POLITYKA OCHRONY DANYCH OSOBOWYCH

W GRATIFICA SP. Z O.O.

1 OGÓLNE ZASADY OCHRONY DANYCH W GRATIFICA SP. Z O.O.

1. Jako administrator danych Gratifica Sp. z o.o. (dalej „Gratifica") działa z poszanowaniem wymogów i zasad ochrony danych osobowych wynikających z przepisów 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) [Dz.U.UE.L.2016.119.1] oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j.: Dz. U. z 2019 r., poz. 1781) i innych przepisów o ochronie danych osobowych.
2. Ochrona danych osobowych w Gratifica realizowana jest poprzez zastosowanie adekwatnych środków technicznych i organizacyjnych służących ochronie danych osobowych, z uwzględnieniem charakteru, zakresu, kontekstu, celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.
3. Gratifica dokłada należytej staranności w celu zapewnienia:
    a) Poufności danych,
    b) Integralności danych,
    c) Rozliczalności danych,
    d) Integralności stosowanych systemów.

4. Zasady określone w niniejszym dokumencie mają zastosowanie do danych osobowych przetwarzanych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania danych w sposób tradycyjny (papierowy) i obowiązują wszystkie osoby dopuszczone do przetwarzania przez Administratora.
5. Standard ochrony danych ustalony przez Administratora musi być zachowany także w przypadku powierzenia przetwarzania danych innemu podmiotowi, które zawsze stwierdzone być musi umową powierzenia przetwarzania zgodnie z wymogami art. 28 RODO.
6. Administrator dba o to, by w przypadku przetwarzania prowadzonego na zasadzie współadministrowania, przetwarzanie spełniało standard ochrony ustalony w Polityce lub wyższy.
7. Ze względu na skalę prowadzonej działalności i strukturę organizacji, Administrator wykonuje obowiązki związane z ochroną danych osobowych poprzez przedstawicieli swoich organów.

2 OBOWIĄZKI ADMINISTRATORA

1. Administrator:

    a) prowadzi i aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych,
    b) weryfikuje i zapewnia legalność przetwarzania danych,

c) zapewnia odpowiednią autoryzację dostępu do danych oraz zapewnia zapoznanie każdej osoby, która otrzymuje upoważnienie do przetwarzania danych z zasadami obowiązującymi w Gratifica w zakresie ochrony danych osobowych,
d) zapewnia użytkownikom odpowiednie stanowiska pracy, w tym sprzęt informatyczny, umożliwiające bezpieczne i zgodne z prawem przetwarzanie danych osobowych,
e) odpowiada za spełnienie obowiązku prowadzenia rejestru czynności przetwarzania danych osobowych,
f) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zasad bezpiecznego przetwarzania danych osobowych,
g) nadzoruje przeprowadzanie regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych osobowych,
h) nadzoruje proces wykonania analizy ryzyka,
i) odpowiada za przeprowadzenie oceny skutków dla ochrony danych osobowych w sytuacji, gdy wymagają tego przepisy prawa,
j) prowadzi z osobami, których dane dotyczą wszelką komunikację w związku z realizacją żądań na mocy art. 12 oraz art. 15-22 RODO.

2. Do przetwarzania danych u Administratora dopuszczone być mogą wyłącznie osoby upoważnione do przetwarzania danych osobowych w indywidualnie określonym zakresie, odpowiadającym zakresowi ich obowiązków. Administrator prowadzi ewidencję upoważnień.
3. W przypadku przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, Administrator dokonuje oceny możliwości takiego przekazania z uwzględnieniem regulacji Rozdziału V RODO, a transfer odbywa się wyłącznie po spełnieniu wymogów określonych przepisami RODO.
4. Administrator przetwarza dane dokładając należytej staranności w celu zabezpieczenia praw i wolności osób, których dane dotyczą, w tym:

