Key-Systems Anti-Missbrauchs-Richtlinie

I) Alle Dienstleistungen der Key-Systems GmbH ("Dienstanbieter" oder "Wir") werden auf der Grundlage dieser Richtlinie erbracht. Diese Richtlinie gilt gemäß den Bestimmungen des Registrierungsvertrags und / oder der Servicevereinbarungen zwischen dem Dienstanbieter und seinen Kunden. Diese Richtlinie gilt in ihrer aktuellen Form ab ihrer ersten Veröffentlichung auf der Website des Dienstanbieters und kann vom Dienstanbieter von Zeit zu Zeit durch Setzung einer angemessenen Frist auf seiner Website oder in seinen Newslettern aktualisiert oder geändert werden. Diese Richtlinie wurde erstellt, um den Meldeprozess zu unterstützen und Kunden über die verbotene Nutzung unserer Dienste zu informieren.

Diese Richtlinie gilt für alle vom Dienstanbieter bereitgestellten Dienste, einschließlich Registrierungs- und Verwaltungsdienste für Domainnamen, DNS-Dienste, Hostingdienste, E-Mail-Dienste, Zertifikatdienste, Routingdienste und andere Dienste („die Dienste“ oder „ein Dienst“).

Der Dienstanbieter erkennt die Rechte seiner Kunden an und wird im Allgemeinen keine Einschränkungen in Bezug auf die Nutzung der Dienste auferlegen. Der Kunde ist verpflichtet, die veröffentlichten Richtlinien einzuhalten, die sich auf seinen jeweiligen Service beziehen.
Der Dienstanbieter setzt alle angemessenen Mittel ein, um sicherzustellen, dass der Kunde die veröffentlichten Richtlinien der zuständigen Aufsichtsbehörden wie die von ICANN veröffentlichten Richtlinien einhält. Kunden müssen auch unseren Nutzungsbedingungen zustimmen, wenn sie einen Dienst beantragen.Der Dienstanbieter verpflichtet sich, zur Aufrechterhaltung einer sicheren Online-Umgebung beizutragen und das Potenzial für erhebliche Schäden für Internetnutzer zu begrenzen. Eine Schlüsselkomponente dieser Verpflichtung besteht darin, alle begründeten Berichte über böswillige, illegale oder betrügerische Nutzung ihrer Dienste zu untersuchen und angemessen darauf zu reagieren.
Missbrauch im Rahmen dieser Richtlinie ist definiert als eine Handlung, die Dritten tatsächlichen und erheblichen Schaden zufügt oder wahrscheinlich zufügt, eine wesentliche Eigenschaft für einen solchen Schaden darstellt oder illegal, rechtswidrig oder anderweitig gegen diese Richtlinie verstößt.

Alle Kunden des Dienstanbieters und seiner Wiederverkäufer erklären sich damit einverstanden, die Bestimmungen dieser Richtlinie einzuhalten, indem sie den Bestimmungen und Bedingungen des Dienstanbieters zustimmen, zu denen diese Richtlinie ein wesentlicher Bestandteil ist. Kunden, die die Dienste zur Bereitstellung von Diensten für Dritte nutzen, müssen diese Parteien an die Bestimmungen dieser Richtlinie binden.

Mit dieser Richtlinie soll sichergestellt werden, dass Dritte verstehen, was Missbrauch ist, und Informationen darüber bereitgestellt werden, wie solche Berichte an den Dienstanbieter übermittelt werden sollen.

Die Dienste dürfen nicht im Widerspruch zu geltenden Gesetzen oder Vorschriften, guten Sitten oder dieser Richtlinie verwendet werden. Die Richtlinie soll es dem Dienstanbieter ermöglichen, im Falle einer missbräuchlichen oder anderweitig verbotenen Nutzung Nachforschungen anzustellen und rasch Maßnahmen zu ergreifen und Kunden davon abzuhalten, die Dienste illegal oder betrügerisch zu nutzen. Der Dienstanbieter kann diese Richtlinie gegenüber seinen Kunden durchsetzen, indem er den Kundenzugriff auf den Dienst deaktiviert oder den Dienst nach Bedarf unterbricht, um diese Richtlinie durchzusetzen.

