Regulamin Bug Bounty inFakt

§1 Przedmiot regulaminu

Niniejszy regulamin określa zasady programu Bug Bounty inFakt, w tym prawa i obowiązki jego uczestników oraz obowiązki i zakres odpowiedzialności organizatora programu.

§2 Słowniczek

Użyte w niniejszym dokumencie terminy oznaczają:

1. Organizator – Infakt Sp. z o. o. z siedzibą w Krakowie, z adresem ul. Szlak 49, Kraków 31-153, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa – Śródmieścia Wydział XI Gospodarczy Krajowego Rejestru Sądowego pod numerem 0000325203, posiadającą NIP 9452121681, tj. podmiot udostępniający zasoby Serwisu oraz Aplikację;
2. Aplikacja – oferowana przez Organizatora aplikacja mobilna Infakt zarówno w wersji na platformę iOS/iPadOS jak i Android;
3. Nagroda - nagroda pieniężna wypłacana Uczestnikowi Programu na zasadach opisanych w Regulaminie;
4. Podatności - podatności, luki czy błędy w zakresie bezpieczeństwa szeroko rozumianych produktów IT;
5. Program - program Bug Bounty inFakt, którego zasady opisuje Regulamin;
6. Regulamin – niniejszy dokument wraz z załącznikami stanowiącymi jego integralną część;
7. Uczestnik – osoba fizyczna biorąca udział w Programie;
8. Witryny - zarządzane przez Organizatora witryny w domenach *.infakt.pl oraz infaktpliki.pl z wyłączeniem:
    - www.infakt.pl,
    - infakt.pl,
    - pomoc.infakt.pl,
    - *.pomoc.infakt.pl,
    - dev.infakt.pl,
    - *.dev.infakt.pl.

§3 Uczestnicy Programu

1. W Programie może wziąć udział Uczestnik, który:
    a. posiada pełną zdolność do czynności prawnych i status polskiego rezydenta podatkowego;
    b. nie jest pracownikiem ani współpracownikiem Organizatora oraz podmiotu realizującego szeroko rozumiane audyty bezpieczeństwa w przedsiębiorstwie Organizatora, ani członkiem rodziny w/w osób do drugiego stopnia pokrewieństwa włącznie;
    c. Uczestnik zobowiązany jest zapewnić sobie we własnym zakresie wszelkie narzędzia i środki, w tym środki techniczne niezbędne do udziału w Programie i przyjmuje do wiadomości, że udział w Programie odbywa się wyłącznie na jego koszt i ryzyko.
2. Przed wzięciem udziału w Programie Uczestnik powinien zapoznać się z Regulaminem, którego treść dostępna jest pod adresem https://www.infakt.pl/bugbounty/regulamin-bugbounty.pdf i może zostać w każdym momencie zapisana na nośniku bądź wydrukowana.

