Polityka Ochrony Danych
Wersja 01 aktualna na dzień 25 maja 2018 r.

Polityka Ochrony Danych

Zatwierdzający:	Zarząd: □ Dyrektor generalny □ Dyrektor finansowy
Zarządzający:	Dział ds. prawnych i zgodności z przepisami
Dotyczy:	Wszystkich pracowników FläktGroup, FläktGroup Holding GmbH i wszystkich spółek stowarzyszonych
Data wejścia w życie:	25 maja 2018 r.

Spis treści

1. Cel i zakres

Jako międzynarodowa grupa przedsiębiorstw o silnej pozycji w Unii Europejskiej firma FläktGroup wraz z przedsiębiorstwami stowarzyszonymi należącymi do grupy (dalej łącznie „FläktGroup") dąży do zapewniania globalnej zgodności z przepisami ochrony danych, w tym w szczególności z ogólnym rozporządzeniem Unii Europejskiej o ochronie danych.

Niniejsza Polityka Ochrony Danych zawiera niezbędne postanowienia ramowe dotyczące Przesyłania Danych przez Przedsiębiorstwa z grupy FläktGroup i pomiędzy nimi, a jej celem jest nie tylko zapewnienie zgodności z ogólnym rozporządzeniem Unii Europejskiej o ochronie danych i przepisami krajowymi, lecz także wyznaczenie jednolitego, standardowego poziomu ochrony danych w obrębie grupy FläktGroup.

Niniejsza Polityka Ochrony Danych określa zatem globalnie przyjęte zasady prywatności danych i stanowi uzupełnienie obowiązujących krajowych i europejskich przepisów ochrony danych. Obowiązujące przepisy krajowe lub europejskie będą mieć pierwszeństwo przed niniejszą Polityką Ochrony Danych, jeśli są sprzeczne z jej zapisami lub narzucają bardziej rygorystyczne wymagania. Przestrzeganie postanowień niniejszej Polityki Ochrony Danych jest wymagane również w przypadku braku stosownych przepisów krajowych.

Każde Przedsiębiorstwo z grupy FläktGroup odpowiada za zapewnienie zgodności z niniejszą Polityką Ochrony Danych i wszelkimi zobowiązaniami prawnymi.

Przedsiębiorstwom z grupy FläktGroup nie wolno wprowadzać żadnych przepisów sprzecznych z niniejszą Polityką Ochrony Danych, ponieważ mogłoby to osłabić postanowienia Polityki. Jeśli wymagają tego obowiązujące przepisy krajowe, możliwe jest tworzenie dodatkowych zasad ochrony danych w porozumieniu z działem ds. prawnych i zgodności z przepisami grupy FläktGroup.

Jeśli w jednym z Przedsiębiorstw grupy FläktGroup zaistnieje podejrzenie, że zobowiązania prawne są sprzeczne z obowiązkami wynikającymi z niniejszej Polityki Ochrony Danych, należy niezwłocznie powiadomić Inspektora Ochrony Danych w odpowiednim Przedsiębiorstwie grupy FläktGroup. Jeśli w przedsiębiorstwie nie został wyznaczony Inspektor Ochrony Danych, należy powiadomić na piśmie dział ds. prawnych i zgodności z przepisami. W razie sprzeczności przepisów krajowych z Polityką Ochrony Danych dział ds. prawnych i zgodności z przepisami będzie współpracować z odpowiednim Przedsiębiorstwem grupy FläktGroup w celu wypracowania praktycznego rozwiązania zgodnego z celem Polityki.

2. Definicje

2.1 Dane Osobowe

Za Dane Osobowe uznawane są wszelkie informacje, które można powiązać z konkretną osobą fizyczną (bezpośrednio lub pośrednio z wykorzystaniem dodatkowej wiedzy).
Przykłady Danych Osobowych:

- imię, nazwisko, wiek, adres zamieszkania lub adres e-mail konkretnej osoby;
- nazwa użytkownika (nazwa logowania), jeśli można ją jednoznacznie powiązać z konkretną osobą.

2.2 Dane Wysoce Wrażliwe
Dane Wysoce Wrażliwe wymagają szczególnie starannej ochrony. Za Dane Wysoce Wrażliwe uznawane są między innymi informacje o pochodzeniu rasowym lub etnicznym, przekonaniach politycznych, religijnych lub filozoficznych, przynależności do związków zawodowych, stanie zdrowia i orientacji seksualnej.
Przykłady Danych Wysoce Wrażliwych:

- kolor skóry;
- miejsce urodzenia lub obywatelstwo;
- liczba dni zwolnienia chorobowego w ciągu roku;
- dokumenty dotyczące opieki przedszkolnej (notatki, wiadomości e-mail itp.);
- członkostwo w związku zawodowym.

W zależności od przepisów krajowych dane uznawane za wysoce wrażliwe mogą obejmować również inne kategorie lub zawartość poszczególnych kategorii może mieć inną strukturę.

2.3 Dane Anonimizowane
Anonimizacja to proces modyfikowania Danych Osobowych w taki sposób, aby nie dało się bez niepraktycznie dużych nakładów pracy przypisać ich do konkretnej osoby fizycznej.

Gdy stosowana jest pseudonimizacja, wybrane informacje są zastępowane pseudonimem, aby uniemożliwić lub poważnie utrudnić przypisanie danych do konkretnej osoby fizycznej bez znajomości klucza. Gdy klucz jest znany, dane można nadal przypisać do konkretnej osoby fizycznej.

