów podstawowych kontroli bezpieczeństwa informatycznego.

Kontroler (kontrolerzy) będzie (będą) odpowiadać za przełożenie zaleceń koordynatora ochrony danych na rzeczywistość systemu.

Najnowsza wersja zasad: http://www..... Intranet ArcelorMittal

ZAŁĄCZNIK III

PODSTAWOWE KONTROLE BEZPIECZEŃSTWA INFORMATYCZNEGO

Najnowsza wersja polityk: http://www..... Intranet ArcelorMittal

ZAŁĄCZNIK IV

KWESTIONARIUSZ OCENY BEZPIECZEŃSTWA (SAQ)

Najnowsza wersja kwestionariusza: http://www..... Intranet ArcelorMittal

SCHEDULE V

Standardowa klauzula umowna grupy ArcelorMittal dotycząca zewnętrznych podmiotów przetwarzających dane

Niniejsza klauzula jest OBOWIĄZKOWA i musi znaleźć się we wszystkich umowach zawieranych przez podmiot zależny ArcelorMittal jako kontrolera danych i zewnętrznego przetwarzającego działającego jako wykonawca, któremu podmiot zależny ArcelorMittal ujawni dane osobowe podlegające zakresowi tej procedury drogą usystematyzowanego przepływu europejskich danych osobowych z podmiotu zależnego ArcelorMittal do zewnętrznego podmiotu przetwarzającego w celu realizacji zamierzeń umownych.

Przyjmuje się, że umowa biznesowa zawierająca tę klauzulę w sposób jasny opisuje (i) ogólny cel umowy, (ii) usługi, jakie mają być świadczone i (iii) dane do przekazania lub udostępnienia przetwarzającemu.

Niniejszy załącznik zawiera również wersję klauzuli dla Niemiec (zob. poniżej).

Ochrona danych

"Dane osobowe" oznaczają wszelkie dane dotyczące określonej lub możliwej do zidentyfikowania osoby (i) dostarczane przez ArcelorMittal lub dowolny podmiot zależny ArcelorMittal, wchodzące w posiadanie dostawcy lub podmiotu zależnego dostawcy zgodnie z tą umową (ii) stworzone na podstawie lub wynikające z danych dostarczonych przez ArcelorMittal lub dowolny podmiot zależny ArcelorMittal zgodnie z tą umową (iii) wygenerowane automatycznie w ramach usług dostarczanych przez dostawcę na rzecz ArcelorMittal.

[ArcelorMittal jest i pozostanie kontrolerem danych, a dostawca będzie działać wyłącznie jako przetwarzający dane w odniesieniu do danych osobowych] (*). Dostawca nie będzie przetwarzać żadnych danych osobowych (w tym danych przetworzonych początkowo przez ArcelorMittal), chyba że będzie działać w celu dostarczenia usług opisanych w tej umowie. Dostawca dołoży wszelkich starań, by zapewnić rzetelność wszystkich pracowników dostawcy mających dostęp do danych osobowych lub odpowiedzialnych za ich przetwarzanie.

W momencie rozwiązania lub wygaśnięcia tej umowy lub na pisemny wniosek ze strony ArcelorMittal dostawca: (i) niezwłocznie zaprzestanie przetwarzać dane osobowe; i (ii) zwróci ArcelorMittal dane osobowe i wszystkie ich kopie, notatki na ich podstawie sporządzone i wyciągi z tych danych lub, w zależności od decyzji ArcelorMittal, zniszczy te dane w ciągu siedmiu (7) dni roboczych od dnia rozwiązania lub wygaśnięcia niniejszej umowy lub otrzymania takiego wniosku. Na wniosek ArcelorMittal dostawca potwierdzi również w formie pisemnej, że spełnił zobowiązania określone w tej klauzuli.

