

## GLOBALNA INFORMACJA O OCHRONIE DANYCH OSOBOWYCH PRACOWNIKÓW

Ostatnia aktualizacja: [30 czerwca 2023 r.]

Johnson Controls International plc. i należące do niej spółki powiązane (zwane łącznie „**Johnson Controls**”) dbają o prywatność pracowników i przetwarzają ich dane osobowe zgodnie z uczciwymi praktykami dotyczącymi ujawniania informacji oraz stosownymi przepisami o ochronie danych.

**O naszym poszanowaniu prywatności świadczą stosowane przez nas obowiązujące reguły korporacyjne (ORK). Zawierają one globalne zobowiązania spółki w zakresie ochrony prywatności, obejmujące zasady przekazywania danych osobowych i powiązane z tym prawa osób do ochrony prywatności, zapewniające ochronę danych osobowych w trakcie przetwarzania przez podmioty powiązane spółki całym światem. Reguły ORK zostały zaaprobowane przez Europejski Urząd Ochrony Danych. Wiążące reguły korporacyjne są dostępne na [Portal Prywatności](#).**

### 1. Zakres

Niniejsza informacja globalna wyjaśnia, w jaki sposób Johnson Controls przetwarza dane osobowe pracowników, kandydatów do pracy, stażystów, byłych pracowników, osób pozostających na utrzymaniu pracowników, świadczeniobiorców, wykonawców, konsultantów oraz pracowników tymczasowych w ramach prowadzenia działalności przez spółkę.

Przez dane osobowe rozumie się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, którą można zidentyfikować bezpośrednio lub pośrednio przy użyciu takich identyfikatorów, jak imię i nazwisko, numer identyfikacyjny, informacje o lokalizacji, identyfikator online, bądź jednego lub wielu cech fizycznych, fizjologicznych, genetycznych, mentalnych, ekonomicznych, kulturowych lub społecznych osoby fizycznej.

Specjalne kategorie danych osobowych (znane również jako wrażliwe dane osobowe) oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych oraz przetwarzanie danych dotyczących zdrowia lub życia seksualnego, danych genetycznych lub danych biometrycznych.

### 2. Administrator danych

Zasadniczo podmiotem Johnson Controls odpowiedzialnym za przetwarzanie danych osobowych użytkownika (często określanym jako „administrator danych”) jest podmiot Johnson Controls, z którym użytkownik pozostaje w stosunku pracy (lub, jeśli użytkownik nie jest pracownikiem, podmiot Johnson Controls jest odpowiedzialny za jego pracę). W razie jakichkolwiek wątpliwości można skontaktować się z Działem Zasobów Ludzkich lub z Biurem Ochrony Danych ([privacy@jci.com](mailto:privacy@jci.com)).

### 3. Kategorie danych osobowych

W związku z normalnym prowadzeniem działalności gospodarczej lub zarządzaniem personelem spółka przetwarza następujące kategorie danych osobowych:

- dane osobowe umożliwiające ustalenie tożsamości np. imię i nazwisko pracownika, miejsce urodzenia, adres zamieszkania, datę urodzenia, płeć, zdjęcia służbowe oraz domowy numer telefonu;
- numery identyfikacyjne wydane przez organy rządowe np. numery ubezpieczenia społecznego lub krajowe numery identyfikacyjne przetwarzane w celach związanych z wypłatą wynagrodzenia;
- status imigracyjny, prawo do pracy i status pobytu;