2.4 Przetwarzanie Danych
Przez Przetwarzanie Danych rozumie się wszelkie procesy gromadzenia, zapisywania, przetwarzania, organizowania, przechowywania, modyfikowania, odpytywania, używania, przekazywania, przesyłania, upowszechniania lub łączenia i porównywania danych. Dotyczy to również usuwania, blokowania i sprzedaży danych lub nośników zawierających dane.

Nie jest w tym przypadku istotne, czy do Przetwarzania Danych są używane systemy zautomatyzowane, czy też nie.

2.5 Administrator Danych
Administratorem Danych (podmiotem odpowiedzialnym) jest każde Przedsiębiorstwo grupy FläktGroup, którego działalność powoduje zainicjowanie działań związanych z przetwarzaniem. W przypadku Przetwarzania Danych związanego z centralnie

udostępnianymi systemami i procedurami (np. generowania raportów dla całej Grupy) za Administratora Danych uznaje się firmę FläktGroup Holding GmbH.

2.6 Podmiot Przetwarzający Dane
Podmioty Przetwarzające Dane to firmy lub osoby fizyczne, które przetwarzają dane w imieniu Administratorów Danych i zgodnie z ich instrukcjami, nie odpowiadając jednak za proces biznesowy będący przyczyną przetwarzania.
Przykłady Podmiotów Przetwarzających Dane:

- dostawcy usług obsługi księgowej listy płac,
- dostawcy usług archiwizacji,
- firmy udostępniające systemy HR lub CRM,
- zewnętrzne firmy konsultingowe lub serwisowe,
- dostawcy usług chmurowych.

2.7 Osoba, której dane dotyczą
Dla potrzeb niniejszej Polityki Ochrony Danych osobą, której dane dotyczą, jest każda osoba fizyczna, której dane można przetwarzać. W niektórych krajach (np. Austrii i Danii) również osoby prawne mogą być osobami, których dane dotyczą.

2.8 Strona Trzecia
Przez Stronę Trzecią rozumie się dowolny podmiot poza osobą, której dane dotyczą i Administratorem Danych. Podmioty Przetwarzające Dane w imieniu innego podmiotu nie są w świetle przepisów ochrony danych UE uznawane za strony trzecie, ponieważ są prawnie powiązane z Administratorem Danych odpowiedzialnym za przetwarzanie.

2.9 Kraje Trzecie
Dla potrzeb niniejszej Polityki Ochrony Danych za Kraje Trzecie uważa się wszystkie kraje leżące poza Unią Europejską (UE) i Europejskim Obszarem Gospodarczym (EOG).

Bezpieczne Kraje Trzecie to takie, które zapewniają adekwatny i zatwierdzony przez Komisję Europejską poziom ochrony danych (z uwzględnieniem ewentualnych ograniczeń). Lista bezpiecznych Krajów Trzecich wraz z wszelkimi obowiązującymi ograniczeniami jest udostępniana przez Komisję Europejską w Internecie i regularnie aktualizowana.

Kraje Trzecie Nieuznawane za Bezpieczne to takie, w których poziom ochrony danych został uznany przez Komisję Europejską za niewystarczający lub dla których nie jest dostępna ocena Komisji Europejskiej.

W przypadku komunikacji wymagającej wysyłania danych do Krajów Trzecich Administratorzy Danych z grupy FlaktGroup mają obowiązek raz do roku weryfikować aktualność statusu partnerskiego danego Kraju Trzeciego.

2.10 Przesyłanie Danych
Przesyłanie Danych to każde ujawnienie chronionych danych Stronom Trzecim przez Administratora Danych.

3. Przetwarzanie Danych Osobowych

Przy przetwarzaniu Danych Osobowych obowiązują następujące zasady:

3.1 Zgodność z prawem

Gromadzenie i przetwarzanie Danych Osobowych musi się odbywać zgodnie z prawem, w dobrej wierze i w sposób uzasadniony z punktu widzenia osoby, której one dotyczą.

3.2 Ograniczenie do konkretnego celu

Dane Osobowe można przetwarzać wyłącznie w celu wskazanym przed ich zgromadzeniem. Późniejsze zmiany celu są możliwe jedynie w ograniczonym zakresie i muszą zostać uzasadnione przed rozpoczęciem przetwarzania.

3.3 Przejrzystość

Co do zasady Dane Osobowe muszą być pobierane bezpośrednio od osoby, której dotyczą. Niezależnie od sytuacji osoba ta musi znać lub otrzymać następujące informacje:

- cel Przetwarzania Danych;
- tożsamość Podmiotu Przetwarzającego Dane;
- Strony Trzecie, do których dane mogą być przesyłane (lub kategorie takich stron).

3.4 Minimalizacja zakresu i rozmiaru danych

Przed przystąpieniem do przetwarzania Danych Osobowych należy ustalić, czy i w jakim zakresie przetwarzanie Danych Osobowych jest niezbędne do realizacji celu, w którym jest podejmowane. Gdy cel to umożliwia, a niezbędne koszty są proporcjonalne do korzyści z realizacji celu, należy używać danych anonimizowanych lub statystycznych.

To samo dotyczy ustalania procedur przetwarzania Danych Osobowych.

3.5 Usuwanie

Gdy Dane Osobowe nie są już niezbędne z powodu wygaśnięcia celu ich przetwarzania (prawnego lub innego), muszą zostać usunięte. W uzasadnionych przypadkach wynikających z indywidualnej sytuacji lub obowiązujących przepisów dane nie będą usuwane do czasu jednoznacznego ustalenia, czy podlegają one archiwizacji.