Dostawca będzie zawsze przestrzegać polityk bezpieczeństwa informatycznego (**) dołączonych do tej umowy oraz odpowiednich przepisów i uregulowań dotyczących ochrony danych (przepisy dotyczące ochrony danych). W przypadku i w zakresie jakim przepisy dotyczące ochrony danych nakładają na dostawcę ostrzejsze zobowiązania, w tym ściślejsze środki ochrony niż przewiduje niniejsza umowa, obowiązują przepisy dotyczące ochrony danych.

Dostawca nie będzie w żaden sposób przekazywać danych osobowych żadnej stronie trzeciej, w tym żadnemu podmiotowi lub podwykonawcy dostawcy (podwykonawcy podmiotu przetwarzającego) bez wcześniejszej pisemnej zgody ze strony ArcelorMittal, którą to zgodę ArcelorMittal może wycofać z dowolnego powodu lub bez powodu wedle własnego uznania. Przed zwróceniem się o zgodę ArcelorMittal dostawca poda ArcelorMittal wszystkie szczegóły dotyczące zaangażowania proponowanego podwykonawcy podmiotu przetwarzającego, między innymi jego dane identyfikacyjne, dane dotyczące bezpieczeństwa danych, lokalizację obiektów, w których będą przetwarzane dane, opis propozycji dostępu do danych ArcelorMittal i wszelkie inne informacje, jakich w rozsądnym zakresie może domagać się ArcelorMittal w celu oceny ryzyka związanego z dopuszczeniem podwykonawcy podmiotu przetwarzającego do przetwarzania danych osobowych. Jako warunek wyrażenia zgody na każdą propozycję podwykonawcy podmiotu przetwarzającego, ArcelorMittal może wymagać od dostawcy zawarcia pisemnej umowy z podwykonawcą-podmiotem przetwarzającym określającej warunki równoważne z tą umową (pod warunkiem, że dostawca nie będzie uprawniony do wyrażenia zgody dla podwykonawcy-podmiotu przetwarzającego dane na dalsze podzlecanie bądź inne delegowanie całości lub części przetwarzania przez podwykonawcę-podmiot przetwarzający bez wcześniejszej pisemnej zgody ArcelorMittal, wedle uznania ArcelorMittal).

W każdym przypadku dostawca doprowadzi do tego, by upoważniony przez niego podwykonawca-podmiot przetwarzający spełniał pod każdym względem zobowiązania związane z ochroną danych ujęte w tej umowie oraz wszelkie odpowiednie przepisy dotyczące ochrony danych.

Dla spełnienia wymogów dyrektywy europejskiej 95/46 ArcelorMittal może wymagać od dostawcy realizacji dodatkowych warunków, w tym między innymi wykonania standardowych klauzul umownych celem przekazania informacji osobowych do krajów trzecich zgodnie z dyrektywą 95/46/WE, a dostawca powinien je spełnić.

Dostawca przekaże ArcelorMittal wszelkie reporty z audytu wystawione przez dział audytu wewnętrznego dostawcy dotyczące w części lub w całości usług świadczonych na rzecz ArcelorMittal.

Ponadto dostawca poinformuje na piśmie koordynatora ds. zgodności z procedurami informatycznymi i bezpieczeństwa na temat każdego przypadku naruszenia bezpieczeństwa lub takiego podejrzenia, co do naruszenia, które zagroziło lub mogło zagrozić poufności lub bezpieczeństwu jakichkolwiek danych ArcelorMittal

(w tym danych osobowych) w ciągu dwudziestu czterech (24) godzin od momentu wystąpienia takiego naruszenia lub jego podejrzenia. Zawiadomienie takie będzie zawierać opis wszystkich już podjętych kroków i kroków, które dostawca podejmie w celu zaradzenia naruszeniu lub podejrzeniu naruszenia.

Dostawca służyć pełnym wsparciem ArcelorMittal w zakresie udzielania odpowiedzi na wszelkie wnioski podmiotu danych dotyczące dostępu do jego danych osobowych. W przypadku gdy podmiot danych będzie wymagać bezpośrednio od dostawcy dostarczenia informacji dotyczących swoich danych osobowych, dostawca niezwłocznie przekaże taką prośbę ArcelorMittal i nie będzie udzielać odpowiedzi podmiotowi danych bez odpowiedniego wniosku ze strony ArcelorMittal.

