Ogólna polityka prywatności UE

Grupa Bondioli & Pavesi

Spis treści

1. WSTĘP

Grupa Bondioli & Pavesi przywiązuje dużą wagę do przestrzegania przepisów dotyczących ochrony prywatności i danych osobowych w celu prawidłowego rozwoju swojej działalności, biznesu i wizerunku na rynku. Ochrona danych osobowych, które każda spółka grupy gromadzi i przechowuje, za pomocą systemów elektronicznych lub tradycyjnych, stanowi istotną i strategiczną wartość dla grupy i dla rozwoju działalności.

Mając to na uwadze, rozporządzenie (UE) 2016/679 (zwane dalej również **RODO/GDPR**) stanowi istotę nowych europejskich przepisów dotyczących ochrony danych i jest główną podstawą działań dotyczących danych osobowych w UE.

Z tego powodu niezbędne jest przyjęcie wspólnej polityki prywatności (zwanej dalej **Polityką**) dla spółek zlokalizowanych na terenie UE wskazanych w punkcie 3 (zwanych dalej, każdą z osobna **Spółką**, a łącznie **Grupą UE**) oraz poinformowanie wszystkich pracowników i osób pracujących w imieniu i na rzecz poszczególnych spółek o zasadach i regułach, którymi Grupa UE zamierza się kierować w celu zapewnienia jednolitego i wysokiego poziomu ochrony danych osobowych.

W świetle złożoności przepisów z jednej strony, a z drugiej strony procesów korporacyjnych obejmujących dane osobowe, konieczne jest przede wszystkim przyjęcie struktury zarządzania prywatnością w spółkach Grupy UE, określając strukturę ról, odpowiedzialności i zadań związanych z ochroną danych osobowych.

2. CEL

Niniejsza Polityka ma na celu opisanie:

(i). zasad i procedur, których każda Spółka musi przestrzegać przy przetwarzaniu danych osobowych,
(ii). organizacji ochrony danych i jej zarządzania oraz
(iii). przydziału zadań i obowiązków na różnych poziomach operacyjnych.

Z tego powodu Polityka musi być podana do wiadomości wszystkich osób, które przetwarzają dane osobowe w Spółce.

3. ZAKRES STOSOWANIA

Niniejsza Polityka musi być przestrzegana przez następujące Spółki:

- wszystkie włoskie spółki Grupy Bondioli & Pavesi;
- Bondioli & Pavesi GMBH;
- Bondioli & Pavesi France SA;
- Bondioli & Pavesi Iberica SA;
- Bondioli & Pavesi Sp. z o.o.
- OM Protivin AS.

Każda z nich, oprócz przestrzegania poniższej polityki, musi oczywiście przestrzegać RODO/GDPR oraz lokalnych przepisów uzupełniających dotyczących prywatności i ochrony danych osobowych.

4. DEFINICJE

Dla celów niniejszej polityki podano następujące definicje zaczerpnięte z RODO/GDPR w kolejności odpowiadającej ich znaczeniu:

- **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;
  Ponadto, w przypadku działań marketingowych, o które nie prosił odbiorca (np. spontaniczne wysyłanie materiałów reklamowych, sprzedaż bezpośrednia, badania rynku lub powiadomienia handlowe), również wszelkie informacje dotyczące osoby prawnej - w tym organów lub stowarzyszeń.
  Należą do nich na przykład: dane osobowe, adresy pocztowe, telefoniczne i telematyczne, kody identyfikacyjne, zamówienia, obroty, wizerunek, głos, życiorys, zwyczaje zakupowe, rejestry dostępu do systemu oraz, bardziej ogólnie, wszystko, co jest zapisane na papierze lub w komputerze i może być powiązane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą.

- **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.
  Należą do nich na przykład: zarządzanie listą płac i obecnością pracowników, zarządzanie umowami, wysyłanie komunikatów marketingowych, profilowanie, nadzór wideo itp.

- **Specjalne kategorie danych osobowych:** dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych i biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Jest to podzbiór danych osobowych.
  Należą do nich na przykład: zaświadczenia lekarskie, przynależność do związków zawodowych, urlopy okolicznościowe, niepełnosprawność, kontuzje, przynależność partyjna, stan zdrowia itp.