§4 Cel i warunki Programu

1. Celem Programu jest promowanie oferowanych przez Organizatora produktów i rozwiązań IT jako zapewniających bezpieczne przetwarzanie gromadzonych w nich danych oraz samego Organizatora jako podmiotu dbającego o bezpieczeństwo oferowanych przez niego produktów poprzez wyeliminowanie Podatności. Dodatkowym celem Programu jest poprawienie bezpieczeństwa wszystkich użytkowników korzystających z produktów oferowanych przez Organizatora.
2. Program stanowi przyrzeczenie publiczne w rozumieniu przepisów art. 919 – 921 Kodeksu cywilnego.
3. Programem objęte są wyłącznie Witryny i Aplikacje.
4. Programem nie są objęte:
    a. błędy u zewnętrznych partnerów Organizatora czy w aplikacjach podmiotów trzecich, które np. wykorzystują interfejs programistyczny API Organizatora;
    b. błędy w bibliotekach oraz programach, które nie były tworzone przez Organizatora;
    c. podatności wynikające z wykorzystywanego przez użytkownika oprogramowania, np. przestarzałe wersje oprogramowania przeglądarek czy systemów operacyjnych; wykorzystywania dodatków do przeglądarek czy też mających swe źródło w ataku na urządzenie, z którego korzysta użytkownik (m.in. atak Self-XSS);
    d. ataki Cross-Site Request Forgery (CSRF),
    e. podatności z listy OWASP o kategorii LOW;
    f. ataki typu Content Spoofing,
    g. niepoprawna konfiguracja rekordów DNS dla poczty (SPF, DKIM, DMARC);
    h. błędna lub niepoprawna konfiguracja nagłówków;
    i. błędy związane z protokołem DNS i pochodnymi (np. wpisy typu CAA, TXT...), zapytaniami do bazy WHOIS (np. nadmierna publikacja informacji);
    j. wszelkie kwestie związane z infrastrukturą, którą nie zarządza Organizator;
    k. kwestie związane z certyfikatami bezpieczeństwa (np. SSL/TLS, GPG, PGP…);
    l. błędy w nieaktualnych wersjach aplikacji mobilnych, jak i wersjach dostępnych w ramach publicznych oraz niejawnych testów;
    m. publicznie dostępne informacje wynikające z założeń działania aplikacji,
    n. elementy Aplikacji wczytywane w sposób jawny lub niejawny z podstron w domenach (subdomenach) wyłączonych w udziału w programie,
    o. zgłoszenia o otwartych portach sieciowych usług umożliwiających zarządzanie infrastrukturą (SSH, SFTP itp.), gdy dana usługa wymaga dalszej autoryzacji lub fakt jej publicznego udostępnienia nie wpływa bezpośrednio na bezpieczeństwo,
    p. zgłoszenia dotyczące wymagań w zakresie złożoności i siły haseł (np. brak mechanizmu w danym formularzu albo możliwość pominięcia mechanizmu)
    q. nadmiarowe informacje przekazywane w nagłówkach protokołu HTTP (np. o wersjach serwera www) oraz innych protokołów sieciowych (np. DNS),
    r. enumeracja kont i innych zasobów,
    s. e-mail flooding/bombing,
    t. brak zabezpieczenia przez mechanizmy typu captcha lub rate-limiting mało wrażliwych elementów systemu,
    u. CSV/XML injection i ataki z użyciem innych typów plików,
    v. odkrycie zasobów z informacjami niewrażliwymi, które nie są linkowane z innych stron serwisu,
    w. brak implementacji flag HttpOnly/Secure dla plików cookies,
    x. zasoby o kodach odpowiedzi innych niż http/200,
    y. możliwość wgrania do aplikacji lub pobrania z aplikacji zainfekowanego pliku.
5. Uczestnik przyjmuje do wiadomości, że poniższe działania nie są akceptowalne jako sposób na realizację celów Programu i jako takie mogą spotkać się z adekwatną reakcją prawną Organizatora:

a. uzyskanie dostępu do zasobów poprzez dostęp za pomocą danych autoryzacyjnych, które zostały opublikowane przez użytkownika lub jemu wykradzione;
b. ataki typu DDoS/DoS na infrastrukturę;
c. ataki typu brute-force (siłowe, słownikowe…) skutkujące odkryciem danych dostępowych,
d. obejście limitów bezpieczeństwa aplikacji, systemów bezpieczeństwa infrastruktury itp.;
e. ataki socjotechniczne (np. polegające na podszyciu się pod inną osobę) lub wywołane z naruszeniem prawa (np. szantaż);
f. fizyczne ataki na serwerownię, biura inFakt, jak i pracowników czy współpracowników;
g. działania oparte o ramki (np. iframe) oraz proxy ruchu;
h. podszywanie się pod Organizatora, np. poprzez modyfikację nagłówków wiadomości e-mail;
i. testy obciążeniowe aplikacji.

§5 Procedura zgłaszania Podatności

1. W celu zgłoszenia Podatności w ramach Programu należy skorzystać z formularza dostępnego pod adresem https://www.infakt.pl/bugbounty lub wysłać email na adres bugbounty@infakt.pl.
2. Formularz umożliwia podanie informacji opisujących zgłaszaną kwestię i im więcej informacji zostanie w nim podane, tym większa pewność, że Organizator należycie przeanalizuje i oceni tak zgłoszoną kwestię. Na powyższe informacje składać się mogą w szczególności:
    a. informacja na temat miejsca wystąpienia tj. adres strony, miejsce w aplikacji web lub mobilnej itp.;
    b. krótki opis Podatności, wraz ze stosownym zrzutem ekranu;
    c. rodzaj Podatności;
    d. sposób postępowania w celu odtworzenia zgłaszanej Podatności przez Organizatora;
    e. dane kontaktowe osoby zgłaszającej.
3. Organizator umożliwia zgłoszenie Podatności w formie zaszyfrowanej publicznym kluczem GPG Organizatora dostępnym pod adresem https://www.infakt.pl/.well-known/bugbounty.asc.