Usuwanie danych kadrowych musi się odbywać zgodnie z przyjętymi okresami przechowywania we wszystkich rejestrach danych kadrowych, a okresy przechowywania muszą być zgodne z lokalnymi przepisami.

3.6 Aktualność i zgodność z prawdą

Dane Osobowe muszą być poprawne, kompletne i w stosownych przypadkach na bieżąco aktualizowane. Należy stosować odpowiednie środki, aby dane niezgodne z prawdą lub niekompletne były usuwane lub aktualizowane.

3.7 Bezpieczeństwo i poufność

Dane Osobowe należy traktować jako poufne i zapewnić ich ochronę. Należy stosować odpowiednie środki techniczne i organizacyjne pozwalające zapobiegać nieuprawnionemu

dostępowi, nielegalnemu przetwarzaniu lub rozpowszechnianiu oraz przypadkowemu utraceniu, zmodyfikowaniu lub zniszczeniu.

4. Wiarygodność przetwarzania danych

Gromadzenie, przetwarzanie i używanie Danych Osobowych jest dozwolone wyłącznie pod warunkiem spełnienia poniższych wymogów prawnych. Jeden z tych wymogów prawnych musi być spełniony również w przypadku zmiany pierwotnego celu Przetwarzania Danych.

4.1 Warunki ogólne

a) Osoba, której dane dotyczą dobrowolnie udzieliła pisemnej zgody na Przetwarzanie Danych w zamierzonym celu.
b) Przetwarzanie jest niezbędne dla realizacji umów lub postanowień umownych na żądanie osoby, której dane dotyczą (jako strony umowy).
c) Administrator Danych jest podmiotem uprawnionym do przetwarzania danych.
d) Przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.
e) Przetwarzanie jest niezbędne z punktu widzenia uzasadnionego interesu Administratora Danych lub Strony Trzeciej, o ile uzasadniony interes osoby, której dane dotyczą nie jest przeciwwskazaniem dla takiego przetwarzania. W razie wątpliwości konieczne jest uzyskanie zgody przedmiotowej osoby.

4.2 Dane Pracownika[1]

4.2.1 Przetwarzanie Danych dla potrzeb stosunku zatrudnienia

Dane Osobowe w stosunkach zatrudnienia (Dane Pracownika) mogą być przetwarzane, gdy jest to konieczne dla zawarcia, realizacji, przenoszenia i rozwiązywania umowy o pracę.

W przypadku podań o pracę dozwolone jest przetwarzanie Danych Osobowych kandydatów. Dane kandydatów nieprzyjętych muszą zostać usunięte po upływie wymaganego okresu przechowywania, chyba że kandydat wyraził zgodę na zachowanie jego danych dla potrzeb przyszłej selekcji kandydatów. Uzyskanie zgody jest również niezbędne w celu używania danych w dalszych procesach rekrutacji oraz przed udostępnieniem wniosku kandydata innym przedsiębiorstwom grupy FläktGroup.

Przetwarzanie Danych w ramach istniejącego stosunku zatrudnienia musi zawsze być powiązane z celem umowy o pracę, o ile nie ma zastosowania żadna z poniższych podstaw prawnych Przetwarzania Danych.

Jeśli podczas procedury aplikacyjnej lub istniejącego stosunku pracy zajdzie konieczność gromadzenia informacji od Strony Trzeciej, konieczne jest przestrzeganie wymagań stosownych przepisów krajowych. W razie wątpliwości należy uzyskać zgodę osoby, której dane dotyczą.

[1] Dla potrzeb niniejszego dokumentu termin „Dane Pracownika” obejmuje dane wszystkich pracowników zgodnie z §26, ust. 8 BDSG n.F.

Przetwarzanie Danych Osobowych związanych ze stosunkiem pracy, ale pierwotnie niewymaganych do realizacji umowy o pracę, musi mieć odpowiednią podstawę prawną. Dopuszczalne podstawy to między innymi wymogi prawne, umowy zbiorowe z przedstawicielami pracowników, zgoda pracownika lub uzasadniony interes firmy.

4.2.2 Przetwarzanie Danych na podstawie uzasadnienia prawnego
Przetwarzanie Danych Osobowych Pracownika jest dozwolone w przypadkach, gdy jest wymagane na podstawie przepisów krajowych lub innego uzasadnienia prawnego. Rodzaj i zakres Przetwarzania Danych muszą być niezbędne z punktu widzenia uzasadnionego prawnie działania Przetwarzania Danych i zgodne ze stosownymi wymogami ustawowymi. Jeśli podstawy prawne pozostawiają swobodę wyboru, należy uwzględniać interesy pracownika wymagające ochrony.

4.2.3 Umowy zbiorowe dotyczące Przetwarzania Danych
Przetwarzanie Danych Osobowych Pracownika jest dozwolone, jeśli zostało dopuszczone w umowie zbiorowej. Umowy zbiorowe to między innymi umowy dotyczące przedziałów wynagrodzeń lub inne umowy zawierane między pracodawcą a przedstawicielami pracowników w zakresie dozwolonym przez obowiązujące prawo pracy. Umowy zbiorowe muszą określać szczegółowy cel planowanego Przetwarzania Danych i spełniać wymagania krajowego ustawodawstwa w dziedzinie ochrony danych.