- **Dane osobowe dotyczące wyroków skazujących i czynów zabronionych**: (dalej **dane karne**) to dane dotyczące wyroków skazujących i czynów zabronionych lub związanych z nimi środków bezpieczeństwa. Jest to podzbiór danych osobowych.

- **Administrator danych:** osoba fizyczna lub prawna, organ publiczny, służba lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. *Na przykład, jeśli strona internetowa jest zarządzana w całości przez Bondioli & Pavesi S.p.A., za przetwarzanie danych z nią związanych będzie odpowiedzialny ten sam podmiot.*
  Każda spółka, która samodzielnie decyduje, w jaki sposób będzie dokonywać przetwarzania danych jest administratorem danych. Na przykład przetwarzanie danych pracowników oznacza, że poszczególne Spółki są odpowiedzialne za to przetwarzanie.

- **Przetwarzający dane**: oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora, zgodnie z art. 28 RODO/GDPR.

- **Osoba upoważniona do przetwarzania danych**: osoba fizyczna, która przetwarza dane osobowe pod bezpośrednim zwierzchnictwem administratora lub przetwarzającego dane;

- **Osoba, której dane dotyczą** Zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna, do której odnoszą się dane osobowe. Ponadto, w przypadku działań marketingowych, które nie zostały zamówione przez odbiorcę (np. spontaniczne wysyłanie materiałów reklamowych, sprzedaż bezpośrednia, badania rynku lub komunikacja handlowa), osobą, której dane dotyczą jest również osoba prawna - w tym organy lub stowarzyszenia - zgodnie z dyrektywą (UE) o prywatności i łączności elektronicznej 2002/58 wraz z późniejszymi uzupełnieniami i zmianami. *Są to na przykład: klienci, w tym potencjalni, pracownicy, kandydaci do pracy, konsultanci, dostawcy, goście, użytkownicy stron internetowych administratora danych, itp.*

5. MODEL ORGANIZACYJNY OCHRONY DANYCH W GRUPIE UE

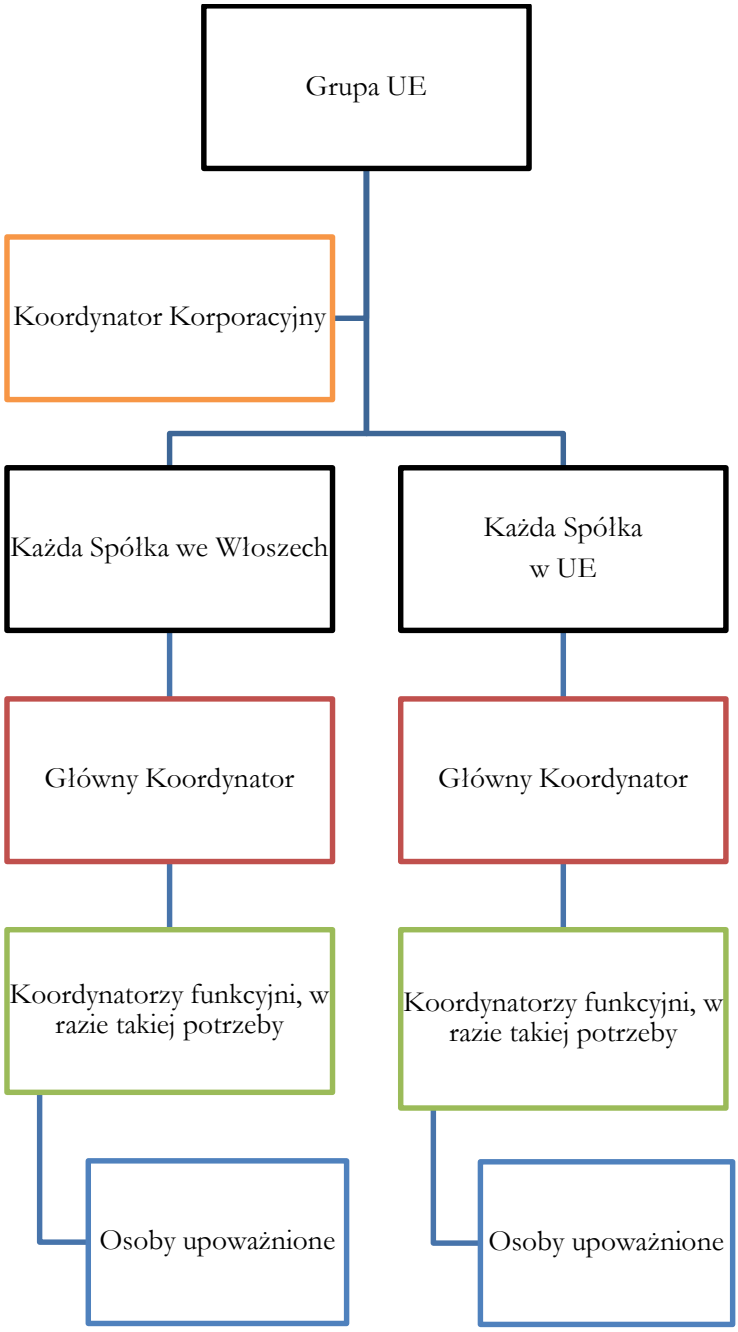
W celu ujednolicenia działań wewnętrznych w zakresie ochrony danych osobowych, Grupa UE zdecydowała się przyjąć następujący model organizacyjny:

- **Koordynator Korporacyjny**: ma za zadanie koordynować kwestię ochrony danych na poziomie całej grupy UE i udzielać wskazówek funkcjonalnych wszystkim osobom kontaktowym ds. ochrony danych wyznaczonym w ramach grupy UE. Szczegółowe informacje na temat zakresu odpowiedzialności i przydzielonych zadań można znaleźć w dokumencie PRCY011 dostępne w firmowym intranecie;
- **Główny Koordynator**: ma on za zadanie koordynować temat ochrony danych na poziomie pojedynczej Spółki, która go powołała, rozpatrując go w całości, oraz udzielać wskazówek wszystkim Koordynatorom Funkcyjnym, którzy mogą być powołani w ramach tej samej Spółki Szczegóły dotyczące obowiązków i przydzielonych zadań można znaleźć w dokumencie PRCY014 dostępne w firmowym intranecie;

- **Koordynator Funkcyjny:** ma za zadanie koordynować temat ochrony danych na poziomie przydzielonego mu działu w Spółce, która go wyznaczyła. Szczegółowe informacje na temat zakresu odpowiedzialności i przydzielonych zadań można znaleźć w dokumencie PRCY015 dostępne w firmowym intranecie. Ten Koordynator jest powoływany tylko, jeżeli uzna to za konieczne Główny Koordynator.
- **Osoba upoważniona / wyznaczona:** osoba fizyczna, która materialnie wykonuje operacje przetwarzania danych, za pomocą narzędzi komputerowych i / lub za pomocą nośników papierowych w ramach działu firmy, do którego jest przypisana. Każda Spółka musi wyznaczyć jako Osobę Upoważnioną każdego ze swoich pracowników, którzy przetwarzają dane osobowe w ramach wykonywania swoich obowiązków. Dokument powołujący na Osobę Upoważnioną wraz z określeniem zakresu dozwolonego przetwarzania danych, udzielonymi instrukcjami i powierzonymi zadaniami znajduje się **PRCY016** dostępne w firmowym intranecie.

6. SCHEMAT ORGANIZACJI OCHRONY DANYCH UE

W związku z powyższym, schemat organizacji ochrony danych osobowych przedstawia się następująco:



7. INNE PODMIOTY UCZESTNICZĄCE

W zarządzanie danymi osobowymi mogą być zaangażowane inne podmioty, w tym:

- **Przetwarzający dane**: jak już widzieliśmy, jest to strona zewnętrzna, która przeprowadza przetwarzanie danych osobowych w imieniu administratora danych. Takie przetwarzanie musi odbywać się na podstawie pisemnej umowy określającej przedmiot umowy, czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa administratora danych. W kontekście UE taka umowa musi również zawierać istotne elementy określone w art. 28 ust. 3 RODO/GDPR.