Dostawca będzie pomagać ArcelorMittal w spełnieniu wymogów rejestracyjnych lub innych wymaganych zgodnie z przepisami o prywatności i ochronie danych, w tym między innymi w dostarczaniu wnioskowanych informacji i rejestracji u organów ochrony danych lub w udziale w programach samorządów gospodarczych zgodnie z wnioskiem ArcelorMittal.

Komentarze:

W powyższym zapisie umownym „dostawca" oznacza podmiot przetwarzający a „ArcelorMittal" oznacza dany podmiot zależny ArcelorMittal. W razie potrzeby treść powyższych klauzul można dostosować do treści umowy, bez wpływu na poziom zobowiązania zewnętrznego podmiotu przetwarzającego.

Umowa podpisana między podmiotem zależnym ArcelorMittal a zewnętrznym podmiotem przetwarzającym musi również zawierać klauzulę o prawie do audytu. Zgodnie z tą klauzulą podmiot zależny ArcelorMittal będzie mieć prawo do skontrolowania, czy dostawca spełnia wymogi podstawowych kontroli bezpieczeństwa informatycznego ArcelorMittal w okresie obowiązywania umowy.

(*) Niniejszy *[zapis]* musi być ujęty jedynie wtedy, gdy podmiot prawny ArcelorMittal podpisujący umowę znajduje się w Europie. Niniejszy zapis obowiązuje jedynie dla prawa europejskiego.

(**) Polityki bezpieczeństwa informatycznego wymienione w trzecim akapicie wynikają z oceny bezpieczeństwa. W większości przypadków będą mieć formę polityk bezpieczeństwa dostawcy, ewentualnie zmodyfikowanych dla spełnienia wymogów podstawowych kontroli bezpieczeństwa informatycznego ArcelorMittal.

Najnowsza obowiązująca wersja klauzul: http://www..... intranet ArcelorMittal

ZAŁĄCZNIK VI

UWAGA: Ze względów bezpieczeństwa ZAŁĄCZNIK VI pozostanie pusty w wersji opublikowanej poza ArcelorMittal. ZAŁĄCZNIK VI będzie ujęty w kopii procedury umieszczonej w intranecie.

Koordynatorzy ochrony danych

Ostatnia aktualna wersja listy: http://www.....arcelormittal Intranet

Koordynatorzy ds. zgodności z procedurami informatycznymi i bezpieczeństwa (ITCS)

Ostatnia aktualna wersja listy: http://www.....arcelormittal Intranet

ZAŁĄCZNIK VII

Kwestionariusz audytu

Audyt zgodności z procedurami dotyczącymi ochrony danych

Lista kontrolna

Nazwa aplikacji / bazy danych oprogramowania

Cel(e) aplikacji

Nazwisko/dział osoby odpowiedzialnej za aplikację
. Aspekty informatyczne
. aspekty funkcjonalne

Kim są podmioty danych?
(wszyscy pracownicy AM? czy określona kategoria pracowników AM? klienci AM? ...)

Ile podmiotów danych obejmuje proces?
(w przybliżeniu)

Jakiego rodzaju dane osobowe obejmuje proces?
(zrzuty z ekranu)

Czy są wśród nich dane wrażliwe?
Skąd pochodzą dane?
(Innymi słowy, jakie jest (są) źródło (źródła) danych?) Bezpośrednio od podmiotów danych? Skąd?)

Jak długo dane będą przechowywane?

Kto ma dostęp do danych?
. w ramach AM
. poza AM

Dostęp do danych: Skąd? Czy dochodzi do transgranicznego transferu danych?

Czy prowadzona jest migracja danych/są one wykorzystywane przez inną aplikację?