§6 Nagrody

1. Organizator przyznaje Nagrody w walucie polskiej za zgłoszone w ramach Programu Podatności, których ostateczną wysokość określa Organizator, ale których minimalna wysokość wynosi:

LP	Rodzaj Podatności	Minimalna wysokość Nagrody
1	Krytyczna	3000 zł
2	Wysoka	1000 zł
3	Średnia	500 zł
4	Niska	100 zł

2. Nagrody wypłacane są na rachunek bankowy wskazany przez Uczestnika.
3. Do Nagrody zostanie dodana dodatkowa nagroda pieniężna stanowiąca równowartość zryczałtowanego podatku od Nagrody. Rzeczona dodatkowa nagroda pieniężna nie będzie wypłacona Uczestnikowi, lecz zostanie pobrana jako podatek zryczałtowany od wartości

przyznanej Nagrody, o którym mowa w ustawie z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (tekst jednolity: Dz. U. z 2000 r., Nr 14, poz. 176 z późn. zm) na co Uczestnik wyraża zgodę. Za pobranie i odprowadzenie należnego podatku odpowiedzialny jest wyłącznie Organizator.

4. W przypadku gdy więcej niż jeden Uczestnik zgłosi daną Podatność, o przyznaniu Nagrody decyduje data dokonania prawidłowego zgłoszenia takiej Podatności, odnotowana przez Organizatora.
5. Warunkami wydania Nagrody są:
    a. wstrzymanie się z opublikowaniem informacji o zgłoszonej Podatności do czasu wyrażenia na to specjalnej zgody przez Organizatora;
    b. podanie Organizatorowi danych, które umożliwią wypłatę Nagrody.

§7 Obowiązki Uczestnika

1. Uczestnik zobowiązany jest do podania w ramach uczestnictwa w Programie prawdziwych danych osobowych i kontaktowych. Uczestnik ponosi wszelką odpowiedzialność z tytułu naruszenia wyżej określonego obowiązku.
2. Uczestnik przyjmuje do wiadomości, że wykorzystywanie odkrytej Podatności w sposób sprzeczny z celem Programu spotka się z adekwatną, prawną reakcją Organizatora i/bądź osób, których prawa zostały zagrożone bądź naruszone takim działaniem Uczestnika. W szczególności dotyczy to wykorzystywania odkrytej Podatności w celu nieuprawnionego uzyskania informacji stanowiącej tajemnicę przedsiębiorstwa.

§8 Postępowanie reklamacyjne

1. Wszelkie ewentualne reklamacje Uczestnik winien zgłaszać na piśmie na adres wskazany w oznaczeniu Organizatora, bądź za pośrednictwem poczty elektronicznej na adres bugbounty@infakt.pl, pod rygorem ich nieuwzględnienia.
2. Zgłoszenie reklamacyjne winno zawierać szczegółowy opis zdarzenia uzasadniającego zgłoszenie reklamacji, imię i nazwisko oraz adres e-mail Uczestnika.
3. Organizator rozpatrzy zgłoszenie reklamacyjne w terminie 14 dni od dnia otrzymania zgłoszenia, chyba że koniecznym będzie dla rozpatrzenia reklamacji dostarczenie Organizatorowi dodatkowych informacji. W takim przypadku termin 14 dni liczony jest od daty dostarczenia takich informacji.
4. Odpowiedź na reklamację wysyłana jest wyłącznie na adres email podany w zgłoszeniu reklamacyjnym.