Usługi, które zazwyczaj mogą być zlecane Przetwarzającym to na przykład: zarządzanie listą płac, zarządzanie stroną internetową, zarządzanie wsparciem IT, itp.

- **IOD/DPO**: Inspektor Ochrony Danych/Data Protection Officer, to osoba przewidziana przez RODO/GDPR w art. 37 i następnych, którą spółka musi wyznaczyć w przypadku, gdy:
  - podstawowa działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych na dużą skalę; lub
  - główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu, na dużą skalę, szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO/GDPR lub danych dotyczących wyroków skazujących i przestępstw, o których mowa w art. 10 RODO/GDPR.

  Do głównych zadań należy nadzorowanie zgodności z RODO/GDPR, doradzanie spółce, monitorowanie działań, zapewnianie szkoleń i podnoszenie świadomości w tym zakresie itp.

  Powołanie IOD/DPO zostało uznane za zbędne w przypadku Spółek, ponieważ, biorąc pod uwagę ich typową działalność, która ze swej natury nie pociąga za sobą żadnego ryzyka w dziedzinie ochrony danych osobowych, uwzględniając minimalne przetwarzanie danych osobowych osób, których dane dotyczą, z pewnością nie na dużą skalę, oraz biorąc pod uwagę fakt, że przetwarzanie szczególnych kategorii danych w ramach stosunku pracy nie stanowi działalności podstawowej, lecz pomocniczą (zob. Grupa Robocza Art. 29, Wytyczne dotyczące IOD/DPO, 2.1.2., s. 9), nie wydaje się, by powyższe warunki były spełnione.
  Jeśli lokalne wytyczne lub przepisy wymagają wyznaczenia IOD/DPO w jednej ze spółek (innej niż włoska), okoliczność ta musi zostać zgłoszona z wyprzedzeniem Koordynatorowi Korporacyjnemu.

- **Inne potencjalne podmioty:** lokalne przepisy mogą wymagać określenia innych podmiotów istotnych dla ochrony danych osobowych. Każda Spółka ma obowiązek rozważyć, czy istnieją lokalne przepisy nakładające takie obowiązki.
  We Włoszech, na przykład, istnieją administratorzy systemu, którzy są osobami fizycznymi odpowiedzialnymi za techniczne zarządzanie całym systemem informatycznym lub nawet tylko jednym z jego elementów lub związanych z nim działań. Osoby takie muszą zostać specjalnie wyznaczone na administratora systemu oraz otrzymać specjalne instrukcje.

8. ZASADY OGÓLNE

W związku z przetwarzaniem danych osobowych, Grupa UE zamierza przyjąć wszelkie środki technologiczne, organizacyjne i logistyczne, które są najbardziej odpowiednie do zapewnienia skutecznego przestrzegania gwarancji ochrony danych osobowych.
W tym celu procedury firmowe i operacje przetwarzania danych wykonywane przez pracowników, upoważnionych do przetwarzania, muszą być zgodne z poniższymi zasadami.

8.1. **Zgodność z prawem, rzetelność i przejrzystość**

Przetwarzanie danych osobowych może odbywać się tylko wtedy, gdy spełniony jest jeden z warunków przewidzianych przez prawo, tylko jeżeli dana osoba o tym wie i odpowiada to temu, co zostało jej zadeklarowane.

8.2. **Ograniczenie celu**

Dane osobowe mogą być przetwarzane wyłącznie do celów zadeklarowanych osobie, której dane dotyczą, i nie mogą być niezgodne z tymi celami.

8.3. **Minimalizacja**

Wykorzystanie danych osobowych musi być ograniczone do minimum i dlatego, jeżeli cele mogą być osiągnięte bez wykorzystania danych osobowych, przetwarzanie musi odbywać się z wykorzystaniem danych anonimowych. Dane anonimowe to dane, których w żaden sposób nie można powiązać ze zidentyfikowaną lub możliwą do zidentyfikowania osobą, której dane dotyczą. W szczególności, dane osobowe muszą być adekwatne, właściwe i ograniczone do tego, co niezbędne w związku z celami, dla których są przetwarzane.