4.2.4 Zgoda na Przetwarzanie Danych
Dane Pracownika można przetwarzać za zgodą osoby, której one dotyczą. Zgoda musi być wyrażona dobrowolnie — w przeciwnym razie będzie ona nieważna. Generalnie oświadczenie o zgodzie trzeba uzyskać w formie pisemnej lub elektronicznej. Gdy nie jest to możliwe, w wyjątkowych przypadkach dopuszczalne jest uzyskanie zgody ustnej. Niezależnie od formy zgoda musi być prawidłowo udokumentowana. Jeśli dane zostały przez przedmiotową osobę podane dobrowolnie i świadomie, dopuszczalne jest przyjęcie zgody domniemanej, o ile przepisy krajowe nie wymagają uzyskania zgody wyraźnej. Przed wyrażeniem zgody przedmiotowa osoba musi zostać poinformowana zgodnie z wymogami niniejszej Polityki Ochrony Danych.

4.2.5 Przetwarzanie Danych na podstawie uzasadnionego interesu
Przetwarzanie Danych Pracownika jest również dozwolone, gdy wymaga tego uzasadniony interes grupy FläktGroup. Uzasadniony interes jest przeważnie natury prawnej (np. wysuwanie, egzekwowanie lub odpieranie roszczeń prawnych) lub handlowej (np. wycena przedsiębiorstw).

Przetwarzanie Danych Pracownika na podstawie uzasadnionego interesu nie jest dozwolone w przypadkach, gdzie może być wymagana ochrona indywidualnego interesu pracownika. Przed przystąpieniem do przetwarzania Danych Pracownika należy ustalić, czy występuje interes wymagający ochrony.

Środki kontrolne wymagające przetwarzania Danych Pracownika można podejmować jedynie wtedy, gdy istnieje uzasadniony powód lub obowiązek prawny. Nawet gdy istnieje uzasadniony powód, należy zawsze zapewnić proporcjonalność środków kontrolnych. Uzasadniony interes określonego Przedsiębiorstwa grupy FläktGroup będący podstawą

zastosowania środków kontrolnych (np. konieczność zapewnienia zgodności z przepisami prawa lub wewnętrznymi zasadami firmy) trzeba rozważać w kontekście ochrony ewentualnego interesu pracownika w wykluczeniu takich środków. Przed wdrożeniem jakichkolwiek środków należy zidentyfikować i udokumentować uzasadniony interes jednego lub kilku Przedsiębiorstw grupy FläktGroup (stosownie do przypadku) oraz ewentualny interes pracownika wymagający ochrony. Należy uwzględnić wszelkie dodatkowe wymagania wynikające z przepisów krajowych, np. prawo do wspólnego stanowienia przez przedstawicieli pracowników lub prawa osób, której dane dotyczą do informacji.

4.2.6 Przetwarzanie Danych Wysoce Wrażliwych
Przetwarzanie Danych Wysoce Wrażliwych jest dozwolone wyłącznie w ściśle określonych warunkach.

Przetwarzanie musi być wyraźnie dozwolone lub nakazane przepisami prawa krajowego. Przetwarzanie może też być dozwolone, jeśli jest niezbędne dla realizacji praw i obowiązków Administratora Danych wynikających z prawa pracy. Pracownik może też udzielić wyraźnej zgody na takie przetwarzanie.

O wszelkich planach przetwarzania Danych Wysoce Wrażliwych należy z wyprzedzeniem poinformować lokalnego Inspektora Ochrony Danych lub lokalny dział kadr.

4.2.7 Decyzje zautomatyzowane
Jeśli podczas automatycznego przetwarzania Danych Pracownika w ramach stosunku pracy wykonywana jest ocena określonych Danych Pracownika (np. w procesie selekcji personelu lub oceny profili kwalifikacji), przetwarzanie automatyczne nie może być jedyną podstawą żadnych decyzji, które mogłyby mieć negatywne konsekwencje dla pracownika lub rodzić dla niego znaczące trudności. Pracownik musi być informowany o ocenianych informacjach i wynikach decyzji zautomatyzowanych oraz musi mieć możliwość reagowania na nie.

4.2.8 Telekomunikacja i Internet
Sprzęt telefoniczny, adresy e-mail oraz dostęp do Internetu, intranetu i wewnętrznych sieci użytkowników to zasoby udostępniane przez Przedsiębiorstwo grupy FläktGroup przede wszystkim do celów związanych z pracą. Są to narzędzia i zasoby służbowe, których wykorzystanie podlega stosownym przepisom prawa, wewnętrznym zasadom firmy i ewentualnym umowom dotyczącym zatrudnienia. W przypadkach autoryzowanego wykorzystywania do celów prywatnych konieczne jest przestrzeganie przepisów tajności telekomunikacji i stosownych krajowych przepisów telekomunikacyjnych (jeśli mają zastosowanie).

Nie będzie prowadzony całościowy monitoring komunikacji telefonicznej, poczty elektronicznej ani nawiązywanych połączeń internetowych bądź intranetowych. Dla zapewnienia ochrony przed atakami wymierzonymi w infrastrukturę informatyczną lub konkretnych użytkowników dozwolone jest stosowanie prewencyjnych środków kontroli połączeń z siecią grupy FläktGroup w celu blokowania szkodliwych danych lub analizowania wzorców ruchu w poszukiwaniu ataków. Ze względów bezpieczeństwa korzystanie ze sprzętu telefonicznego, adresów e-mail, Internetu, intranetu i wewnętrznych sieci użytkowników może być tymczasowo rejestrowane w dziennikach. Analiza takich danych w odniesieniu do

konkretnej osoby jest dozwolona tylko w konkretnych przypadkach uzasadnionego podejrzenia o naruszenie prawa lub zasad grupy FläktGroup. Analizę może prowadzić jedynie dział prowadzący dochodzenie, dbając przy tym o przestrzeganie zasady proporcjonalności. Przez cały czas należy przestrzegać stosownych przepisów krajowych oraz zasad i przepisów grupy FläktGroup.

