Regulamin ochrony danych osobowych

w FAST FOOD FRANCHISING GROUP EU SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

I. PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

1. Pracownicy, współpracownicy i inne osoby mające dostęp do danych osobowych, których Administratorem jest spółka FAST FOOD FRANCHISING GROUP EU SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ (dalej również: Administrator) zobowiązani są do przestrzegania zapisów niniejszego regulaminu oraz przepisów prawa regulujących kwestie ochrony danych osobowych, tj. Rozporządzenie 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* i Ustawa z dnia 10.05.2018 r. *o ochronie danych osobowych*.
2. Osoby przetwarzające dane osobowe przed dopuszczeniem ich do przetwarzania danych osobowych zapoznają się z niniejszym Regulaminem. Osoby przetwarzające dane osobowe wskazuje Zarząd.
3. Osoby zapoznane z treścią Regulaminu ochrony danych osobowych zobowiązane są podpisać Oświadczenie o poufności.
4. Zakres przetwarzania danych osobowych obejmuje: nazwisko, imiona, PESEL, e-mail, telefon, adres: miejscowość, ulica, nr budynku, numer lokalu, kod pocztowy, powiat, województwo, pocztę, NIP, Regon, numer dowodu osobistego, numer paszportu (przy braku numeru PESEL lub dowodu osobistego).
5. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a) przetwarzania danych osobowych wyłącznie w zakresie i celu określonym przez Administratora danych,
   b) zachowania w tajemnicy danych osobowych, do których ma dostęp w związku z wykonywanymi zadaniami, właściwymi do zajmowanego stanowiska,
   c) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych stosowanych przez Administratora,
   d) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych,

nieuprawnionym ujawnieniem, dostępem do danych osobowych oraz przetwarzaniem.

6. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie wykazują się podstawą prawną uprawniającą do dostępu do takich danych.
7. Zabrania się przekazywania bezpośrednio lub za pomocą środków porozumiewania się na odległość danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zidentyfikować.
8. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do odbycia szkolenia w zakresie ochrony danych osobowych.

II. UŻYTKOWANIE SPRZĘTU ELEKTRONICZNEGO

1. Każdy użytkownik przetwarzający dane osobowe za pomocą sprzętu elektronicznego (np. na komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) posiada swój własny indywidualny identyfikator (login) do logowania się i hasło. Dostęp do danych osobowych nie jest możliwy bez podania indywidualnego loginu i hasła. Zabronione jest umożliwianie innym osobom korzystanie z własnego konta.
2. Każde trwałe odejście od sprzętu elektronicznego, na którym znajdują się dane osobowe (opuszczenie miejsca pracy, zakończenie pracy itp.) winno być poprzedzone wylogowaniem z systemu, tak aby dane nie były dostępne osobom nieupoważnionym.
3. W czasie przetwarzania danych osobowych sprzęt wyświetlający dane osobowe winien być ustawiony w sposób uniemożliwiający wgląd osobom nieuprawionym do przetwarzania danych osobowych.
4. W pomieszczeniu, w którym odbywa się przetwarzanie danych osobowych nie mogą przebywać bez nadzoru osoby nieupoważnione do przetwarzania danych osobowych.
5. Zakończenie pracy wiąże się z zakończeniem działania oprogramowania wykorzystywanego do przetwarzania danych osobowych.
6. Wszystkie osoby przetwarzające dane osobowe, korzystające ze sprzętu elektronicznego (np. z komputerów stacjonarnych, laptopów, monitorów, drukarek, skanerów, urządzeń kserujących, służbowych tabletów i telefonów) mają obowiązek jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem.
7. Zabronione jest samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie

jakichkolwiek niedopuszczonych przez administratora urządzeń lub systemów do systemu informatycznego Administratora.

8. W przypadku zagubienia, utraty lub zniszczenia sprzętu użytkownik ma obowiązek natychmiast zgłosić takie zdarzenie administratorowi danych bądź powołanemu Inspektorowi ochrony danych osobowych.
9. Należy używać programu antywirusowego. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

III. POLITYKA HASEŁ

1. Można używać od 8 do 16 znaków, w tym wielkich i małych liter, cyfr oraz znaków specjalnych (!"#$%&'()*+,-./:;<=>?@[]^_`{|}~ i spacji). Hasło musi zawierać co najmniej dwa różne typy wymienionych znaków.
2. Zabronione jest udostępnianie swoich haseł nieuprawnionym osobom. W przypadku ujawnienia hasła – należy dokonać niezwłocznej zmiany.
3. Nie dopuszcza się zapisywania haseł.