8.4. **Prawidłowość**

Przetwarzane dane muszą być prawidłowe i aktualizowane, a osoba, której dane dotyczą, musi mieć możliwość sprawdzenia i skorygowania ich.

8.5. **Ograniczenie przechowywania**

Przetwarzane dane osobowe nie powinny być przechowywane przez czas nieokreślony. Muszą być usuwane po osiągnięciu celu, dlatego każda spółka musi określić czas przechowywania zgodny z celem i zgodny z lokalnymi przepisami.

8.6. **Integralność i poufność**

Każda Spółka musi przetwarzać dane osobowe w taki sposób, aby zapewnić odpowiednie bezpieczeństwo i poufność, w tym zapobiegać nieuprawnionemu dostępowi do danych osobowych i do sprzętu używanego do ich przetwarzania lub wykorzystywania.

8.7. **Rozliczalność**

Każda Spółka musi zapewnić zgodność z powyższymi zasadami i musi być w stanie wykazać taką zgodność.

9. ZASADY POSTĘPOWANIA

W zastosowaniu zasad opisanych powyżej oraz dalszych norm przewidzianych przez RODO/GDPR, każda Spółka będzie działać zgodnie z następującymi zasadami postępowania.

9.1. **Rejestry czynności przetwarzania**

Każda Spółka, poprzez swoich Koordynatorów, musi przechowywać dowody przetwarzania, zarówno skomputeryzowanego jak i ręcznego, dokonywanego wewnętrznie przez różne działy Spółki. Każda Spółka musi wypełnić ten obowiązek poprzez sporządzenie rejestrów czynności

przetwarzania, o których mowa w art. 30 RODO/GDPR, przestrzegając wskazówek udzielonych w tym zakresie w każdym kraju przez lokalne organy nadzorcze.
Odpowiedzialność za zapewnienie, że każda Spółka posiada dokumentację wymaganą przez RODO/GDPR i że jest ona stale aktualizowana, spoczywa na Głównym Koordynatorze, który w tym celu musi zdefiniować konkretną procedurę zarządzania, określającą obowiązki i zadania w ramach Spółki oraz, jeśli wyznaczenia, angażującą Koordynatorów Funkcjonalnych.
Rejestry muszą być aktualizowane co najmniej raz w roku.

9.2. **Informacje i gromadzenie danych (*przejrzystość i rzetelność*)**

Co do zasady, dane osobowe są przekazywane bezpośrednio przez zainteresowanych w ramach normalnych kontaktów służbowych oraz w ramach realizacji działań operacyjnych Spółki lub za pośrednictwem strony internetowej, ale mogą być również pozyskiwane od osób trzecich. Pracownicy, którzy zbierają dane osobowe od osoby, której dane dotyczą, muszą zadbać o to, aby podczas zbierania danych osoba, której dane dotyczą, została odpowiednio poinformowana o celach, dla których dane są zbierane, a następnie przetwarzane.
W tym celu muszą dostarczyć odpowiedni dokument informacyjny przygotowany przez Spółkę.
Informacja ta jest zawsze należna, nawet jeśli nie jest konieczne zwracanie się do osoby zainteresowanej o zgodę na przetwarzanie jej danych.
Czynności, o których nie poinformowano lub które nie są opisane w samych informacjach, są niezgodne z prawem i dlatego nie mogą być przeprowadzane.
Powiadomienie (informacja) musi być dostarczone jednorazowo i musi poprzedzać pierwsze pobranie danych od osoby, której dane dotyczą.
W przypadku zmiany któregokolwiek z elementów wskazanych w poprzednim powiadomieniu przedstawia się nowe powiadomienie.

9.3. **Warunki zgodności z prawem przetwarzania**

Dla każdego celu wymienionego w informacji należy wskazać co najmniej jedną podstawę prawną, która czyni przetwarzanie danych zgodnym z prawem.
Podstawami prawnymi są te wskazane w art. 6 RODO/GDPR dla zwykłych danych osobowych, które składają się, w skrócie, z następujących, alternatywnych elementów:

- Zezwolenie
- Wykonanie umowy
- Wykonanie obowiązku prawnego
- Ochrona żywotnych interesów
- Zadanie leżące w interesie publicznym
- Uzasadniony interes (który nie jest nadrzędny w stosunku do praw danej osoby)

W odniesieniu do przetwarzania szczególnych kategorii danych podstawy prawne są określone w art. 9 RODO/GDPR i art. 10 w odniesieniu do danych karnych i są bardziej restrykcyjne niż w przypadku zwykłych danych.