4.3 Dane klientów, dostawców i partnerów

4.3.1 Przetwarzanie Danych dla potrzeb relacji umownej

Dane Osobowe klientów, potencjalnych klientów, dostawców i partnerów można przetwarzać dla potrzeb zawarcia, realizacji lub rozwiązania umowy. Dotyczy to również ogólnych usług doradczych oferowanych partnerowi, jeśli są one związane z celem umowy. Przed zawarciem umowy (w fazie przygotowywania umowy) dozwolone jest przetwarzanie Danych Osobowych w celu przygotowywania ofert i zamówień zakupu lub realizowania innych żądań potencjalnego klienta związanych z zawarciem umowy. W procesie przygotowywania umowy dozwolone jest kontaktowanie się z potencjalnym klientem z wykorzystaniem podanych przez niego informacji. Należy przestrzegać wszelkich ograniczeń wskazanych przez potencjalnych klientów.

4.3.2 Przetwarzanie Danych w celach reklamowych

Jeśli potencjalny klient skontaktuje się z przedsiębiorstwem grupy FläktGroup (np. w celu uzyskania materiałów informacyjnych dotyczących produktów), dozwolone jest Przetwarzanie Danych Osobowych w celu spełnienia tego żądania.

Wszelkie akcje lojalnościowe lub reklamowe podlegają dodatkowym wymaganiom prawnym. Dozwolone jest przetwarzanie Danych Osobowych w celach reklamowych lub do prowadzenia badań rynku i opinii, jeśli jest to zgodne z celem pierwotnego zgromadzenia tych danych. Konieczne jest informowanie osób, których dane dotyczą o używaniu ich danych w celach reklamowych. Gdy dane są gromadzone wyłącznie w celach reklamowych, ujawnienie ich przez osobę, której dotyczą jest dobrowolne, o czym należy te osobę wyraźnie poinformować. W kontaktach z osobą, której dane dotyczą konieczne jest uzyskanie wyraźnej zgody tej osoby na przetwarzanie jej danych w celach reklamowych. Osoba, której dotyczą musi mieć możliwość wyboru formy udzielenia swojej zgody, na przykład pocztą tradycyjną, pocztą elektroniczną lub telefonicznie.

Jeśli osoba, której dane dotyczą nie wyrazi zgody na używanie swoich danych do celów reklamowych, dalsze używanie tych danych jest zabronione i należy zablokować możliwość ich używania do tego celu. Należy też przestrzegać wszelkich krajowych ograniczeń dotyczących używania danych do celów reklamowych.

4.3.3 Zgoda na Przetwarzanie Danych

Dane można przetwarzać po uzyskaniu zgody osoby, której dane dotyczą. Przed wyrażeniem zgody osoba, której dane dotyczą musi zostać poinformowana zgodnie z wymogami niniejszej Polityki Ochrony Danych. Oświadczenie o zgodzie należy uzyskać w formie pisemnej lub elektronicznej. W wyjątkowych przypadkach, gdy uzyskanie zgody pisemnej nie jest możliwe (np. podczas rozmowy telefonicznej), dopuszczalna jest zgoda wyrażona ustnie. Niezależnie od formy zgoda musi być prawidłowo udokumentowana.

4.3.4 Przetwarzanie Danych na podstawie uzasadnienia prawnego
Przetwarzanie Danych Osobowych jest dozwolone, jeśli krajowe przepisy prawa dopuszczają takie przetwarzanie lub go wymagają.

4.3.5 Przetwarzanie Danych na podstawie uzasadnionego interesu
Przetwarzanie Danych Osobowych jest dozwolone, gdy wymaga tego uzasadniony interes grupy FläktGroup. Uzasadniony interes jest przeważnie natury prawnej (np. dochodzenie zaległych należności) lub handlowej (np. zapobieganie naruszeniom umowy). Przetwarzanie Danych Osobowych na podstawie uzasadnionego interesu nie jest dozwolone, jeśli w konkretnym przypadku istnieją dowody wskazujące na pierwszeństwo wymagających ochrony interesów osoby, której dane dotyczą. Ewentualne istnienie takich interesów wymagających ochrony należy każdorazowo ustalić przed rozpoczęciem przetwarzania.

4.3.6 Przetwarzanie Danych Wysoce Wrażliwych
Przetwarzanie Danych Wysoce Wrażliwych jest dozwolone tylko wtedy, gdy wymaga tego prawo lub uzyskano wyraźną zgodę osoby, której dane dotyczą. Przetwarzanie Danych Wysoce Wrażliwych jest dozwolone również wtedy, gdy jest to niezbędne do wnoszenia, egzekwowania lub odpierania roszczeń prawnych dotyczących osoby, której dane dotyczą.

O wszelkich planach przetwarzania Danych Wysoce Wrażliwych należy z wyprzedzeniem poinformować lokalnego Inspektora Ochrony Danych lub dział ds. prawnych i zgodności z przepisami grupy FläktGroup.