- dane kontaktowe rodziny pracownika i dane osoby, którą należy powiadomić w razie wypadku;
- informacje związane z pracą np. staż pracy, miejsce pracy, numer identyfikacyjny pracownika, wyniki pracy, informacje o wykorzystanym urlopie oraz informacje o zawartej umowie;
- informacje o wykształceniu i ukończonych szkoleniach np. uzyskane tytuły, świadectwa i licencje, rejestry szkolenia zawodowego oraz informacje o uczestnictwie w szkoleniach wewnętrznych;
- dane związane z rekrutacją i osiąganymi wynikami np. wyznaczone cele, oceny, komentarze, informacje zwrotne, doświadczenie zawodowe, używany sprzęt służbowy, planowanie kariery i zmian kadrowych, umiejętności i kompetencje oraz inne kwalifikacje związane z pracą i osobą;
- informacje dotyczące korzystania z zasobów Johnson Controls, w szczególności z komputerów, urządzeń mobilnych i urządzeń telekomunikacyjnych spółki oraz korzystania z Internetu;
- informacje gromadzone przez oprogramowanie do zarządzania urządzeniami mobilnymi, w tym imię i nazwisko, numer telefonu komórkowego, służbowy adres e-mail, kraj operatora sieci komórkowej oraz informacje zawarte w aplikacjach firmowych zainstalowanych na urządzeniu.
- informacje potrzebne do zarządzania ryzykiem i zgodnością z przepisami np. informacje o zastosowanych środkach dyscyplinarnych, raporty z weryfikacji informacji o osobie, dane bezpieczeństwa;
- informacje związane z listą płac, płatnością wynagrodzeń oraz wypłatą świadczeń np. stan cywilnym informacje o pensji i ubezpieczeniu, rządowe numer identyfikacyjny lub numer identyfikacji podatkowej, szczegóły rachunku bankowego, informacje o świadczeniach związanych z pracą, informacje o członkach rodziny i osobach pozostających na utrzymaniu pracownika;
- informacje związane z lokalizacją i zarządzaniem czasem pracy;
- informacje o podróżach i paszporcie;
- nagrania głosowe/wideo związane z pracą; oraz
- zdjęcia.

Ponadto spółka może przetwarzać specjalne kategorie danych osobowych pracownika np:

- informacje na temat zdrowia i chorób, takie jak objawy, diagnoza, leczenie i w razie potrzeby leki, zaświadczenia lekarskie oraz informacje o urazach i chorobach w miejscu pracy;
- informacje związane z bezpieczeństwem i higieną pracy;
- rasa i narodowość, jeśli jest to wymagane przez prawo lub dozwolone przez prawo;
- informacje biometryczne, w tym informacje dotyczące rozpoznawania twarzy, w przypadku gdy nasze lokalizacje obsługują takie systemy, zgodnie z obowiązującym prawem;
- dokładne dane dotyczące lokalizacji geograficznej, w sytuacjach, gdy wymaga tego rola użytkownika, gdy jest to dozwolone przez prawo, w tym w przypadku obsługi jednego z naszych pojazdów;
- informacje o przynależności do związków zawodowych;
- wyroki skazujące i postępowania karne oraz inne informacje dotyczące sprawdzania przeszłości (jeśli jest to dozwolone przez prawo w niektórych krajach); oraz
- w niektórych jurysdykcjach numer paszportu, numer ubezpieczenia społecznego lub krajowy numer identyfikacyjny.
- W Indiach hasła i informacje finansowe (takie jak dane konta bankowego, karty kredytowej, debetowej lub innego instrumentu płatniczego) są uważane za wrażliwe dane osobowe.

Oprócz gromadzenia danych osobowych bezpośrednio od użytkownika, możemy również gromadzić dane osobowe użytkownika z innych źródeł, np:

- organizacje rządowe, dostawcy usług zdrowotnych i świadczeń;
- dostawcy usług, np. firmy przeprowadzające weryfikację przeszłości;
- przełożeń, współpracownicy lub wyznaczeni sędziowie; oraz
- informacje dostępne publicznie.

#### 4. Cele przetwarzania danych:

Johnson Controls przetwarza dane osobowe w następujących celach:

- zasoby ludzkie i zatrudnienie, w tym planowanie siły roboczej, rekrutacja i zatrudnienie; administracja siłą roboczą, lista płac, programy wynagrodzeń i świadczeń, zarządzanie wydajnością, nauka i rozwój, awans i planowanie sukcesji;
- fuzje, przejęcia i zbycia;
- zapewnienie zgodności z przepisami, w tym zarządzanie przedsiębiorstwem, spełnienie żądań ze strony organów rządowych o podanie informacji, ustanowienie zastawów, zajęcie wynagrodzenia oraz w celu zachowania zgodności z przepisami podatkowymi;
- zarządzanie miejscem pracy np. programami podróży i wydatków oraz programami bezpieczeństwa i higieny pracy;
- sprawozdawczość wewnętrzna;
- przeprowadzanie kontroli;
- ochrony spółki Johnson Controls, jej pracowników oraz społeczeństwa przed szkodą, kradzieżą, odpowiedzialnością prawną, oszustwem, nadużyciem lub innego rodzaju naruszeniem;
- szkolenia i prezentacje produktów;
- rozwój produktu, który angażowałby lub odnosił się do pracowników; oraz
- w innych celach prawnych i typowo związanych z prowadzeniem działalności.