9.4. **Zgoda osoby, której dane dotyczą (zgodność z prawem)**

Wśród podstaw prawnych zgodności z prawem jest wymieniona zgoda osoby, której dane dotyczą. Zgoda nie musi być zbierana, jeżeli przetwarzanie opiera się na jednym z pozostałych warunków

zgodności z prawem (jak określono w poprzednim punkcie). Jednakże niektóre operacje przetwarzania danych wymagają zgody jako warunku zgodności z prawem. Operacje przetwarzania muszą być zgodne z tą zgodą udzieloną przez osobę, której dane dotyczą, w odpowiedzi na zawiadomienie informacyjne. Zgoda musi być dobrowolnie wyrażona przez daną osobę, musi być uzyskana dopiero po udzieleniu odpowiednich informacji oraz musi być wyraźna i jednoznaczna.
Jeżeli zgoda jest konieczna do przeprowadzenia przetwarzania, nie może ono zostać przeprowadzone bez jej uzyskania.

9.5. **Dostępność danych i dozwolone działania dla personelu**

Dostęp do danych osobowych i wykonywanie czynności przetwarzania jest dozwolone tylko osobom, które zostały należycie upoważnione i otrzymały odpowiednie instrukcje. Osoby upoważnione do przetwarzania danych będą miały dostęp do danych wyłącznie na zasadzie *need to know* (wiedzy koniecznej). Dane muszą być wykorzystywane wyłącznie w celu realizacji powierzonych zadań i obowiązków.
Jak wskazano powyżej, podkreślamy fakt, że:

- czynności, o których nie poinformowano lub które nie są opisane w samych informacjach nie mogą być przeprowadzane;
- przetwarzanie, na które nie uzyskano wymaganej zgody, nie jest dozwolone.

9.6. **Dostęp do specjalnych kategorii danych i danych dotyczących wyroków skazujących, czynów zabronionych i działania dozwolone dla pracowników**

Takie dane mogą być przetwarzane tylko przez osoby upoważnione do przetwarzania, które mają ścisłą potrzebę, niezbędną do wykonywania swoich obowiązków i specjalnie upoważnione.
Poza opisanymi powyżej ograniczeniami dotyczącymi potrzeby informacji i ewentualnej zgody, należy zauważyć, że operacje przetwarzania takich danych muszą być również zgodne z warunkami i ograniczeniami określonymi przez przepisy lokalne.
Na przykład we Włoszech warunki i ograniczenia są określone w ogólnych zezwoleniach wydanych przez rzecznika ds. ochrony danych, które można znaleźć na stronie internetowej (www.garanteprivacy.it).
Dlatego nie wolno przeprowadzać czynności przetwarzania, które nie są zgodne z lokalnymi przepisami.

9.7. **Środki bezpieczeństwa**

Wszystkie osoby upoważnione są zobowiązane do przestrzegania przepisów bezpieczeństwa opracowanych przez Spółkę, których nieprzestrzeganie może pociągać za sobą poważne konsekwencje prawne, niekiedy nawet o charakterze karnym. Przestrzeganie określonych środków bezpieczeństwa zależy wyłącznie od postępowania osób upoważnionych.

9.8. **Obieg danych i przekazywanie danych stronom trzecim**

Dane osobowe mogą być przekazywane w ramach Spółek Grupy UE osobom upoważnionym, które muszą je znać w celach służbowych (*need to know*) i które otrzymały stosowne instrukcje. Natomiast nie mogą być przekazywane - ani w żadnym wypadku udostępniane - osobom trzecim spoza Grupy UE, z wyjątkiem jednego z następujących przypadków:

- przekazanie danych stronie trzeciej jest konieczne w celu spełnienia obowiązku prawnego lub nakazu władz publicznych;
- przekazanie danych stronie trzeciej jest konieczne do wykonania zobowiązań wynikających z umowy zawartej z osobą, której dane dotyczą;
- jeśli osoba trzecia została wyznaczona jako Przetwarzający dane, zgodnie z art. 28 RODO/GDPR, a dane są niezbędne do wykonania zleconej usługi;
- osoba, której dane dotyczą, wyraźnie wyraziła zgodę na przekazanie tych danych danej stronie trzeciej.