4.3.7 Decyzje zautomatyzowane
Jeśli podczas automatycznego przetwarzania Danych Osobowych wykonywana jest ocena określonych Danych Osobowych (np. ocena zdolności kredytowej), takie przetwarzanie automatyczne nie może być jedyną podstawą żadnych decyzji, które mogłyby mieć negatywne konsekwencje prawne dla osoby, której dane dotyczą lub znacząco utrudnić jej funkcjonowanie. Osoba, której dane dotyczą musi być informowana o ocenianych informacjach i wynikach decyzji zautomatyzowanych oraz mieć możliwość reagowania na nie.

4.3.8 Dane użytkownika a Internet
Jeśli Dane Osobowe są zbierane, przetwarzane i używane na stronach internetowych lub w aplikacjach, osoby, których dane dotyczą muszą być o tym informowane w oświadczeniu dotyczącym prywatności i (jeśli ma zastosowanie) informacji o używaniu plików cookie. Informacje muszą być integrowane na stronach internetowych i w aplikacjach w taki sposób, aby były dla osób, których dane dotyczą łatwe w zidentyfikowaniu oraz bezpośrednio i w spójny sposób dostępne.

Jeśli tworzone są profile użytkowników w celu analizy użytkowania stron internetowych i aplikacji (śledzenia), informacja ta musi być zawarta w oświadczeniu dotyczącym prywatności dostarczanym osobom, których dane dotyczą. Śledzenie osobiste jest dopuszczalne tylko wtedy, gdy zezwala na nie prawo krajowe lub osoba, której dane dotyczą wyraziła na nie zgodę. Jeśli stosowane jest śledzenie z pseudonimizacją, w oświadczeniu

dotyczącym prywatności powinna być dostępna opcja rezygnacji z takiego śledzenia przez osobę, której dane dotyczą (wyrażenia sprzeciwu).

Jeśli witryny internetowe lub aplikacje dają zarejestrowanym użytkownikom dostęp do ich Danych Osobowych w obszarze dostępnym tylko dla danego użytkownika, proces identyfikowania i uwierzytelniania użytkownika musi zapewniać wystarczającą ochronę takiego dostępu.

5. Kontraktowe Przetwarzanie Danych

Podmioty Przetwarzające Dane kontraktowo to firmy lub osoby fizyczne, które przetwarzają dane w imieniu Administratorów Danych i zgodnie z ich instrukcjami, nie odpowiadając jednak za proces biznesowy będący przyczyną przetwarzania (Przetwarzanie Danych w imieniu Administratora). Firma zlecająca pozostaje właścicielem wszystkich danych i ponosi pełną odpowiedzialność za prawidłowy przebieg Przetwarzania Danych.

Warunki Przetwarzania Danych w imieniu Administratora muszą być wyszczególnione w pisemnej umowie między klientem a wykonawcą. Dotyczy to współpracy zarówno z wykonawcami zewnętrznymi, jak i z innymi przedsiębiorstwami grupy FläktGroup.

Przy wystawianiu zlecenia muszą być spełnione następujące wymagania, a dział zlecający ma obowiązek dopilnować ich przestrzegania:

- Przy wyborze wykonawcy należy się kierować jego zdolnością do zapewnienia wymaganych technicznych i organizacyjnych środków ochrony.
- Siedziba wykonawcy powinna mieścić się w UE lub Bezpiecznym Kraju Trzecim.
- Jeśli siedziba wykonawcy mieści się w kraju trzecim nieuznawanym za bezpieczny, wykonawca musi pisemnie wskazać przedstawiciela na terenie UE, który będzie działać w jego imieniu.
- Zlecenie musi mieć formę pisemną. Instrukcje Przetwarzania Danych oraz obowiązki klienta i wykonawcy muszą być udokumentowane.
- Należy uwzględniać standardy umowne ochrony danych.
- Przed przystąpieniem do Przetwarzania Danych klient musi mieć pewność, że wykonawca wywiąże się ze swoich zobowiązań. Wykonawca może udokumentować zgodność z wymogami ochrony danych między innymi poprzez odpowiedni certyfikat.
- W przypadkach obejmujących międzynarodowe Przetwarzanie Danych muszą być spełnione stosowne wymagania krajowe dotyczące ujawniania Danych Osobowych za granicą. W szczególności przetwarzanie Danych Osobowych z Europejskiego Obszaru Gospodarczego w kraju trzecim jest dozwolone tylko wtedy, gdy wykonawca może udokumentować stosowanie standardów ochrony danych porównywalnych z niniejszą Polityką Ochrony Danych. Akceptowane metody udokumentowania zgodności to między innymi umowa dotycząca stosowania standardowych klauzul umownych UE do kontraktowego Przetwarzania Danych w Krajach Trzecich lub przynależność wykonawcy do akredytowanego przez UE, instytucję certyfikacyjną lub odpowiedzialny urząd regulacji systemu certyfikacji gwarantującego stosowanie przez wykonawcę wystarczającej ochrony danych.

6. Prawa osoby, której dane dotyczą

Każda osoba, której dane dotyczą ma prawa wymienione poniżej. Każde żądanie skorzystania z tych praw musi być niezwłocznie rozpatrywane przez Administratora Danych i nie może się wiązać z niekorzystnymi konsekwencjami dla osoby, której dane dotyczą.

