. RUHR Rapid Takedown Policy

Die vorliegenden Bedingungen, die gegenüber Registraren und Registranten von [.RUHR] Domains gelten, definieren klar und eindeutig, wie die Registry bei dem Bekanntwerden von Missbrauchsfällen vorgehen wird. Sie sind kein Ersatz für die Uniform Dispute Resolution Policy (UDRP) oder für die Uniform Rapid Suspension (URS) oder für sonstige Streitbeilegungsverfahren, in deren Rahmen Auseinandersetzungen zwischen Dritten gelöst werden sollen. Vielmehr richten sich dieses Bedingungen gegen Missbrauchsfälle, die eine Gefahr für die öffentliche Sicherheit und damit auch eine Gefahr gegenüber allen .RUHR Nutzern darstellen.

1. Missbrauchsfälle

a. Ein Missbrauchsfall im Sinne dieser Bedingungen wird wie folgt definiert:

- **Verletzung der geltenden Gesetze oder Vorschriften , insbesondere Verstöße gegen das deutschen Strafgesetzbuches (StGB) , gegen das deutsche Jugendschutzgesetz (JuSchG) und/oder gegen den deutschen Jugendmedienschutz-Staatsvertrag (JMStV),**
- **Die Nutzung einer Domain zur Verbreitung von Inhalten, die Teile der Bevölkerung und/oder bestimmte Volksgruppen sowie religiöse oder ethnische Gruppe diffamieren und/oder die Verbreitung von Inhalten, die gewaltverherrlichend sind sowie die Verbreitung von Inhalten, die gegen die Menschenwürde verstoßen sowie Inhalte, die die während der Herrschaft des Nationalsozialismus begangene Handlungen leugnet oder verharmlost,**
- **Die Verbreitung von kindesmissbräuchlichen Inhalten,**
- **Die Nutzung einer Domain für Versendung von Spammails, also die massenhafte und unerwünschte Kommunikation mit Dritten (per E-Mail, über Instant und Mobile Messaging, auf Webseiten und Foren),**
- **Die Nutzung einer Domain zur Durchführung von Distributed Denial of Service Attacken ("DDoS-Attacken“),**
- **Die Nutzung einer Domain zu Phishingaktivitäten, also zum betrügerischen „Abfischen“ von personenbezogenen Daten Dritter, wie Namen, Adressen, Bankdaten oder Benutzernamen und Passwörter,**
- **Die Nutzung einer Domain im Zusammenhang mit Pharming, also z.B. DNS-Hijacking und/oder DNS-Cache-Poisoning,**
- **Die Nutzung einer Domain für die vorsätzliche Verbreitung von schädlicher Software wie z.B. Spyware, Malware, Keyloggern, Bots, Viren und/oder Trojaner,**
- **Die Nutzung einer Domain zur Steuerung und Kontrolle eines sog. „Botnet“, also einem Netzwerk aus infizierten Rechnern oder „Zombies“,**
- **Die Nutzung einer Domain im Zusammenhang mit Handlungen, die dem illegalen Zugriff auf Rechner bzw. auf Netzwerke Dritter („Hacking“) dienen bzw. solche unerlaubten Zugriffe vorbereiten,**
- **Die Nutzung einer Domain im Zusammenhang mit Fast Flux Techniken, die der Verschleierung von IPs bzw der von Webserverstandorten dienen.**

b. Die in diesen Bedingungen genannten Missbrauchsfälle stellen keine abschließenden Regelungen dar, denen bezüglich sonstiger denkbarer Missbrauchsfälle eine Ausschlusswirkung zu kommen soll.

c. Verstöße gegen diese Bedingungen stellen gleichzeitig Verstöße gegen die .RUHR Acceptable Use Policy dar.

d. Die Registry ist dazu berechtigt, durch Auswertung von Blacklists, Malware- und Phishing-Feeds und/oder ähnlichen Quellen, eigenständig Missbrauchsfälle festzustellen und zu verfolgen.