Jeśli tak: jaką aplikację?

Prawo podmiotu danych do dostępu do własnych danych: w jaki sposób podmiotom danych przekazywane są informacje na temat ich prawa do wglądu do swoich danych?

Czy w proces zaangażowana jest jakaś strona trzecia (w ramach lub poza AM)?

Jeśli tak: w jakim celu (np. hosting...) ?

Czy informacja trafiła do aplikacji (jeśli powinna) ?

Jakie zabezpieczenia są stosowane?

Najnowsza obowiązująca wersja kwestionariusza: http://www.....arcelormittal Intranet

ZAŁĄCZNIK VIII

Opis przetwarzania danych

Kategorie danych

Dane personalne

Dane biznesowe

Dane informatyczne

Dane związane ze społeczną odpowiedzialnością biznesu

Dane BHP

Podmioty danych

Większość podmiotów danych, których dane są przetwarzane, to pracownicy ArcelorMittal.

Oprócz pracowników ArcelorMittal podmioty danych, których dane są przetwarzane przez ArcelorMittal to:

. Przedstawiciele klientów (ArcelorMittal prowadzi transakcje z przedsiębiorstwami, w swojej bazie klientów nie posiada konsumentów indywidualnych)

. Przedstawiciele dostawców

. Wykonawcy pracujący w imieniu ArcelorMittal

. Strony zainteresowane w otoczeniu przedsiębiorstwa

Dane personalne

Cele transferu/przetwarzania danych

Dział personalny i zarządzania personelem obejmujący rekrutację, dostarczanie wynagrodzenia, zarządzanie ścieżką kariery i umiejętnościami, szkolenia (e-learning), administrację świadczeniami pracowniczymi, ocenę wyników pracowników, tworzenie książek adresowych pracowników, przestrzeganie obowiązujących wymogów prawnych.

Dane biznesowe (dane osobowe dotyczące klientów, dostawców i wszelkiego rodzaju kontrahentów).

Osoby te funkcjonują jako osoby do kontaktu z ArcelorMittal po stronie danej firmy, reprezentujące tę firmę.

Cele transferu/przetwarzania danych

Zarządzanie i ocena procesu biznesowego, w tym działalność sprzedażowa, zakupowa, księgowa, kontrolingowa, zarządzanie majątkiem spółki, przestrzeganie obowiązujących wymogów prawnych.

Zarządzanie infrastrukturą informatyczną, w tym pocztą e-mail, dostępem do intranetu ArcelorMittal, wykorzystaniem wspólnych narzędzi i ogólnie zarządzanie dostępem użytkownika do aplikacji informatycznych;

Dane związane ze społeczną odpowiedzialnością biznesu

Cele transferu/przetwarzania danych

Odpowiedzialność społeczna, w tym zrozumienie otoczenia, w jakim działamy i interesów stron zainteresowanych, zarządzanie stałym programem ArcelorMittal mającym na celu zaangażowanie na rzecz społeczności lokalnych.

Dane dotyczące zdrowia i ochrony

Cele transferu/przetwarzania danych

: Procesy BHP to działania mające na celu zapewnienie bezpieczeństwa i ochrony pracowników i zasobów ArcelorMittal. Przykłady to ochrona bezpieczeństwa i higieny pracy oraz potwierdzanie statusu pracownika w celu zgody na dostęp do zasobów i obiektów ArcelorMittal.

ZAŁĄCZNIK IX

UWAGA: Ze względów bezpieczeństwa ZAŁĄCZNIK VI zostanie pusty w wersji upublicznionej poza ArcelorMittal. ZAŁĄCZNIK VI będzie ujęty w kopii procedury umieszczonej w intranecie.

Komitet ochrony danych

. [nazwisko 2]

Pierwszymi członkami komitetu ochrony danych wyznaczonymi przez wiceprezesa wykonawczego Grupy ds. personalnych są:

. [nazwisko 2]

Sekretarz: Emmanuel CAUVIN