Informacja na temat ochrony danych osobowych przetwarzanych przez Balticus S.A

Z dniem 25 maja 2018 roku weszły w życie przepisy ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, inaczej RODO).

Prowadząc korespondencję za pośrednictwem formularza kontaktowego oraz zapisując się do naszego newslettera umieszczonych na naszej stronie www, jak również wysyłając nam wiadomości e-mail na adresy poczty elektroniczne info@balticus-watches.com l możesz przekazywać nam swoje dane osobowe. W takiej sytuacji stajemy się Administratorem (Twoich) Danych Osobowych.

Balticus S.A dalej (Balticus) dostosowało organizacyjne i techniczne środki bezpieczeństwa przy przetwarzaniu danych osobowych powierzonych nam przez Ciebie w ramach prowadzonej przez nas działalności gospodarczej.

Zależy nam na zachowaniu wysokiego standardu ochrony danych oraz pełnej przejrzystości przetwarzania danych osobowych nam powierzonych dlatego przekazujemy Ci syntetyczną informację o przetwarzanych danych osobowych oraz związanych z tym prawach.

W sprawie pytań o zakres wdrożenia RODO w Balticusie prosimy o kontakt e-mailowy pod adresem info@balticus-watches.com lub kontakt pisemny, za pomocą poczty tradycyjnej, na adres:
Baltcius ul. Osiedlowa 12/1, 84-123 Rekowo Górne NIP 587-143-55-54

Twoje prawa względem ADMINISTRATORA DANYCH OSOBOWYCH dalej „Administrator" lub „Ado" są następujące

Prawo do dostępu do danych: art. 15 RODO. Masz prawo uzyskania dostępu do Twoich danych przetwarzanych przez Administratora (Administrator dostarczy Ci kopię danych osobowych podlegających przetwarzaniu ewentualnie za opłatą regulowaną przez RODO) oraz do informacji dotyczących: celu przetwarzania; kategorii odnośnych danych osobowych; odbiorców lub kategorii odbiorców danych którym dane ujawniono lub będą ujawnione w tym jeśli są przekazywane do państwa spoza UE lub do organizacji międzynarodowej o zabezpieczeniach związanych z przekazaniem; w miarę możliwości planowanego okresu przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriów ustalania tego okresu; prawa do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych oraz do wniesienia sprzeciwu wobec takiego przetwarzania; prawa wniesienia skargi do organu nadzorczego; jeżeli dane osobowe nie zostały zebrane od Ciebie - ich źródła; zautomatyzowanego podejmowania decyzji, w tym profilowani oraz o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla Ciebie.

Prawo do sprostowania danych: art. 16 RODO. Masz prawo żądania od Administratora niezwłocznego sprostowania dotyczących Ciebie danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, masz prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Prawo do usunięcia danych, tzw. prawo do bycia zapomnianym: art. 17 RODO. Masz prawo żądania od Administratora niezwłocznego usunięcia Twoich danych osobowych jeżeli zachodzi jedna z następujących okoliczności: dane osobowe nie są już niezbędne do celów, w których zostały zebrane

lub w inny sposób przetwarzane; właściciel danych cofnął zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania; wnosisz sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania w sprawach innych niż marketing bezpośredni; dane osobowe były przetwarzane niezgodnie z prawem; dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega Administrator; dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego. Wyżej opisane prawo jest jednak wyłączone w zakresie w jakim przetwarzanie jest niezbędne: do korzystania z prawa do wolności wypowiedzi i informacji; do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi; z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego; do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że wyżej opisane prawo właściciela danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do ograniczenia przetwarzania danych: art. 18 RODO. Masz prawo żądania od Administratora ograniczenia przetwarzania w następujących przypadkach: kwestionujesz prawidłowość danych osobowych - na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych; przetwarzanie jest niezgodne z prawem, a sprzeciwiasz się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania; Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne Tobie do ustalenia, dochodzenia lub obrony roszczeń; właściciel danych wniósł sprzeciw wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą, za wyjątkiem przetwarzania w celu marketingu bezpośredniego. Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za Twoją zgodą lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

Prawo do przenoszenia danych: art. 20 RODO. Masz prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego Twoje dane osobowe, które Administrator ma od Ciebie, a także masz prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora, jeżeli: przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy, oraz przetwarzanie odbywa się w sposób zautomatyzowany. Masz prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Prawo do wniesienia sprzeciwu wobec przetwarzania danych: Masz prawo w dowolnym momencie wnieść sprzeciw - z przyczyn związanych z Twoją szczególną sytuacją - wobec przetwarzania dotyczących Ciebie danych osobowych opartego na Twojej zgodzie lub na prawnie uzasadnionym interesie ADO (patrz informacja powyżej), w tym profilowania. W przypadku wniesienia takiego sprzeciwu ADO nie wolno już przetwarzać Twoich danych osobowych, chyba że ADO wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec Twoich interesów, praw i wolności, albo gdy wykaże istnienie podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Możesz skorzystać z tych uprawnień w dowolny sposób, w tym mailowo na adres info@blticus-watches.com

Najważniejsze zapisy polityki bezpieczeństwa Balticus S.A

W ramach swojej działalności Balticus realizuje obowiązki wynikające z RODO w zależności od zakresu przetwarzania danych jako Administrator Danych Osobowych lub Podmiot przetwarzający dane na podstawie umowy. W celu dostosowania procedur wewnętrznych związanych z przetwarzaniem danych osobowych do RODO zrealizowano szereg działań w tym:

1) powołano Inspektora Ochrony Danych Osobowych (IOD),

2) dokonano przeglądu zasobu danych osobowych w celu przeprowadzenia nowych dokumentów i określenia środków technicznych spełniających wymagania RODO i IOD,