a) Realizuje obowiązek informacyjny, o którym mowa w art. 13 RODO w przypadku zbierania danych bezpośrednio od osoby, której dane dotyczą oraz obowiązek określony w art. 14 RODO, jeżeli dane zbierane są niebezpośrednio od podmiotu danych;
b) W celu prawidłowej realizacji obowiązków informacyjnych Administrator stosuje ustalone wzory klauzul informacyjnych dla poszczególnych grup osób;
c) Na każde żądanie podmiotu danych złożone zgodnie z przepisami RODO, udziela podmiotowi danych informacji o przetwarzaniu;
d) Realizuje obowiązek sprostowania lub uzupełnienia niekompletnych danych osobowych przypadku zgłoszenia takiego żądania przez podmiot danych odnotowując dla celów dowodowych zgłoszenie takiego żądania;
e) Po spełnieniu przesłanek określonych w art. 17 RODO, realizuje na żądanie podmiotu danych prawo do usunięcia danych;
f) Po spełnieniu przesłanek określonych w art. 18 RODO, realizuje na żądanie podmiotu danych prawo do ograniczenia przetwarzania danych;
g) W przypadku przetwarzania danych w oparciu o uzasadniony interes respektuje prawo do zgłoszenia sprzeciwu, jeżeli spełnione są warunki określone w art. 21 RODO.

5. Administrator przetwarza dane z poszanowaniem zasady *Privacy by Design* tj. zgodnie z zasadą ochrony danych w fazie projektowania. Oznacza to, że Administrator wdraża odpowiednie środki techniczne i organizacyjne zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, uwzględniając:
   a) stan wiedzy technicznej;
   b) koszt wdrażania;
   c) charakter, zakres, kontekst i cele przetwarzania;
   d) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

6. Administrator przetwarza dane z poszanowaniem zasady *Privacy by Default* tj. zgodnie z zasadą domyślnej ochrony danych. Oznacza to, że Administrator wdraża odpowiednie środki techniczne i organizacyjne, by domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągniecia danego celu przetwarzania.
7. Administrator uwzględnia ochronę danych od początku każdego procesu, dbając o odpowiednią analizę zarówno zakresu gromadzonych danych jak i stosowanych środków bezpieczeństwa i dba o zachowanie należytego standardu ochrony danych aż do momentu ich nieodwracalnego usunięcia.
8. Dane osobowe przetwarzane są przez Administratora przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Po osiągnięciu celów przetwarzania dane powinny zostać usunięte albo zanonimizowane.
9. Okresy retencji poszczególnych procesów przetwarzanych danych osobowych zostały uwzględnione w rejestrze czynności przetwarzania danych osobowych, stanowiącym Załącznik nr 6 do Polityki.

3 ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Zadania Administratora Systemu Informatycznego w Gratifica realizuje Webconstructor z siedzibą przy ul. Bartoka 29, Łódź (92-546), którego zadania obejmują:
   a) Wdrażanie środków bezpieczeństwa w systemach informatycznych,
   b) przydzielanie każdemu użytkownikowi identyfikatora i hasła do systemu informatycznego oraz dokonywanie ewentualnych modyfikacji uprawnień, w tym usuwanie kont użytkowników i ich wyrejestrowywanie na polecenie Administratora,
   c) zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem administracyjnym dostępu do wszystkich stacji roboczych i serwerów z pozycji Administratora,
   d) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
   e) nadzór nad prawidłowym działaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych i kontroli identyfikatorów dostępu do systemu informatycznego,
   f) współdziałanie z Administratorem w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego,
   g) nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe,
   h) nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
   i) działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4 OBOWIĄZKI PERSONELU ADMINISTRATORA

1. Zadania i obowiązki personelu Administratora związane z ochroną danych oraz wytyczne co do sposobu postepowania w celu zapewnienia należytej ochrony danych ujęte są w Regulaminie Ochrony Danych Osobowych stanowiącym załącznik nr 1 do Polityki ochrony danych Gratifica.