§9 Prawa własności intelektualnej

Organizator zastrzega, iż w myśl art. 921 Kodeksu cywilnego na mocy Programu nabywa pełnię majątkowych praw autorskich do utworów składających się na zgłoszenie Podatności pod warunkiem wydania Nagrody. Tym samym w momencie wydania Nagrody Organizator nabędzie prawo do nieograniczonego czasowo i terytorialnie korzystania i rozporządzania w/w utworami wraz z prawem pobierania pożytków z nich, na wszystkich znanych polach eksploatacji, w szczególności co obejmuje:

1. rozpowszechnienie w/w utworów, co obejmuje publiczne wykonanie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do niej dostęp w miejscu i w czasie przez siebie wybranym, przy użyciu wszelkich dostępnych technik, w szczególności z wykorzystywaniem w sieci Internet i w innych sieci komputerowych;
2. utrwalanie i zwielokrotnianie w/w utworów, co obejmuje w szczególności strony internetowe, materiały i wydawnictwa promocyjne, profile w portalach społecznościowych;

3. wprowadzanie w/w utworów do obrotu przy użyciu wszelkich dostępnych nośników, użyczania, najmu lub dzierżawy, wprowadzenie do pamięci komputera i serwerów sieci komputerowych w/w utworów bądź ich części;
4. przeniesienie wyłącznego prawa zezwalania na wykonywanie zależnego prawa autorskiego do w/w utworów w szczególności uprawnienie do wprowadzania do w/w utworów zmian niezbędnych do ich wykorzystania, w tym do łączenia ich z innymi utworami oraz innych modyfikacji i opracowania utworu zależnego;
5. tworzenie i rozpowszechnianie utworów zależnych, w tym dalszych utworów opartych na w/w utworów lub ich poszczególnych elementach, w tym opracowanie odmiennych wersji językowych, graficznych, kolorystycznych, formatów wizualnych lub przestrzennych utworów i korzystanie z tak powstałych utworów zależnych w zakresie i na wszystkich polach eksploatacji określonych powyżej.

§10 Dane osobowe

1. Poprzez udział w Programie Uczestnik wyraża zgodę na przetwarzanie przez Organizatora danych osobowych podanych w ramach uczestnictwa w Programie. Tak powierzone dane przetwarzane będą w toku czynności koniecznych do prawidłowego przeprowadzenia Programu - tj. w celu oceny zasadności zgłoszenia Podatności, wydania Nagrody wraz z realizacją przez Organizatora stosownych obowiązków podatkowych czy archiwizacji związanej z Programem korespondencji. Dane te przetwarzane będą do momentu utraty ich przydatności dla Organizatora.
2. Administratorem danych osobowych Uczestnika jest Organizator.
3. Podanie danych osobowych przez Uczestnika ma charakter dobrowolny, lecz jest niezbędne do wydania ewentualnej Nagrody.
4. Organizator zastrzega sobie prawo do przekazania powierzonych danych osobowych podmiotom z nim współpracującym oraz - w przypadkach określonych powszechnie obowiązującymi przepisami prawa - organom i instytucjom państwowym w zakresie niezbędnym do przeprowadzenia Programu, a w szczególności zaś do przyznania ewentualnej Nagrody Uczestnikowi i zrealizowania przez Organizatora stosownych obowiązków podatkowych.
5. W zakresie nieuregulowanym w Regulaminie zastosowanie w zakresie przetwarzania danych osobowych Uczestnika ma polityka prywatności dostępna pod adresem www.infakt.pl/polityka-prywatnosci.

§11 Postanowienia końcowe

1. Regulamin jest wyłącznym dokumentem określającym zasady Programu, a wszelkie informacje o Konkursie zawarte w jakichkolwiek materiałach promocyjnych i reklamowych mają jedynie charakter pomocniczy.
2. Ewentualna odpowiedzialność Organizatora wobec Uczestnika w żadnym przypadku nie przekracza wartości nagrody przekazanej danemu Uczestnikowi. Ograniczenie odpowiedzialności, o którym mowa w zdaniu poprzednim nie dotyczy sytuacji, w której takie ograniczenie odpowiedzialności pozostaje w sprzeczności z obowiązującym prawem, a w szczególności nie dotyczy szkód wyrządzonych przez Organizatora czynem niedozwolonym lub w sposób zawiniony.
3. Organizator zastrzega sobie prawo zmiany Regulaminu i zmiany te obowiązują z chwilą udostępnienia Regulaminu w nowym brzmieniu.
4. Program trwa od dnia 6.11.2019 r. do odwołania przez Organizatora.
5. Regulamin w niniejszym brzmieniu wchodzi w życie z dniem 11.09.2020 r.