IV. ZASADY POSTĘPOWANIA Z DOKUMENTACJĄ PAPIEROWĄ, ZAWIERAJĄCĄ DANE OSOBOWE

1. Osoby pracujące z danymi osobowymi zobowiązane są zabezpieczać dokumenty zawierające dane osobowe przed kradzieżą lub wglądem osób nieupoważnionych zarówno w czasie godzin pracy, jak i po jej zakończeniu.
2. Osoby przetwarzające dane osobowe zobowiązane są niszczyć niepotrzebną dokumentację i jej wydruki zawierające dane osobowe w niszczarkach.
3. Zabronione jest pozostawianie dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, poza siedzibą Administratora.

V. WYNOSZENIE NOŚNIKÓW Z DANYMI POZA SIEDZIBĘ ADMINISTRATORA

1. Użytkownicy nie mogą wynosić na zewnątrz wymiennych elektronicznych nośników informacji (np. twardych dysków, pendriveów, pamięci typu flash, płyt) z zapisanymi danymi osobowymi bez zgody administratora danych lub inspektora ochrony danych osobowych.
2. Jeżeli dokumenty przewozi pracownik, to on jest odpowiedzialny za zabezpieczenie przewożonych dokumentów przed zgubieniem i kradzieżą.

3. Dane osobowe w wersji papierowej muszą być bezpiecznie przewożone np. w torbach, plecakach, teczkach. W razie możliwości należy korzystać ze sprawdzonych firm kurierskich
4. W przypadku gdy dane na takich nośnikach są wynoszone poza siedzibę Administratora powinny być właściwie zaszyfrowane.

VI. KORZYSTANIE Z INTERNETU

1. Zabronione jest uruchamianie jakichkolwiek nielegalnych programów oraz plików pobranych z niewiadomych źródeł. W przypadku takich działań użytkownik ponosi odpowiedzialność za szkody spowodowane przez takie oprogramowanie.
2. Administrator wprowadził ograniczenia w dostępie do stron internetowych, dlatego zabronione jest wchodzenie na strony budzące podejrzenia co do ich zgodności z prawem oraz zasadami bezpieczeństwa.
3. W opcjach przeglądarki internetowej nie należy włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

VII. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

1. E-mail służbowy należy wykorzystywać wyłącznie do wykonywania obowiązków służbowych.
2. Nie należy wysyłać korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
3. W przypadku wysyłania dokumentacji zawierającej dane osobowe za pośrednictwem poczty elektronicznej należy zabezpieczać je hasłami, a hasło udostępnić w inny sposób niż drogą e-mail.
4. Należy zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Przed otwarciem załączników (plików) w mailach zawsze należy przeprowadzić wcześniejszą weryfikację nadawcy oraz weryfikację bezpieczeństwa pliku np. przy użyciu programu antywirusowego.
6. Zabronione jest „klikanie” na hiperlinki pochodzące z adresów niezweryfikowanych.
7. W przypadku wysyłania poczty elektronicznej do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.
8. Użytkownik bez zgody Administratora nie może wysyłać wiadomości zawierających dane osobowe dotyczące Administratora, jego pracowników,

klientów, dostawców, kontrahentów oraz osób które udostępniły dane osobowe, za pośrednictwem prywatnej elektronicznej skrzynki pocztowej.

VIII. ZGŁASZANIE NARUSZEŃ ODPOWIEDZIALNOŚĆ DYSCYPLINARNA

1. Każda osoba mająca dostęp do danych osobowych obowiązana jest do niezwłocznego poinformowania Administratora o każdym naruszeniu lub podejrzeniu naruszenia obowiązków w zakresie danych osobowych.
2. Przypadki świadomego naruszenia regulacji Regulaminu ochrony danych osobowych lub nieuzasadnionego zaniechania obowiązków mogą zostać uznane przez Administratora za ciężkie naruszenie obowiązków pracowniczych oraz za naruszenie przepisów karnych zawartych w RODO.