5 ŚRODKI TECHNICZNE I FIZYCZNE OCHRONY DANYCH

1. W siedzibie Administratora zastosowano następujące zabezpieczenia:
   a) Siedziba znajduje się w niezależnym budynku, do którego dostęp z zewnątrz jest ograniczony. Budynek jest ogrodzony, a wejście na teren obiektu możliwe jest po użyciu domofonu przy furtce lub otwarciu bramy.
   b) Budynek jest wyposażony w system monitoringu wizyjnego (monitoring wewnętrzny i zewnętrzny).
   c) Okna budynku wyposażone są w system rolet antywłamaniowych.
   d) Dostęp do pomieszczeń biurowych jest ograniczony poprzez 2 pary drzwi.
   e) Klucze do budynku posiadają wyłącznie upoważnione osoby oraz Administrator.
   f) Pilot do bramy wjazdowej oraz magazynu znajdują się w dyspozycji Administratora oraz najstarszego stażem pracownika.
   g) W budynku rozmieszczone są gaśnice.
2. Siedziba Administratora wykorzystywana jest wyłącznie przez personel Gratifica.
3. Sprzątanie siedziby odbywa się wyłącznie w godzinach pracy i pod nadzorem Administratora lub wyznaczonego pracownika.
4. Dla serwerów, na których przechowywane są systemy, bazy danych oraz kopie bezpieczeństwa, wykorzystano urządzenia zapewniające podtrzymanie źródła zasilania (UPS), na wypadek awarii sieci lub przerw w dostawie zasilania.
5. Stacje robocze wykorzystują oprogramowanie chroniące przed zagrożeniami – stosowany jest program antywirusowy Eset.
6. Zastosowano metody uwierzytelniające do systemów informatycznych, za pomocą których przetwarzane są dane osobowe.
7. Zastosowano wygaszacze ekranu, zabezpieczające dostęp do stacji roboczych w momencie nieaktywności użytkownika.
8. Wykorzystywane telefony komórkowe posiadają podstawowe środki zabezpieczenia dostępu (hasło, wężyk, kod) oraz zabezpieczone są programem antywirusowym Eset.
9. Sieć bezprzewodowa (wi-fi) nie jest dostępna dla osób trzecich oraz zabezpieczono ją odpowiednim hasłem. Administrator dysponuje także siecią wi-fi dla gości, niezależną od sieci podstawowej.
10. Sieć wykorzystywana przez Administratora zabezpieczona jest firewallem.
11. U Administratora uregulowano proces dodawania użytkowników oraz zasady nadawania uprawnień. Dodawanie nowych użytkowników, modyfikowanie uprawnień lub ich odbiór możliwe są wyłącznie po uzyskaniu zgody Administratora, który ww. czynności wykonuje osobiście lub zleca ich wykonanie osobie odpowiedzialnej za IT.
12. W przypadku korzystania z przenośnych nośników danych, nośniki są szyfrowane (wykorzystywany jest Bitlocker).
13. Dla systemów, za pomocą których przetwarzane są dane osobowe, tworzona jest kopia bezpieczeństwa (backup) na serwerze własnym Administratora, serwerze dedykowanym dostarczanym przez OVH lub na zasobach hostingodawcy (home.pl).

14. Użytkownicy korzystają z dysku współdzielonego z zachowaniem gradacji i podziału uprawnień nadawanych przez Administratora zgodnie z zakresem zadań i obowiązków danego Użytkownika.
15. Administrator przechowuje zasoby zawierające dane osobowe na dedykowanym serwerze dostarczanym przez OVH i serwerze własnym spółki (SYNOLOGY 8TB), na którym zainstalowano oprogramowanie antywirusowe (ESET). Doraźnie wykorzystywany jest przenośny dysk SSD.
16. Łączenie z serwerem następuje przez VPN.
17. Losy i zgłoszenia udziału w konkursach przechowywane są w kopertach bąbelkowych, zabezpieczonych plombami Administratora, w szafkach ognioodpornych, do których klucze ma Administrator. Szafki usytuowane są w niezależnym, zamykanym na klucz pomieszczeniu w siedzibie Administratora.

6 ŚRODKI ORGANIZACYJNE

1. Administrator opracował niezbędną dokumentację ochrony danych.
2. Do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez Administratora. Wzór upoważnienia pisemnego stanowi Załącznik nr 4 do Polityki. Administrator dopuszcza przekazywanie informacji o upoważnieniu oraz zakresie nadanych uprawnień drogą elektroniczną, zgodnie ze wzorem z Załącznika nr 5 do Polityki.
3. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
4. Osoby, które przetwarzają dane osobowe z upoważnienia Administratora zostały zapoznane z zasadami ochrony danych osobowych.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane są do zachowania tych danych oraz sposobów ich zabezpieczenia w tajemnicy. Wzór oświadczenia o poufności stanowi Załącznik nr 6 do Polityki.
6. W przypadku powierzenia przetwarzania danych stosuje się umowy powierzenia zgodnie z art. 28 RODO.
7. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej oraz w warunkach zapewniających bezpieczeństwo danych.
8. W przypadku niszczenia dokumentów, a w szczególności w przypadku niszczenia losów, zdrapek, kuponów, formularzy zgłoszeniowych do loterii, Administrator korzysta z usług profesjonalnych firm, legitymujących się odpowiednim certyfikatem ISO, a zniszczenie dokumentów potwierdza odpowiednim protokołem.