Każda potrzeba przekazania danych stronie trzeciej z powodów innych niż wymienione powyżej musi uzyskać pisemne upoważnienie od Głównego Koordynatora Spółki.

W każdym razie, nie jest polityką Grupy UE, aby z jakiegokolwiek powodu i w jakimkolwiek celu przekazywać listy, spisy lub adresy w formie marketingu danych osobowych.

9.9. **Nowe przetwarzanie i przetwarzanie obarczone wysokim ryzykiem**

Bez uprzedniej autoryzacji nie można rozpocząć nowych operacji przetwarzania, które wiążą się z wysokim ryzykiem, określonym i uregulowanym w polityce firmy dotyczącej oceny wpływu planowanego przetwarzania na ochronę danych osobowych *(Impact Assessment* lub **DPIA**). Główne elementy podlegające ocenie, które mogą pociągać za sobą wysokie ryzyko dla osób, których dane dotyczą, są następujące:

- ocena punktowa lub profilowanie
- zautomatyzowany proces podejmowania decyzji wywołujący skutki prawne lub w podobny sposób znacząco wpływający na osoby
- regularne monitorowanie;
- przetwarzanie szczególnych kategorii danych
- przetwarzanie danych na dużą skalę
- tworzenie dopasowań lub łączenie zestawów danych
- przetwarzanie danych dotyczących osób wymagających szczególnej troski
- innowacyjne wykorzystanie lub zastosowanie nowych rozwiązań technologicznych lub organizacyjnych
- przetwarzanie, które samo w sobie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub skorzystanie z usługi lub umowy

Oprócz tych elementów, lokalne przepisy mogą przewidywać dodatkowe przypadki ryzyka lub przypadki, w których DPIA jest obowiązkowa. We Włoszech rzecznik ds. ochrony danych nakazał, aby ocena DPIA była obowiązkowa w wielu przypadkach, w tym na przykład w przypadku nie okazjonalnego przetwarzania danych dotyczących osób szczególnej troski, systematycznego przetwarzania danych biometrycznych itp.

9.10. **Naruszenie danych osobowych (*Data breach*)**

Naruszenie danych osobowych definiuje się jako "naruszenie bezpieczeństwa, które przypadkowo lub bezprawnie powoduje zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do

danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" (zwane dalej również ***Data Breach***).

W przypadku naruszenia danych osobowych, należy obowiązkowo powiadomić organ nadzorczy (lokalnego rzecznika) w ciągu 72 godzin od powzięcia informacji o naruszeniu.

Grupa UE przyjęła politykę zarządzania naruszeniami danych, która musi być znana i rozumiana przez wszystkie osoby upoważnione, które po wystąpieniu opisanej sytuacji muszą niezwłocznie zgłosić ten fakt stosownemu Koordynatorowi funkcyjnemu w swoim departamencie lub, jeżeli takowego nie ma, Głównemu Koordynatorowi w celu dotrzymania terminów zgłoszeń.

9.11. ***Privacy by design* i *by default***

Grupa UE przyjęła politykę *privacy by design* i *privacy by default*, której należy przestrzegać przy opracowywaniu nowych aplikacji i nowych operacji przetwarzania danych i o której należy poinformować wszystkie osoby zaangażowane w projektowanie i opracowywanie takich aplikacji i operacji przetwarzania danych.