- Osoba, której dane dotyczą może zażądać informacji o przechowywanych na jej temat Danych Osobowych oraz metodach i celu zgromadzenia tych danych. Nie wpływa to na ewentualne dodatkowe prawa dostępu do dokumentów dotyczących stosunku pracy (np. akt osobowych) przechowywanych przez pracodawcę na mocy prawa pracy.
- W przypadku przesyłania Danych Osobowych stronom trzecim wymagane jest udostępnienie informacji o tożsamości odbiorcy lub kategoriach odbiorców.
- Jeśli Dane Osobowe są niepoprawne lub niekompletne, osoba, której dane dotyczą może zażądać ich poprawienia lub uzupełnienia.
- Osoba, której dane dotyczą ma prawo sprzeciwić się wykorzystywaniu swoich danych w celach reklamowych bądź do prowadzenia badań rynku i opinii. W razie wyrażenia takiego sprzeciwu konieczne jest zablokowanie używania danych do takich celów.
- Osoba, której dane dotyczą na prawo zażądać usunięcia swoich danych, jeśli są one przetwarzane bez podstawy prawnej lub jeśli dotychczasowa podstawa prawna nie ma już zastosowania. Takie samo prawo przysługuje, jeśli cel Przetwarzania Danych wygasł lub z innych powodów przestał mieć zastosowanie. Konieczne jest przestrzeganie obowiązujących okresów przechowywania oraz uwzględnianie sprzecznych interesów wymagających ochrony.
- Osoba, której dane dotyczą ma prawo wyrazić ogólny sprzeciw wobec wykorzystywania swoich danych. Trzeba to wziąć pod uwagę, jeśli ze względu na indywidualną sytuację ochrona interesu osoby, której dane dotyczą ma pierwszeństwo przed interesem wymagającym Przetwarzania Danych. Zastrzeżenie to nie ma to zastosowania, jeśli Przetwarzanie Danych jest wymagane przepisami prawa.
- Sprzeciwy nie działają wstecz.

7. Poufność przetwarzania

Dane Osobowe należy traktować jako poufne. Zabrania się nieautoryzowanego gromadzenia, przetwarzania lub używania takich danych przez pracowników. Przetwarzanie Danych przez pracownika uznaje się za nieautoryzowane, jeśli nie należy do powierzonych mu obowiązków i jeśli nie został on do takiego przetwarzania upoważniony.

Obowiązuje tu zasada minimalnej wiedzy potrzebnej do wykonywania obowiązków. Pracownicy mogą uzyskiwać dostęp do Danych Osobowych wyłącznie w zakresie niezbędnym do wykonania konkretnego zadania, które zostało im powierzone. Aby tego dopilnować, należy utrzymywać staranny podział ról i obowiązków.

Pracownikom nie wolno używać Danych Osobowych do własnych celów osobistych lub komercyjnych, ujawniać ich osobom nieautoryzowanym ani udostępniać w żaden inny sposób. Przedsiębiorstwa grupy FläktGroup mają obowiązek informowania pracowników podejmujących stosunek pracy o obowiązku ochrony poufności danych. Obowiązek ten pozostaje w mocy również po rozwiązaniu stosunku pracy.

8. Bezpieczeństwo przetwarzania

Dane Osobowe muszą być chronione przed nieautoryzowanym dostępem, nielegalnym przetwarzaniem i ujawnianiem oraz przypadkowym utraceniem, zmodyfikowaniem lub zniszczeniem. Dotyczy to zarówno danych w postaci elektronicznej, jak i papierowej.

Konieczne jest stosowanie odpowiednich środków technicznych i organizacyjnych ochrony z uwzględnieniem aktualnego stanu wiedzy technicznej, kosztu implementacji, charakteru, kontekstu i celów przetwarzania oraz wszelkich związanych z przetwarzaniem zagrożeń (niezależnie od prawdopodobieństwa ich wystąpienia i wagi zagrożenia) dla praw i wolności osób fizycznych, przy czym czynniki te należy uwzględniać zarówno przy wyborze metody przetwarzania, jak i w trakcie samego przetwarzania. Środki te należy zaprojektować w sposób pozwalający efektywnie wdrażać zasady ochrony danych opisane w niniejszej Polityce i integrować niezbędne zabezpieczenia w procesach przetwarzania.

Wdrażane środki techniczne i organizacyjne powinny gwarantować domyślne ograniczanie Danych Osobowych do minimalnego zakresu niezbędnego dla konkretnego celu przetwarzania. Obowiązek ten ma zastosowanie do ilości gromadzonych Danych Osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Stosowane środki muszą w szczególności uniemożliwiać udostępnienie Danych Osobowych nieokreślonej z góry liczbie osób fizycznych przy domyślnych ustawieniach.

Każdy dział odpowiedzialny za definiowanie i wdrażanie środków technicznych i organizacyjnych może zasięgnąć w tym zakresie porady lokalnego Inspektora Ochrony Danych lub działu ds. prawnych i zgodności z przepisami grupy FläktGroup.

Środki techniczne i organizacyjne ochrony Danych Osobowych muszą być na bieżąco dostosowywane do rozwoju technologicznego i zmian organizacyjnych.

9. Audyt ochrony danych

Zgodność z Polityką Ochrony Danych i stosownymi przepisami podlega regularnej weryfikacji. Wykonywanie audytu jest obowiązkiem Inspektora Ochrony Danych danego Przedsiębiorstwa grupy FläktGroup lub zatrudnionej w tym celu zewnętrznej firmy audytorskiej.

Wyniki audytu ochrony danych należy dostarczać kierownictwu lokalnego Przedsiębiorstwa grupy FläktGroup oraz firmie FläktGroup Holding GmbH. O szczególnie istotnych wynikach należy informować dział ds. prawnych i zgodności z przepisami grupy FläktGroup.