2. Meldung von Missbrauchsfällen

a. Die Registry stellt unter www.dotruhr.de eine Webseite zur Verfügung, über die Dritte die Möglichkeit erhalten, Missbrauchsfälle, die unter .RUHR Domains mutmaßlich festgestellt worden sind, zu melden. Hierzu stellt die Registry ein Kontaktformular zur Verfügung. Weiterhin stellt die Registry eine telefonische Kontaktmöglichkeit während der gewöhnlichen Geschäftszeiten sowie einen E-Mail Kontakt bereit.

b. Dritte, die diese Kontaktmöglichkeiten nutzen, sind dazu verpflichtet, den der Missbrauchsmeldung zugrunde liegenden Sachverhalt möglichst vollständig darzustellen und zu belegen. Weiterhin sind dazu verpflichtet, der Registry mindestens eine Kontaktmöglichkeit (z.B. E-Mail Adresse und/oder Telefonnummer) zu nennen. Diese Daten wird die Registry ausschließlich zur Bearbeitung des gemeldeten Missbrauchfalls verwenden und in keinem Fall an Dritte übermitteln. Ausgenommen davon ist die Übermittlung an staatliche Stellen (z.B. Polizei und/oder Staatsanwaltschaften) für den Fall, dass die Registry wegen eines konkreten Missbrauchsfalls strafrechtliche Schritte einleitet.

c. Gemeldete Missbrauchsfälle werden umgehend mit einer einmaligen Fallnummer versehen, die dem Dritten vorzugsweise per E-Mail mitgeteilt werden wird. Die Registry ist dazu berechtigt, aber nicht verpflichtet, bei dem Dritten ggf. weitere Informationen anzufordern, die zur Aufklärung des Sachverhaltes notwendig sind.

3. Prüfung von Missbrauchsfällen / Bedrohungsstufen

a. Anhand der übermittelten Daten wird die Registry prüfen, ob ein Missbrauchsfall vorliegt, der die in diesen Bedingungen geregelten Konsequenzen zur Folge haben kann. Die Registry ist dazu berechtigt, den Sachverhalt anhand der übermittelten Daten zu prüfen und zu bewerten. Weiterhin ist die Registry dazu berechtigt, aber nicht verpflichtet, eigenständige Ermittlungen durchzuführen, um einen übermittelten Sachverhalt aufzuklären.

b. In Zweifelsfällen ist die Registry – unabhängig vom Threat-Level und unabhängig von der Person / der Behörde, welche den Missbrauch gemeldet hat – dazu berechtigt, den Missbrauchsfall von sachkundigen Dritten prüfen zu lassen.

c. Die an einem konkreten Missbrauchsfall beteiligten Dritten werden nach Möglichkeit von der Registry per E-Mail über den aktuellen Stand, über die Klassifizierung und über die ergriffene Maßnahme informiert.

d. Die Registry wird Missbrauchsfälle anhand von drei Bedrohungsstufen klassifizieren, nach denen sich die weiteren Maßnahmen sowie die Reaktionszeiten der Registry im konkreten Fall bestimmen:

- **Threat-Level 1:** Ein schwerwiegender Missbrauchsfall, der die öffentliche Sicherheit („Public Security) bereits konkreten Gefahren aussetzt; die Registry wird den Vorfall innerhalb von 48 Stunden nach Meldung lösen;

- **Threat-Level 2:** Ein ernstzunehmender Missbrauchsfall, der zwar die öffentliche Sicherheit noch nicht konkret gefährdet, es aber zu befürchten ist, dass eine solche Gefährdung unmittelbar bevorsteht; die Registry wird den Vorfall innerhalb von 72 Stunden nach Meldung lösen;
- **Threat-Level 3:** Ein Missbrauchsfall, den die Registry anhand der übermittelten Daten sowie auf Grundlage eigener Prüfungen nicht bestätigen konnte; die Registry wird den gemeldeten Missbrauchsfall einstellen.

e. Bei der Klassifizierung wird die Registry in erster Linie die Gefahren für die öffentliche Sicherheit berücksichtigen, die von einem konkreten Missbrauchsfall ausgehen (Ermessen der Registry). Weiterhin wird die Registry die Interessen des Registranten im konkreten Einzelfall in ihre Ermessensentscheidung miteinbeziehen, insofern dies möglich ist. Die Registry wird die wesentlichen Prüfungsschritte und Prüfungsergebnisse in elektronischer Form festhalten. Dies gilt auch für die von Registry nach Ziffer 6 getroffenen Maßnahmen.

f. Ein schwerwiegender Missbrauchsfall, bei dem die konkrete Gefahr für die öffentliche Sicherheit die Interessen des Registranten deutlich überlagert, liegt **immer,** aber nicht ausschließlich, vor, wenn die Registry von einer Ermittlungsbehörde (z.B. Polizei, Staatsanwaltschaft), von Gerichten oder Behörden über einen konkreten Sachverhalt informiert wird. Ein derartiger Vorfall wird von der Registry als **Threat-Level 1** klassifiziert. Ein schwerwiegender Missbrauchsfall liegt auch dann vor, wenn Dritte, die keine öffentliche Stelle sind, der Registry melden, dass unter .RUHR Domains