9.12. **Zarządzanie prawami osób, których dane dotyczą**

Rozporządzenie RODO/GDPR przyznaje podmiotom danych następujące prawa:

- Prawo dostępu do własnych danych osobowych (art. 15)
- Prawo do sprostowania (art. 16);
- Prawo do usunięcia danych („prawo do bycia zapomnianym) (art. 17);
- Prawo do ograniczenia przetwarzania danych (art. 18);
- Prawo do przenoszenia danych (art. 20);
- Prawo do wyrażenia sprzeciwu (art. 21);
- Prawo do sprzeciwu wobec decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu danych (art. 22);
- Prawo do cofnięcia w dowolnym momencie udzielonej zgody, bez uszczerbku dla zgodności z prawem przetwarzania opartego na zgodzie udzielonej przed jej cofnięciem (art. 7.3);

Grupa UE przyjęła politykę zarządzania wnioskami o skorzystanie z powyższych praw, ilustrując jej treść. Polityka ta musi być znana i możliwa do poznania przez każdą osobę zaangażowaną w proces rozpatrywania takich wniosków. Należy pamiętać, że w przypadku braku prawidłowego rozpatrzenia wniosków, o których mowa w polityce, osoba zainteresowana ma prawo do złożenia reklamacji u rzecznika ds. ochrony danych lub podjęcia kroków prawnych w celu ochrony swoich praw.

10. SZKOLENIE

Rozporządzenie RODO/GDPR wymaga, aby osoby przetwarzające dane były świadome ryzyka związanego z przetwarzaniem danych osobowych. Każda spółka musi zatem zapewnić, aby osoby upoważnione były świadome swoich obowiązków poprzez zapewnienie im odpowiedniego szkolenia, zgodnego z powierzonym zadaniem.

Szkolenie nie może być wydarzeniem jednorazowym, lecz musi być powtarzane okresowo, szczególnie w przypadku zmian w przepisach lub nowych wytycznych interpretacyjnych.

Do celów szkoleniowych mogą być również udostępniane dokumenty i prezentacje wyjaśniające główne aspekty prawodawstwa, programy e-learningowe, wykłady w aulach, seminaria komunikacyjne itp.

Działalność szkoleniowa musi być udokumentowana (zgodnie z zasadą rozliczalności). Każdy pracownik jest zobowiązany do pogłębiania swojej wiedzy w tym zakresie, aby działać w pełnej zgodności z przepisami, niniejszą Polityką oraz instrukcjami wydanymi w zakresie przetwarzania danych. Wszelkie potrzeby w zakresie dalszych szkoleń należy zgłaszać koordynatorom funkcyjnym (lub, w przypadku ich braku, głównemu koordynatorowi), którzy będą musieli podjąć działania w związku z tymi wnioskami.

11. OKRESOWE KONTROLE

Każda Spółka, realizując swoje zobowiązania wynikające z RODO/GDPR, organizuje okresowe audyty, w tym za pośrednictwem wyznaczonych w niej koordynatorów (Głównego Koordynatora i ewentualnych Koordynatorów Funkcjonalnych), dotyczące zgodności z postanowieniami RODO/GDPR, przepisami lokalnymi oraz politykami Grupy UE, a także wydanymi instrukcjami dotyczącymi przetwarzania danych. Kontrole muszą być udokumentowane. Osoby upoważnione do przetwarzania powinny w pełni współpracować w celu ułatwienia przeprowadzania audytów.

12. SANKCJE

Częściowe lub całkowite naruszenie postanowień przepisów o ochronie danych osobowych może skutkować sankcjami karnymi, cywilnymi i administracyjnymi za bezprawne przetwarzanie danych lub przetwarzanie niezgodne z przedmiotowymi przepisami.
Przypomina się, że w najpoważniejszych przypadkach, grzywna administracyjna stosowana zgodnie z art. 83 ust. 5 RODO/GDPR może wynosić do 20 000 000 EUR, a w przypadku przedsiębiorstw - do 4 % całkowitego rocznego obrotu firmy z poprzedniego roku, w zależności od tego, która z tych kwot jest wyższa.

Zachowanie niezgodne z prawem lub postępowanie niezgodne z niniejszą Polityką, politykami Grupy UE oraz wydanymi instrukcjami dotyczącymi przetwarzania danych osobowych może skutkować podjęciem działań dyscyplinarnych współmiernych do wagi zaistniałych faktów.

*** *** ***