Wyniki audytu ochrony danych należy udostępniać urzędom ochrony danych na ich żądanie, działając w zakresie obowiązujących przepisów. Stosowne urzędy ochrony danych mogą zlecać własne audyty ochrony danych, jeśli leży to w zakresie ich kompetencji.

10. Incydenty Związane z Ochroną Danych

Każdy pracownik ma obowiązek niezwłocznie informować swojego przełożonego lub Inspektora Ochrony Danych w odpowiednim Przedsiębiorstwie bądź dział ds. prawnych i zgodności z przepisami grupy FläktGroup o każdym znanym mu naruszeniu niniejszej Polityki Ochrony Danych lub innych przepisów ochrony Danych Osobowych (Incydencie Związanym z Ochroną Danych). Przełożony ma obowiązek niezwłocznie informować odpowiedniego Inspektora Ochrony Danych lub dział ds. prawnych i zgodności z przepisami grupy FläktGroup o znanych mu Incydentach Związanych z Ochroną Danych.

W przypadku:

- niedozwolonego przesłania danych stronom trzecim,
- niedozwolonego dostępu do Danych Osobowych przez strony trzecie,
- utraty Danych Osobowych,

należy niezwłocznie (w ciągu 24 godzin) powiadomić lokalnego Inspektora Danych Osobowych lub dział ds. prawnych i zgodności z przepisami, aby umożliwić realizację obowiązków sprawozdawczych wynikających z przepisów krajowych.

11. Obowiązki i sankcje

Odpowiedzialność za Przetwarzanie Danych przez Przedsiębiorstwo grupy FläktGroup ponosi zarząd tego przedsiębiorstwa. Tym samym zarząd ma obowiązek dbania o przestrzeganie wymogów prawnych i zapisów niniejszej Polityki Ochrony Danych, a w szczególności krajowych obowiązków sprawozdawczych. Zarząd każdego Przedsiębiorstwa grupy FläktGroup odpowiada za zgodność Przetwarzania Danych z niniejszą Polityką Ochrony Danych poprzez stosowanie odpowiednich środków organizacyjnych, personalnych i technicznych. Zapewnienie zgodności z tymi wymogami jest obowiązkiem konkretnego pracownika. Dział ds. prawnych i zgodności z przepisami grupy FläktGroup należy niezwłocznie powiadamiać o wszelkich audytach ochrony danych prowadzonych przez instytucje rządowe.

Zarząd danego przedsiębiorstwa musi wyznaczyć osobę kontaktową do spraw ochrony danych (lokalnego Inspektora Ochrony Danych) i wskazać ją działowi ds. prawnych i zgodności z przepisami. Dla uniknięcia niejasności zaznacza się, że lokalnym Inspektorem Ochrony Danych może być pracownik przedsiębiorstwa lub usługodawca zewnętrzny (osoba fizyczna).
Dział ds. prawnych i zgodności z przepisami będzie prowadzić rejestr wszystkich Inspektorów Ochrony Danych, a każdą zmianę na stanowisku Inspektora Ochrony Danych należy zgłaszać temu działowi w ciągu 48 godzin.

Lokalny Inspektor Ochrony Danych jest osobą kontaktową lokalnego przedsiębiorstwa we wszystkich sprawach dotyczących ochrony danych. Inspektor może prowadzić audyty, a dodatkowo ma obowiązek zapoznawać pracowników z treścią niniejszej Polityki Ochrony Danych. W zakresie wykonywanych obowiązków Inspektora osoba ta podlega lokalnemu kierownictwu. W celu zapewnienia centralnej koordynacji ochrony danych w całej grupie FläktGroup Inspektor regularnie informuje też dział ds. prawnych i zgodności z przepisami grupy FläktGroup o kwestiach dotyczących ochrony danych. Lokalne kierownictwo ma

obowiązek wspierać lokalnego Inspektora Ochrony Danych w wykonywaniu jego obowiązków.

Działy przedsiębiorstwa realizujące procesy biznesowe i projekty mają obowiązek informowania Inspektora Ochrony Danych z odpowiednim wyprzedzeniem o wszelkich nowych inicjatywach przetwarzania Danych Osobowych. Jeśli zaplanowano Przetwarzanie Danych, które może się wiązać ze szczególnym ryzykiem lub obejmować Dane Wysoce Wrażliwe, przed rozpoczęciem przetwarzania trzeba powiadomić lokalnego Inspektora Ochrony Danych, a w razie konieczności również dział ds. prawnych i zgodności z przepisami grupy FläktGroup.

Nieprawidłowe przetwarzanie Danych Osobowych lub innego rodzaju naruszenie przepisów ochrony danych grozi w wielu krajach postępowaniem karnym i może być podstawą do roszczeń odszkodowawczych. Naruszenia, których dopuścili się konkretni pracownicy, mogą skutkować sankcjami dyscyplinarnymi zgodnie z prawem pracy.

Zgodnie z prawem Unii Europejskiej ewentualne naruszenie przepisów ochrony danych przez przedsiębiorstwo grupy FläktGroup grozi karami do maksymalnej wysokości 20 mln euro lub 4% rocznych obrotów całej grupy FläktGroup (zależnie od tego, która kwota jest wyższa).

12. Wejście w życie

Niniejsza Polityka Ochrony Danych wchodzi w życie 25 maja 2018 r. i zastępuje wszelkie wcześniejsze przepisy dotyczące ochrony danych.
Wersja 01 aktualna na dzień 25 maja 2018 r.