Der Dienstanbieter behält sich ausdrücklich das Recht vor, Dienste zu verweigern, abzubrechen, auszusetzen, zu deaktivieren, zu sperren oder zu übertragen, wenn er dies nach eigenem Ermessen für erforderlich hält und nach eigenem Ermessen (a) zum Schutz der Integrität und Sicherheit des Internets und/oder der DNS, (b) zum Schutz vor Bedrohungen der Cyber-Sicherheit, (c) zur Einhaltung aller anwendbarer Gesetze, Regierungsrichtlinien oder –anforderungen, Anfragen der Strafverfolgung; (d) für den Fall, dass ein Service unter Verstoß dieser Richtlinien oder anderer geltender Richtlinien der Regulierungsbehörden benutzt wird und (e) in Übereinstimmung mit einem Streitbeilegungsverfahren oder zur Vermeidung einer zivil- oder strafrechtlichen Haftung des Dienstleisters und seiner verbundenen Unternehmen, Tochterunternehmen, leitenden Angestellten, Direktoren und Mitarbeitern des Lizenzgebers. Zu diesen Maßnahmen kann gehören, dass der Kunde die Entfernung des betroffenen Inhaltes oder die Deaktivierung der gehosteten Ressource oder die teilweise oder vollständige Aussetzung oder Beendigung des betroffenen Dienstes vornehmen muss und ohne vorherige Ankündigung zu handeln, wenn dies zur Schadensvermeidung erforderlich ist.

Der Dienstanbieter kann Verstöße gegen die Anti-Missbrauchs-Richtlinien mit allen Mitteln feststellen, einschließlich, ohne Einschränkung, einer privaten Beschwerde, einer öffentlichen Warnung, der Einschaltung von Regierungs- oder Vollzugsbehörden, der Benachrichtigung Dritter und der fortlaufenden Überwachung durch den Dienstanbieter oder seine Partner. Nach eigenem Ermessen kann der Dienstanbieter oder sein Beauftragter über ein automatisiertes System oder anderweitig jede Website einsehen, die unter einem Domainnamen bereitgestellt wird, um Verstöße gegen dieser Policy Richtlinien zu identifizieren.

Der Dienstleister setzt alle gültigen gerichtlichen Anordnungen oder Aufforderungen zur Beschlagnahme um, die von Gerichten und Schiedsgerichten, Tribunalen oder Strafverfolgungsbehörden der jeweils zuständigen Gerichtsbarkeiten ausgestellt werden und am Sitz des Dienstleisters vollstreckbar sind.

II) Im Folgenden finden Sie eine zusammenfassende Definition dessen, was Missbrauch und verbotene Verwendung bedeutet. Diese Liste erhebt keinen Anspruch auf Vollständigkeit und kann jederzeit durch Veröffentlichung einer neuen Version dieser Richtlinie geändert werden.

A) DNS Missbrauch:

DNS Missbrauch ist die Verwendung von Registrierungs- und Verwaltungsdiensten für Domainnamen, die sich aus fünf schädlicher Aktivitäten zusammensetzt, die sich mit dem Domainnamensystem überschneiden: Malware, Botnets, Phishing, Pharming und Spam (sofern diese als Übermittlungsmodus für andere Formen des DNS Missbrauchs dienen). Wenn Anhaltspunkte dafür vorliegen, dass unsere Dienste für DNS Missbrauch verwendet werden, werden wir die Aussetzung des Dienstes in Betracht ziehen, sofern uns ausreichende Nachweise vorliegen, zum Schutz der Integrität des Internets und – in Fällen, in denen die Ressource des Kunden betroffen war – dem Kunden helfen, ihn vor möglichen Haftungsproblemen zu schützen.

a) Malware (einschließlich Spyware, Botware, Keylogger-Bots, Viren, Würmer und Trojaner) ist eine bösartiger Code oder eine Software, die ohne Zustimmung des Benutzers auf einem Gerät installiert wird den Betrieb des Geräts stört, vertrauliche Informationen sammelt und/oder Zugriff auf private Computersysteme erhält. Malware umfasst Viren, Spyware, Ransomware und andere unerwünschte Software.

b) Botnets sind Sammlungen von mit dem Internet verbundenen Computern, die mit Malware infiziert und denen befohlen wurden, Aktivitäten unter der Kontrolle eines Remote-Administrators auszuführen, um verschiedene Arten von Schaden zu verursachen – von nicht sanktioniertem Spam bis hin zu hohem Transaktionsverkehr auf validen Computerdiensten wir DNS oder Webservices. Dieses Verbot bezieht sich auch auf den Betrieb von Botnet-Befehls- und Steuerfunktionen (eine geringere Anzahl von Computern, die nachfolgende Befehle ausgeben und/oder an das Botnet verteilen.