7 UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Udostępnienie danych osobowych przez Administratora możliwe jest wyłącznie w przypadku spełnienia przesłanek przetwarzania określonych w art. 6 lub 9 RODO, w tym także po otrzymaniu wniosku o przekazanie określonych informacji.
2. Wniosek o udostępnienie danych podlega każdorazowo ocenie pod kątem zasadności.
3. Wniosek o udostępnienie danych powinien mieć formę pisemną i zawierać:
   a) oznaczenie wnioskodawcy;
   b) wskazanie celu udostępnienia danych;
   c) wskazanie przepisów uprawniających do dostępu do informacji;

d) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia;
e) wskazanie imienia (imion) i nazwiska osoby upoważnionej do pobrania informacji lub zapoznania się z ich treścią.

4. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe elementy pisemnego wniosku może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania po bezsprzecznej identyfikacji osoby żądającej informacji.
5. Osoba udostępniająca dane osobowe jest obowiązana zażądać od osoby uprawnionej pokwitowania udostępnienia danych zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.
6. Jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie otrzymania informacji. Jeżeli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje odnotowuje powyższą informację w rejestrze udostępnień danych osobowych.
7. Jeśli osoba uprawniona pouczyła osobę udostępniającą informacje o konieczności zachowania w tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępnienia informacji.
8. Administrator lub osoba przez niego upoważniona prowadzi rejestr udostępnień danych osobowych realizowanych na wniosek w celu zapewnienia kontroli procesu udostępnień według załącznika nr 2 do Polityki.

8 POSTĘPOWANIE W PRZYPADKU PODEJRZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Instrukcja postępowania w przypadku podejrzenia naruszenia ochrony danych osobowych zawarta jest w rozdziale 9 Regulaminu ochrony danych osobowych stanowiącego załącznik nr 1 do Polityki i wskazuje na zadania i obowiązki personelu Administratora w przypadku podejrzenia wystąpienia naruszenia ochrony danych osobowych.
2. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności zdarzenia, jego skutki i potencjalne skutki oraz podjęte i planowane do wdrożenia środki i działania zaradcze.
3. W celu prowadzenia prawidłowej dokumentacji naruszeń, Administrator posługuje się wzorem raportu naruszeń, który stanowi załącznik nr 3 do Polityki.
4. Za wypełnienie raportu odpowiada osoba odpowiedzialna za ochronę danych w Gratifica wraz z informatykiem Gratifica, jeżeli okoliczności zdarzenia uzasadniają udział informatyka.
5. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości – nie później, niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych.
6. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu powinno co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, z zastrzeżeniem, że w Gratifica inspektor nie został wyznaczony, ale ustalono osobę odpowiedzialną za ochronę danych;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

   d) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
7. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu. Zawiadomienie to musi być napisane jasnym i prostym językiem i ma wskazywać charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w pkt 6 lit. b, c i d powyżej.
8. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych nie jest wymagane w następujących przypadkach:
   a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   c) Zawiadomienie wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane równie w skuteczny sposób.

9 POSTANOWIENIA KOŃCOWE

1. Wszelkie wątpliwości dotyczące interpretacji postanowień Polityki powinny być w sposób zapewniający możliwie najwyższy poziom ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.
2. Polityka lub odpowiednie załączniki podlegają aktualizacji każdorazowo w przypadku zmiany zakresu lub sposobu przetwarzania danych, a także w przypadku zmiany przepisów prawa dotyczących ochrony danych osobowych, wymagającej aktualizacji Polityki. Nowa wersja Polityki zastępuje poprzednio obowiązującą.
3. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.