Ponadto Johnson Controls monitoruje i filtruje informacje o korzystaniu z urządzeń służbowych, sieci spółki oraz Internetu w celach zgodnych z prawem, a w szczególności w celu:

- zapewnienia integralności odpowiednich systemów informatycznych oraz wykrywania i zapobiegania działalności przestępczej w tym cyberprzestępczości;
- ochrony informacji w tym m.in. danych osobowych, informacji poufnych oraz cennych informacji biznesowych przed ich zniszczeniem, utratą, zmianą, wglądem ze strony osób nieupoważnionych, ujawnieniem lub włamaniem do nich;
- bezpiecznego i skutecznego działania systemów informatycznych spółki;
- zapewnienia zgodności z obowiązującymi obowiązkami regulacyjnymi lub samoregulacyjnymi oraz
- wykrycia przypadków niezgodności z zasadami postępowania Johnson Controls dotyczącymi korzystania z Internetu oraz przypadków naruszeń Kodeksu etyki.

W przypadku gdy na urządzeniu osobistym użytkownika zainstalowano oprogramowanie do zarządzania urządzeniami mobilnymi (w celu umożliwienia użytkownikowi dostępu do poczty elektronicznej, usług sieciowych i danych Johnson Controls), może być konieczne wprowadzenie zmian przez firmę Johnson Controls w konfiguracji zabezpieczeń urządzenia w celu zapewnienia zgodności z wymogami firmy w zakresie bezpieczeństwa urządzeń mobilnych. Wszelkie monitorowanie i/lub filtrowanie korzystania z tego urządzenia do wyżej wymienionych celów jest ograniczone do zastosowań korporacyjnych. Więcej informacji można znaleźć w sekcji „Kontakt z nami” poniżej.

#### 5. Podstawy prawne przetwarzania danych

Przetwarzamy dane osobowe użytkownika w oparciu o jedną z następujących podstaw:

- w przypadku, gdy przetwarzanie jest niezbędne do wykonania przez nas umowy z użytkownikiem, np. w celu rekrutacji, wypłaty wynagrodzenia i zarządzania stosunkiem pracy z użytkownikiem;
- gdy przetwarzanie jest niezbędne do celów wynikających z naszych prawnie uzasadnionych interesów, takich jak sprawozdawczość wewnętrzna i audyt; ochrona Johnson Controls, jej pracowników i społeczeństwa przed obrażeniami, kradzieżą, odpowiedzialnością prawną, oszustwem lub nadużyciem lub innymi obrażeniami; zapewnienie integralności systemów informatycznych; zapewnienie zgodności z obowiązującymi zobowiązaniami regulacyjnymi i politycznymi; w związku z fuzjami, przejęciami i zbyciem; rozwojem produktów; szkoleniami i demonstracjami produktów; spotkaniami i rozmowami biznesowymi.
- W przypadku gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego, takiego jak cele podatkowe i ubezpieczenia społecznego; sprawdzenie prawa do pracy; zgodność z żądaniami organów rządowych; zastawy, zajęcia i zgodność z przepisami podatkowymi; oraz
- jeśli użytkownik wyraził na to zgodę.

Przetwarzamy Specjalne kategorie danych osobowych w oparciu o jedną z następujących podstaw:

- w przypadku udzielenia przez użytkownika wyraźnej zgody;
- gdy przetwarzanie jest niezbędne do celów wypełniania obowiązków i wykonywania praw w związku z prawem pracy;
- w przypadku gdy przetwarzanie dotyczy danych osobowych, które są wyraźnie upublicznione przez użytkownika; oraz
- gdy przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń prawnych.

## 6. Odbiorcy danych osobowych

Spółka może ujawniać dane osobowe pracownika w następujących okolicznościach:

- innym podmiotom Johnson Controls, jej spółkom typu joint venture, podwykonawcom, usługodawcom lub dostawcom, którzy świadczą usługi w imieniu spółki w wyżej wymienionych celach;
- nowo utworzonej lub przejmowanej organizacji, jeśli Johnson Controls jest stroną połączenia, sprzedaży lub przeniesienia części lub całości jej aktywów;
- zewnętrznymi dostawcami usług (którzy pomagają nam w prowadzeniu działalności biznesowej), tacy jak dostawcy IT, dostawcy świadczeń, dostawcy usług płacowych i doradcy (na przykład prawnicy, księgowi i audytorzy);
- dowolnemu odbiorcy, jeśli spółka ma obowiązek to uczynić np. na podstawie stosownego nakazu sądu lub przepisów prawa;
- dowolnego odbiorcy za zgodą pracownika np. w celu weryfikacji zatrudnienia lub udzielenia pożyczki bankowej lub
- dowolnemu odbiorcy w uzasadnionych przypadkach np. w przypadku sytuacji zagrażającej życiu.