c) DdoS Angriff bezieht sich auf die Verwendung des Dienstes bei der Initiierung oder absichtlichen Teilnahme an Denial-of-Service Attacken (DOS oder DdoS Attacken, Mail-Bombardierung etc).

d) Phishing liegt vor, wenn ein Angreifer ein Opfer dazu verleitet, vertrauliche persönliche, Unternehmens- oder Finanzinformationen (zB Kontonummern, Anmelde-Ids, Kennwörter) preiszugeben, indem er betrügerische oder ähnliche Emails sendet oder den Endnutzer auf gefälschte Nachahmungs-Webseiten lockt.

e) Pharming ist die Umleitung von unwissenden Benutzern zu betrügerischen Webseiten oder Diensten, typischerweise durch DNS-Hijacking oder Vergiftung oder durch die Nutzung von Weiterleitungen.

DNS-Hijacking tritt auf, wenn Angreifer Malware verwenden, um Opfer auf die Webseite des Angreifers umzuleiten, anstatt auf die ursprünglich angefragte. Eine DNS-Vergiftung führt dazu, das ein DNS-Server (oder Resolver) mit einer falschen IP Adresse mit einem bösartigem Code antworten. Dies schließt auch nicht autorisierte Fast-Flux Techniken mit ein.

f) Spam ist die Verwendung der Infrastruktur oder der Dienste des Dienstanbieters zum Senden unerwünschter massenhaft per Email oder auf andere Weise versendeter Nachrichten, insbesondere wenn der Empfänger keine Erlaubnis zum Versand der Nachricht erteilt hat und die Nachricht als Teil einer größeren Menge von Nachrichten mit im wesentlichen identischem

Inhalt gesendet wurde. Dies gilt auch für Instant- oder Mobile Messaging-Spam sowie für das Spammen von Webseiten und Online-Foren. Spam wird nur dann als DNS-Missbrauch behandelt, wenn er als Übermittlungsmechanismus für die anderen vier Formen des DNS-Missbrauchs verwendet wird.

g) Unter Fast Flux Hosting versteht man den Schutz von Phishing-, Pharming-, Botnet- und Malware-Websites und Netzwerken vor der Entdeckung und die Umgehung der Methoden, die zur Abwehr solcher Praktiken eingesetzt werden, wobei die mit betrügerischen Websites verbundenen IP-Adressen schnell geändert werden, so dass der tatsächliche Standort der Websites schwer zu finden ist.

B) Content Abuse

Der Missbrauch von Inhalten umfasst die Nutzung unserer Webhosting-Dienste zur Förderung folgender Aktivitäten:

a) Verstöße gegen geistiges Eigentum, Marken, Urheberrecht und Patente einschließlich Piraterie: Geistiges Eigentum (IP) ist ein Begriff, der sich auf eine Reihe unterschiedlicher Arten geistiger Schöpfungen bezieht, für die eine Reihe von ausschließlichen Rechten in den entsprechenden Rechtsgebieten anerkannt sind. Nach dem Gesetz über geistiges Eigentum erhalten Eigentümer bestimmte ausschließliche Rechte an einer Vielzahl von immateriellen Vermögenswerten wie Musik-, Literatur- und Kunstwerken; Entdeckungen und Erfindungen; Wörter, Phrasen, Symbole und Designs. Zu den gängigen Arten von Rechten an geistigem Eigentum gehören Urheberrechte, Marken, Patente, gewerbliche Schutzrechte und Geschäftsgeheimnisse in anerkannten Gerichtsbarkeiten. Jede Handlung, die zu Diebstahl, Missbrauch, falscher Darstellung oder einer anderen schädlichen Handlung gegenüber einer Person oder eines Unternehmens führt, wird als Verletzung geistigen Eigentums eingestuft.

b) Hassrede ist die Verbreitung und/oder Veröffentlichung von hasserfüllten, diffamierenden, extremistischen oder abfälligen Inhalten, die auf rassischen, ethnischen oder politischen Gründen beruhen und dazu bestimmt oder allgemein in der Lage sind, einer Person oder Organisation Verletzungen oder Schäden jeglicher Art zu verursachen oder anzuregen, egal ob es allgemeine oder spezifische Anreize zur Gewalt enthält oder nicht.

c) Eine Verletzung der Persönlichkeitsrechte ist die Veröffentlichung von Inhalten, die die Persönlichkeitsrechte Dritter ohne rechtliche Rechtfertigung verletzen, z.B. durch die Veröffentlichung ihrer persönlichen Daten ohne Zustimmung oder Rechtsgrundlage.

d) Inhalte zu Kindesmissbrauch und Kinderpornographie beziehen sich auf die Verbreitung von Filmen und/oder Bildern, Filmen und in einigen Fällen auch Schriften, die sexuell eindeutige Aktivitäten darstellen, an denen Minderjährige entweder beteiligt sind oder die Minderjährige darstellen, die an einer Aktivität sexueller Natur beteiligt sind oder die Minderjährige auf andere Weise schädigen können.