3) przeszkolono pracowników w zakresie nowych przepisów RODO i zapewniono dopuszczenie do przetwarzania danych wyłącznie osoby posiadające upoważnienie oraz zapewniono, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania nieograniczonej w czasie tajemnicy, a także prowadzić ewidencję osób upoważnionych do przetwarzania danych powierzonych Podmiotowi przetwarzającemu,

4) przeprowadzono oceny skutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania (analiza ryzyka - art. 35 RODO),

5) ustanowiono rejestr czynności przetwarzania ochrony danych osobowych,

6) ustanowiono system zgłaszania naruszenia ochrony danych osobowych do organu nadzorczego oraz zawiadamianie o tym osób, których dane te dotyczą (art. 33 i 34 RODO),

7) zapewniono niezwłocznie informowanie Administratora o tym, że osoba której dane dotyczą, skierowała do Podmiotu przetwarzającego korespondencję zawierającą żądanie w zakresie wykonania praw, o których mowa w rozdziale III RODO, jak również udostępniać treść tej korespondencji,

8) zapewniono udostępnianie Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwiono Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji i przyczyniania się do nich,

9) realizowane są wszelkie środki techniczne i organizacyjne wymagane na mocy art. 32 RODO, aby zapewnić stopień bezpieczeństwa przetwarzania danych odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą, w szczególności:

- pseudonimizację lub szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności systemów i usług przetwarzania danych,
- zdolność do szybkiego przywrócenia danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;

Polityka bezpieczeństwa ochrony danych zawiera szczegółowy opis zakresu obowiązków i procedur postępowania w prawidłowym zarządzaniu bezpieczeństwem informacji w Baltciusie. Przez bezpieczeństwo należy rozumieć stan faktyczny uniemożliwiający niezgodne

z RODO wykorzystanie, przepływ, modyfikację i/lub zniszczenie danych osobowych, których Balticus jest Administratorem. Kluczowe ustalenia w tym zakresie to m.in.:

- zabezpieczenie pomieszczeń przed dostępem osób trzecich (biuro ochrony, identyfikacja interesantów, kody dostępu, zabezpieczenia informatyczne),
- wyznaczenie IOD (odpowiedzialnego za nadzór w zakresie obiegu i wykorzystania dokumentacji i danych oraz warunków technicznych i organizacyjnych w jakich są przetwarzane),
- systematyczne organizowanie szkoleń dla pracowników w zakresie przetwarzania danych i sposobów ich ochrony,
- okresowe szacowanie ryzyka zagrożeń obszarów przetwarzania danych,
- kontrola przestrzegania zasad bezpieczeństwa przetwarzania i ochrony danych,
- różne stopnie upoważnień dostępu do danych dla każdego członka zespołu Balticusa,
- każdy z członków zespołu Balticusa zobligowany jest do podpisania wewnętrznej deklaracji
- poufności, w zakresie wszelkich danych pozyskanych oraz przetwarzanych w toku prowadzonej przez Balticusa działalności gospodarczej.

Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych stanowi niejako uszczegółowienie prowadzonej przez Balticusa Polityki bezpieczeństwa ochrony danych. Intensywny rozwój systemów komputerowych, aplikacji oraz digitalizacja informacji powoduje, iż gromadzone przez nas dane są przechowywane na urządzeniach pamięci masowej (serwer), co pozwala na dostęp do nich wszystkim upoważnionym członkom Zespołu Balticusa. Aby zwiększyć niezawodność i zredukować do minimum ryzyko utraty danych i/lub dostępu osób nieuprawnionych Balticus wdrożyły odpowiednie zabezpieczenia informatyczne w tym zakresie. Ryzyko utraty informacji (w tym pozyskanych dokumentów/baz danych itp.) zostało zniwelowany poprzez:

- hasła dostępu (do systemów operacyjnych w komputerach pracowników spółki, do serwera na którym przechowywane są dane, do poczty elektronicznej firmowych serwerów, plików / dokumentów zawierających dane wrażliwe). Hasła składają się z co najmniej 8 znaków, zawierają małe i wielkie litery oraz cyfry i/lub znaki specjalne, takie same znaki nie
- występują obok siebie więcej niż dwukrotnie, użytkownicy są zobowiązani zmieniać hasło co 90 dni, komputery są wyposażone we włączające się po 15 minutach od przerwania pracy wygaszacze ekranu monitorów – wznowienie wyświetlenia następuje dopiero po wprowadzeniu odpowiedniego hasła,
- obowiązujący zakaz wykonywania kopii całych Zbiorów Danych. Całe Zbiory Danych mogą być kopiowane tylko przez Administratora Systemu lub automatycznie przez System Informatyczny, z zachowaniem procedur ochrony Danych,
- możliwość jednostkowego kopiowana informacji na nośniki magnetyczne, optyczne i inne wyłącznie po zaszyfrowaniu dostępu do zapisanych na nich danych. Nośniki przechowywane są w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii, Dane są trwale skasowane lub fizycznie zniszczone nośniki,
- system backup'u, i archiwizacji danych zabezpiecza wytworzone produkty z realizacji badania,
- macierze dyskowe RAID oraz zasilacz UPS,
- programy kontrolujące procesy i dostęp do plików wytworzonych w trakcie trwania badania,
- ograniczenie stosowania nietrwałych nośników informacji,
- ochronę firewall oraz antywirusową (kontrola wszystkich przychodzących i wychodzących
- danych - łącznie z pocztą elektroniczną, ruchem sieciowym oraz wszystkimi interakcjami sieciowymi).

Powyższe narzędzia powodują, iż na każdym etapie naszej działalność ryzyko utraty zgromadzonego materiału informacyjnego i/lub uzyskania do niego dostępu przez osoby nieupoważnione będzie maksymalnie ograniczone.