## 7. Międzynarodowe przekazanie danych

Strony trzecie, podmioty zależne i powiązane, którym mogą być ujawniane dane osobowe pracownika, mogą być zlokalizowane na całym świecie. W związku z tym dane te mogą być przesyłane do krajów, gdzie obowiązują standardy ochrony prywatności inne niż obowiązujące w kraju zamieszkania osoby, której dane dotyczą. W takich przypadkach Johnson Controls podejmie działania zapewniające odpowiedni poziom ochrony danych osobowych w tym stosowanie wiążących reguł korporacyjnych wyznaczających wysokie standardy w zakresie przetwarzania danych osobowych, a także standardowych warunków umownych. W wymaganych przypadkach oraz zgodnie zobowiązującym prawem lokalnym spółka może zażądać od pracownika zgody na przekazanie jego

danych osobowych do innego kraju.

Transgraniczny system zasad prywatności APEC: Praktyki prywatności przyjęte w firmie Johnson Controls, opisane w niniejszej Polityce prywatności, zgodne są z transgranicznym systemem zasad prywatności APEC. System APEC zapewnia ramy dla organizacji, które zapewniają ochronę danych osobowych przekazywanych w ramach gospodarek uczestniczących w tym systemie. Więcej informacji na temat ram APEC można znaleźć [tutaj](#). Kliknij [tutaj](#), aby wyświetlić nasz status certyfikacji APEC CBPR.

W przypadku problemu z prywatnością albo wykorzystaniem danych, który nie został przez nas odpowiednio rozwiązany, prosimy o kontakt (nieodpłatnie) z naszym amerykańskim podmiotem zajmującym się rozstrzyganiem sporów pod adresem: <https://feedback-form.truste.com/watchdog/request>.

## 8. Zatrzymywanie danych

Dane osobowe będą zatrzymane przez okres konieczny dla realizacji celu, w jakim zostały zgromadzone, zwykle przez okres obowiązywania umowy, a także przez okres późniejszy w zakresie wymaganym lub dozwolonym obowiązującymi przepisami prawa. Harmonogram zatrzymania danych osobowych przez Johnson Controls dostępny jest na stronie: <https://my.jci.com/Ethics/Pages/RIM.aspx>.

## 9. Ochrona i bezpieczeństwo

Johnson Controls stosuje środki ostrożności w celu ochrony danych osobowych przed utratą, niewłaściwym wykorzystaniem, wglądem do nich przez osoby nieuprawnione, ujawnieniem, zmianą i zniszczeniem. Spółka stosuje odpowiednie środki techniczne i organizacyjne w celu ochrony systemów informatycznych, na których przechowywane są dane osobowe pracownika oraz wymaga od swoich dostawców i usługodawców, aby chronili dane osobowe pracowników zgodnie z umową i na inne sposoby.

## 10. Twoje prawa

Prawa pracowników mogą być różne w zależności od prawa miejscowego. Spełniając żądania pracowników wymienione poniżej, a dotyczące danych osobowych, Johnson Controls będzie postępować zgodnie z prawem lokalnym.