Wenn wir Berichte erhalten, dass unsere Dienste im Zusammenhang mit Inhalten verwendet werden, die Material über Kindesmissbrauch enthalten, ist es uns gesetzlich nicht gestattet, diese Behauptungen selbst zu überprüfen. Wir empfehlen, dass Sie sich an Ihre örtliche

Strafverfolgungsbehörde wenden, um solche Auffälligkeiten zu melden. Wir arbeiten mit Organisationen wie INHOPE (https://www.inhope.org/EN#hotlineReferral) zusammen, um derartige Inhalte zu identifizieren. Wir werden jeden Domainnamen sofort sperren, sobald wir von einem verifizierten Strafverfolgungsanbieter oder einer anerkannten Partnerorganisation eine schriftliche Bestätigung erhalten haben, dass der Domainname verwendet wird, um auf Server zu verweisen, die Material über Kindesmissbrauch enthalten.

e) Beitrag zum Verkauf oder Vertrieb von verschreibungspflichtigen Medikamenten oder kontrollierten Substanzen ohne gültige Verschreibungs- und/oder Vertriebslizenz, sowie zum Verkauf und Vertrieb nicht lizenzierter oder nicht zugelassener Medikamente.

f) Menschenhandel ist die Handlung oder die Praxis der illegalen Beförderung von Menschen von einem Land bzw. Gebiet in ein anderes, in der Regel zum Zwecke der Zwangsarbeit oder sexuellen Ausbeutung. Dazu gehört auch Sklaverei in jeglicher Form und Gestalt.

g) DNS-Missbrauch wie oben definiert.

Wir sind uns bewusst, dass einige dieser Verwendungen Raum für Interpretationen lassen, oder mit anderen rechtlichen Vorschriften in Konflikt stehen können. Aus diesem Grund können wir nur dann angemessene Maßnahmen ergreifen, wenn die unterstützenden Beweise zwingend und eindeutig sind. Wir können auch gegen bestimmte Formen von inhaltlichem Missbrauch vorgehen, auch wenn wir nicht der Hosting-Service-Provider sind.

C) Sonstige illegale oder verbotene Nutzung

Die Nutzung unserer Dienstleistungen ist weiterhin verboten bei missbräuchlichem, böswilligem oder illegalem Verhalten bei der Verwendung eines Domain-Namens, wie z.B:

a) wenn sie gegen örtliche, staatliche, nationale oder internationale Gesetze oder Vorschriften verstößt, die auf uns oder den Dienst anwendbar sind. Ein Gesetz oder eine Verordnung ist anwendbar, wenn es die Gerichtsbarkeit von Unternehmen, den Kunden oder eine andere Gerichtsbarkeit, auf die der Kunde mit seiner Nutzung des Dienstes abzielt, benennt.

b) wenn sie für die Förderung, die Beteiligung an oder die Unterstützung von illegalen Aktivitäten jeglicher Art sowie für die Förderung von Geschäftsmöglichkeiten oder Investitionen verwendet werden, die nach geltendem Recht nicht zulässig sind.

c) wenn sie zur Begehung betrügerischer Handlungen genutzt werden und um sich mit einer falschen Identität auszustatten.

d) wenn jede andere Werbung oder jedes Angebot zum Verkauf von rechtswidrigen Waren oder Dienstleistungen abzielt, die gegen nationale oder internationale Gesetze bzw. Vorschriften verstoßen.

e) wenn sie gegen nationale oder internationale Sanktionen verstößt, denen das Unternehmen, seine verbundenen Unternehmen und/oder seine Lieferanten unterworfen sind.

f) wenn sie zum Hacken verwendet werden. Unter Hacking versteht man die Nutzung des Dienstes für Aktivitäten, die darauf abzielen, sich illegalen Zugang zu anderen Computern oder Netzwerken zu verschaffen, sowie jede Aktivität zur Vorbereitung auf ein solches illegales

Eindringen in ein System. Dies schließt nicht Aktivitäten ein, die darauf abzielen, sich legalen Zugang zu verschaffen oder die Sicherheit der dritten Partei mit deren Zustimmung zu testen.

g) wenn sie in einem Gerichtsbeschluss oder auf Ersuchen einer Behörde der zuständigen Gerichtsbarkeit als illegal oder anderweitig ungesetzlich bezeichnet wird.