- Informacje o danych oraz wgląd do danych osobowych: Pracownik może zażądać wglądu do swoich danych osobowych, otrzymać informacje dodatkowe oraz otrzymać kopie swoich danych osobowych. Prawo do uzyskania informacji oraz wgląd do danych osobowych ma pewne ograniczenia. Przykładowo spółka może odmówić wglądu do danych osobowych (i) w przypadku wielokrotnych żądań wglądu do danych osobowych składanych w krótkim okresie czasu lub (ii) jeżeli wgląd do danych lub poprawa danych osobowych naruszyłyby prawo do prywatności innej osoby lub bezpodstawnie naraziłoby na ryzyko wrażliwe informacje spółki.
- Sprostowanie swoich danych osobowych: Pracownik może zażądać sprostowania i/lub aktualizacji swoich niezrzetelnych lub nieaktualnych danych osobowych.
- Usunięcie swoich danych osobowych: Pracownikowi może przysługiwać prawo usunięcia swoich danych osobowych. Prawo takie może mieć pewne ograniczenia.
- Ograniczenia zakresu przetwarzania danych: Pracownikowi może przysługiwać prawo ograniczenia zakresu przetwarzania swoich danych osobowych. Ograniczenie zakresu przetwarzania danych osobowych oznacza, że dane osobowe będą przechowywane wyłącznie przez Johnson Controls i nie będą przetwarzane podczas rozstrzygnięcia skargi pracownika.
- Sprzeciw wobec przetwarzania danych: Pracownikowi może przysługiwać prawo złożenia sprzeciwu wobec określonych rodzajów przetwarzania danych. Obejmuje to marketing bezpośredni, przetwarzanie w celach badawczych lub statystycznych oraz przetwarzanie w oparciu o prawnie uzasadnione interesy. Johnson Controls może wykazać podstawy tego, że jej prawnie uzasadnione interesy są nadrzędne w

stosunku do prawa wniesienia sprzeciwu wobec przetwarzania danych.

- Prawo do przenoszenia danych: Pracownikowi może przysługiwać prawo zażądania przeniesienia danych. Przenoszenie danych oznacza przesłanie przez pracownika lub Johnson Controls innemu podmiotowi danych osobowych pracownika w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Prawo do przenoszenia danych podlega pewnym ograniczeniom. Przykładowo prawo do przenoszenia danych nie dotyczy rejestrów w formie papierowej i nie może niekorzystnie wpływać na prawa innych osób lub informacje wrażliwe spółki.
- Prawo do niepodlegania decyzjom podejmowanym wyłącznie w oparciu o zautomatyzowane przetwarzanie: Pracownikowi może przysługiwać prawo do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu (tj. bez interwencji ludzkiej), jeśli decyzje te wywołują skutki prawne lub znacząco na niego wpływają. Zautomatyzowane przetwarzanie to przetwarzanie danych osobowych w sposób zautomatyzowany. Jeśli wdrazamy przetwarzanie, które wykorzystuje zautomatyzowane podejmowanie decyzji, wywołujące skutki prawne lub mające znaczący wpływ na użytkownika, użytkownik ma prawo nie podlegać decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu.

Użytkownikowi przysługuje również prawo wniesienia skargi do organów sprawujących nadzór.

Aby skorzystać z przysługujących mu praw, pracownik powinien skontaktować się z pracownikiem lokalnego Działu Zasobów Ludzkich lub Biurem Ochrony Prywatności, pisząc na adres [privacy@jci.com](mailto:privacy@jci.com).

## 11. Zgoda i wycofanie zgody

Jeśli dane osobowe lub specjalne kategorie danych osobowych pracownika są przetwarzane na podstawie udzielonej przez niego zgody, pracownik ma prawo w dowolnym momencie wycofać udzieloną wcześniej zgodę na przetwarzanie danych w konkretnym celu; może to uczynić bezpłatnie, kontaktując się z Biurem Ochrony Danych na adres: [privacy@jci.com](mailto:privacy@jci.com).

## 12. Modyfikacje naszej Polityki prywatności

W razie konieczności spółka może wprowadzać zmiany do niniejszej informacji. Jeśli zaproponujemy wprowadzenie znaczących zmian, powiadomimy o tym użytkownika, umieszczając odpowiednią informację na tej stronie. Zapisy niniejszej informacji mogą zostać również uzupełnione w ten sposób, aby dostosować je do wymogów prawa lokalnego obowiązującego w kraju zamieszkania pracowników lub kraju stosowania umowy o przedstawicielstwo.

## 13. Wątpliwości dotyczące ochrony prywatności oraz kontakt ze spółką

Jeśli pracownik ma pytania dotyczące niniejszej informacji lub sądzi, że jego dane osobowe są przetwarzane niezgodnie z obowiązującym prawem lub zasadami określonymi w niniejszej informacji, może on:

- skontaktować się z Biurem Ochrony Prywatności, pisząc na adres [privacy@jci.com](mailto:privacy@jci.com);
- omówić sprawę ze swoim przełożonym lub innym przełożonym lub kierownikiem;
- skontaktować się Działem Zasobów Ludzkich lub
- można również skontaktować się z całodobową infolinią Integryty Helpline firmy Johnson Controls pod adresem: [www.johnsoncontrolsintegrityhelpline.com](http://www.johnsoncontrolsintegrityhelpline.com).