D) eingeschränkte Nutzung

Die folgenden Bereiche stellen nicht notwendigerweise einen Missbrauch dar, können aber als solcher behandelt werden, sofern sie nicht bestimmten Anforderungen entsprechen:

a) Die Verbreitung von erotischen, pornografischen oder anderweitig anstössiger sexueller Inhalte, ist nur unter Einhaltung der geltenden gesetzlichen Bestimmungen erlaubt. So ist beispielsweise die Nutzung eines Dienstes zur Veröffentlichung oder Verbreitung solcher Inhalte ohne ausreichende Altersverifikationstechniken (wodurch es Minderjährigen ermöglicht wird, solche Inhalte ohne entsprechende erschwerende Hindernisse zu sehen) sowie die Nutzung unter Verletzung der Anforderungen und Richtlinien der Behörden oder der entsprechenden Registrierungsbehörden, streng verboten.

b) Chat- oder Messaging-Dienste auf unseren Hosting-Diensten sind nur zulässig, wenn der Kunde zuvor eine ausdrückliche schriftliche Genehmigung vom Dienstanbieter einholt.

c) Nutzung der Hosting-Dienste Download- oder Streaming-Server, Online-Dateiablage, P2P-Tracker, P2P-Client oder P2P-Host oder anderweitige Nutzung der Hosting-Dienste zur Teilnahme an File-Sharing-Aktivitäten.

d) Die Verwendung von Domainnamen muss den Richtlinien der entsprechenden Registerbetreiber und der Gerichtsbarkeit entsprechen.

e) Die Nutzung unserer Hosting- und Mail-Dienste zum Versenden jeglicher Form von Spam ist verboten. Es kann für uns unmöglich sein, in jedem Fall festzustellen, ob es sich bei einer Nachricht tatsächlich um Spam, einen Newsletter oder eine legale geschäftliche E-Mail handelt. Weitere Informationen finden Sie in unserer Anti-Spam-Richtlinie.

f) Nutzung unserer Dienste zur Förderung von Aktivitäten, die gegen unsere Unternehmensrichtlinien und/oder Werte verstoßen.

E) Berichte von vertrauenswürdigen Anzeigern

Jegliche Missbrauchsberichte von Unternehmen, die wir nach unserem alleinigen Urteil aufgrund ihrer anerkannten Fachkompetenz und ihres Rufs hinsichtlich der Genauigkeit der

Berichte als "vertrauenswürdige Anzeiger" betrachten, können zu sofortigen Maßnahmen führen, ohne vorherige Rücksprache mit dem Kunden oder Benachrichtigung des Kunden und ohne Untersuchung der Beschwerde.

Gleiches gilt für Berichte von Strafverfolgungsbehörden und anderen ordnungsgemäß autorisierten Vollzugsbehörden. Behörden, die Missbrauch melden, müssen bereit sein, die von ihnen zur Verfügung gestellten Referenzen zu überprüfen, und sollten über ordnungsgemäße rechtliche Kanäle kommunizieren.

III) So melden Sie uns den Missbrauch einer Domain:

Wir unterhalten eine spezielle öffentliche Kontaktmöglichkeit für Missbrauchsfälle unter:

https://www.rrpproxy.net/deutsch/Kontakt/Beschwerdeweg_und_Domain-Missbrauchsmeldeverfahren

Alle Berichte, die bei der Kontaktstelle für Domainmissbrauch eingehen, werden intern in einem Ticketsystem nachverfolgt, um die Rechenschaftspflicht und eine vereinfachte Bezugnahme zu gewährleisten. Dem Berichterstatter wird eine Nachverfolgungsnummer zur Verfügung gestellt. Jeder Bericht wird auf seine Glaubwürdigkeit überprüft und bewertet, um festzustellen, ob das gemeldete Problem einen Domainmissbrauch darstellt, und um die gegebenenfalls erforderlichen Maßnahmen zu bewerten.

Auch wenn eine bestimmte Maßnahme verlangt wird behalten wir uns das Recht vor, andere Maßnahmen zu ergreifen, da im Zweifel die jeweils mildeste, verhältnismäßige Vorgehensweise zur Anwendung kommt, die geeignet ist, das Problem zu lösen..

Bei der Meldung von Missbrauch sollte der Berichterstatter ausreichende Informationen und dokumentarische Beweise zu dem gemeldeten Problem bereitstellen, um eine ordnungsgemäße und angemessene Überprüfung des Berichts zu ermöglichen.

Der Bericht sollte zunächst den Domainnamen, den Link und / oder den spezifischen Dienst angeben, der vom Dienstanbieter angeboten wird, der den Bericht erstellt hat, und eine kurze Zusammenfassung des Problems enthalten, einschließlich, aber nicht beschränkt auf:

a. genaue URL (s), unter denen der Verstoß zu sehen ist

b. für Angelegenheiten, in denen URLs nicht verwendet werden können (d. h. Spam- und / oder Phishing-Vorwürfe), Kopien von Dateien, die als Teil des Verstoßes verwendet werden, und Beweise für ihre Herkunft (d. h. E-Mails einschließlich vollständiger Header-Daten).

c. Alle weiteren unterstützenden Beweise wie Screenshots und / oder Serverprotokolldateien. Auf Anfrage sollte der Berichterstatter zusätzliche unterstützende Informationen bereitstellen, damit wir das Problem untersuchen und bewerten können.

Wir sind bestrebt, auf jeden Bericht so schnell wie möglich zu antworten. Abhängig vom aktuellen Berichtsvolumen kann es unter Umständen einige Zeit dauern, bis Sie eine Antwort auf Ihre Nachricht erhalten. Bitte beachten Sie, dass wir möglicherweise Antworten auf mehrere Berichte eines Reporters bündeln. Bitte senden Sie keine nicht angeforderten Follow-ups oder Erinnerungen, um eine Verzögerung der Gesamtantwortzeiten für Tickets zu vermeiden.

Aus rechtlichen oder datenschutzrechtlichen Gründen können wir die aufgrund des Berichts ergriffenen Maßnahmen möglicherweise nicht angeben. Bei hohem Ticketvolumen oder mehreren Berichten zu demselben Problem können wir uns dafür entscheiden, nicht jedem Reporter individuelle Antworten zu geben. Die Nichtbeachtung dieser Berichtsrichtlinien kann dazu führen, dass Ihr Bericht nicht berücksichtigt wird.

Der missbräuchliche Gebrauch muss zum Zeitpunkt der Untersuchung der Angelegenheit aktiv und überprüfbar sein. Wenn wir den Verstoß nicht überprüfen / herunterladen / verwenden / darauf zugreifen können, können wir ihn nicht überprüfen. Wenn der Verstoß auf bestimmte Subnetze (z. B. geografische Region) oder Zugriffsmethoden (z. B. mobile Geräte) beschränkt ist oder nur von diesen aus zugänglich ist, müssen diese Informationen bereitgestellt werden, um sicherzustellen, dass wir solche Ansprüche überprüfen können.

Der Berichterstatter erklärt sich damit einverstanden, dass wir die Beschwerde dem Kunden oder zwischengeschalteten Dritten zur Überprüfung und weiteren Bearbeitung zur Verfügung stellen können. Wir werden dann mit den betroffenen Parteien zusammenarbeiten, um festgestellte Bedrohungen oder bestätigten Missbrauch schnell zu beseitigen. Falls der Berichterstatter Einwände gegen die Weiterleitung seiner Beschwerde erhebt, sollte dies im ersten Missbrauchsbericht klargestellt werden.

Bei mehreren Beschwerden über denselben Dienst, dieselbe Hosting-Ressource oder denselben Domain-Namen sollte der Berichterstatter diese Beschwerden in einem Bericht bündeln. Bitte senden Sie nicht mehrere Berichte oder Nachrichten bezüglich derselben Ressource.

Der Berichterstatter muss sich durch Angabe seines Namens, seiner Telefonnummer und seiner E-Mail-Adresse ausweisen. In einigen Fällen müssen wir den Bericht möglicherweise mit weiteren Fragen bearbeiten. Wir sind dazu befugt, anonyme Beschwerden und Beschwerden, einschließlich falscher oder irreführender Kontaktdaten, zu ignorieren oder zu schließen.

Der Berichterstatter muss einen höflichen Ton beibehalten. Wir können Berichte unbeachtet lassen, die gegen grundlegende Regeln der Etikette oder der höflichen Konversation verstoßen.