- anzügliche, anstößige, sexuell geprägte, obszöne oder diffamierende Inhalte vorgehalten werden, die geeignet sind, Rassismus, Fanatismus, Hass, körperliche Gewalt oder rechtswidrige Handlungen zu fördern bzw. zu unterstützen (jeweils explizit oder implizit);
- pornografische, gegen Jugendschutzgesetze, gegen das Strafrecht und/oder gegen sonstiges Recht verstoßende Inhalte, Dienste und/oder Produkte vorgehalten werden;
- Malware und/oder sonstige schädliche Software (Viren, Trojaner, Keylogger etc.) verbreitet wird;
- Pharming und/oder Phishing-Webseiten betrieben werden.

g. Sonstige nachvollziehbare Missbrauchsfälle, bei denen die konkrete Gefahr die Interessen des Registranten noch nicht deutlich überlagern, die der Registry gemeldet worden sind, werden als Threat-Level 2 klassifiziert. Bevor die Registry Maßnahmen durchführt, soll der betroffene Registrant zu dem vorgeworfenen Missbrauchsfall angehört werden.

h. Missbrauchsfälle, bei denen keine Gefahr für die öffentliche Sicherheit ersichtlich ist, die von der Registry nicht nachvollzogen werden können, werden als Threat-Level 3 klassifiziert. In diesen Fällen wird die Registry keine Maßnahmen gegen den betroffenen Registranten ergreifen. Der Registrant und der Dritte werden über die Entscheidung der Registry per E-Mail informiert.

i. Die Registry weist darauf hin, dass sie in jedem Fall bei Vorliegen eines Verdachts auf rechtswidrige bzw. strafbare Handlungen dazu berechtigt und ggf. auch verpflichtet ist, solche Vorfälle der Staatsanwaltschaft zur Kenntnis zu bringen.

4. Benachrichtigung des zuständigen Registrars

a. Hat die Registry gemäß Ziffer 3 einen Missbrauchsfalls festgestellt, so wird dieser an den jeweiligen Registrar der betroffenen .RUHR Domain übermittelt. Der Registrar verfügt ob seiner direkten Vertragsbeziehung zum Registranten regelmäßig über weitergehende Daten, die der schnellen Lösung des jeweiligen Missbrauchsfalls dienlich sein können.

b. Die Registry wird dem jeweiligen Registrar mitteilen, ob und innerhalb welcher Frist eine Benachrichtigung an den betroffenen Registranten zu erfolgen hat oder ob eine solche Benachrichtigung zu unterbleiben hat (vgl. Ziffer 4 e).

c. Registrare sind verpflichtet, den jeweiligen Missbrauchsfall innerhalb einer bestimmten Frist zu lösen, welche anhand des gemäß Ziffer 3 ermittelten Threat-Levels von der Registry bestimmt werden wird. Erfolgt innerhalb der Frist keine Rückmeldung des Registrars, so ist die Registry dazu berechtigt, Maßnahmen nach Ziffer 6 zu ergreifen.

d. Der jeweilige Registrar wird den betroffenen Registranten von dem gemeldeten Missbrauchsfall nach Möglichkeit per E-Mail und/oder telefonisch in Kenntnis setzen. Hierbei wird der Registrant Informationen zum konkreten Missbrauchsfall sowie Informationen zum Threat Level erhalten.

e. Die Registry weist darauf hin, dass es in bestimmten Fällen gesetzlich untersagt sein kann, den Registranten vorab über einen Missbrauchsfall zu informieren. In diesen Fällen wird der Registrant keine Information nach Ziffer 4 c erhalten. In diesen Fällen wird der Registrant im gesetzlich zulässigen Rahmen über die vom Registrar / von der Registry ergriffenen Maßnahmen informiert.

5. Äußerungsrecht des Registranten

a. Der betroffene Registrant ist ggf. dazu berechtigt, sich zu dem ihm vorgeworfenen Missbrauchsfall per E-Mail zu äußern. Dies gilt nicht, wenn ein Fall der Ziffer 4 e vorliegt. Die Frist zur Rückmeldung des Registranten beim jeweiligen Registrar bestimmt sich nach dem von der Registry angenommenen Threat-Level:

- beim Threat-Level 1 hat eine Rückmeldung spätestens 24 Stunden nach dem Versand der E-Mail an den Registranten zu erfolgen. Der Registrar kann eine kürzere Frist setzen, soweit der konkrete Fall dies erforderlich macht;
- beim Threat-Level 2 hat eine Rückmeldung spätestens 48 Stunden nach dem Versand der E-Mail an den Registranten zu erfolgen. Der Registrar kann eine kürzere Frist setzen, soweit der konkrete Fall dies erforderlich macht. Weiterhin ist der Registrar dazu berechtigt, den Registranten zur Durchführung bestimmter Maßnahmen (z.B. Entfernung von Inhalten, die unter einer .RUHR Domain vorgehalten werden) aufzufordern.

b. Nimmt der Registrant zu dem konkreten Missbrauchsfall keine Stellung oder erfolgt die Stellungnahme nicht fristgerecht oder wird die vom Registrar bzw. von der Registry geforderte Maßnahme nicht durchführt, ist der Registrar bzw. die Registry dazu berechtigt, die nach Ziffer 6 notwendigen Maßnahmen zu bestimmen und zu ergreifen.

c. Nimmt der Registrant zu dem konkreten Missbrauchsfall Stellung, so weist die Registry darauf hin, dass diese Äußerung an der nach Ziffer 3 vorgenommenen Klassifizierung nichts ändert. Die

Äußerung des Registranten wird die Registry im Rahmen der zu ergreifenden Maßnahmen nach Ziffer 6 berücksichtigen.

d. Nimmt der Registrant Stellung und führt die vom Registrar bzw. von der Registry geforderten Maßnahmen durch und/oder hilft dem festgestellten Missbrauch in sonstiger Art und Weise ab, so wird der Registrar bzw. die Registry dies im Rahmen der zu ergreifenden Maßnahmen nach Ziffer 6 berücksichtigen. Maßnahmen nach Ziffer 6 a scheiden in einem solchen Fall regelmäßig aus.

6. Maßnahmen des Registrars / der Registry / Eskalationsstufen

a. Der Registrar bzw. die Registry ist bezüglich der betroffenen .RUHR Domain dazu berechtigt, diejenigen Maßnahmen zu ergreifen, die dazu geeignet sind, einen konkreten Missbrauchsfall entsprechend der vorgenommenen Klassifizierung zuverlässig zu beseitigen. Sofern sich der Verstoß gegen die AUP nicht offensichtlich aus den vorliegenden Unterlagen oder dem unter der betroffenen .RUHR Domain vorgehaltenem Inhalt ergibt, wird die Registry durch einen fachlich qualifizierten Rechtsanwalt den betreffenden Fall prüfen lassen und dessen Empfehlungen umsetzen. Bei Eingaben seitens staatlicher Stellen ist die Prüfung auf die offensichtliche Rechtswidrigkeit der angeordneten Maßnahme beschränkt. Der Registrar bzw. die Registry ist z.B. dazu berechtigt,

- die Nameserver der betroffenen Domain zu deaktivieren; oder
- die betroffene .RUHR Domain zu löschen; oder
- die betroffene .RUHR Domain mit einem registry lock, hold, oder einem ähnlichen Status zu versehen.

Die Löschung einer Domain soll nur dann erfolgen, wenn sich die Rechtsverletzung ihre Ursache in der betreffenden Domain selbst findet. Ansonsten hat lediglich eine Deaktivierung für den Zeitraum zu erfolgen, bis der Missbrauch beseitigt ist oder eine von Dritten erfolgte Anordnung der Deaktivierung aufgehoben wurde. Jedenfalls wird die Registry rechtskräftige Entscheidungen eines deutschen Gerichts oder eines in Deutschland vollstreckbaren Titels umsetzen.

b. Weiterhin ist der Registrar bzw. die Registry bezüglich des betroffenen Registrierungsvertrages dazu berechtigt, vom Registranten wegen eines oder mehrere konkreter Missbrauchsfälle

- zu verlangen, dass Inhalte, die zur Missbrauchsmeldung geführt haben, zu beseitigen; oder
- ihn wegen der Verletzung seiner Pflichten aus dem Registrierungsvertrag abzumahnen; oder
- den Registrierungsvertrag aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist zu beenden; oder
- Strafantrag / Strafanzeige gegen ihn zu erstatten; oder
- die Reaktivierung einer .RUHR Domain von der Abgabe einer strafbewehrten Unterlassungs- und Verpflichtungserklärung abhängig zu machen, mit der sich der Registrant dazu verpflichtet, eine missbräuchliche Nutzung zukünftig zu unterlassen

c. Die Maßnahmen nach Ziffer 6 a und b bestimmt der Registrant bzw. die Registry nach pflichtgemäßem Ermessen sowie unter Berücksichtigung der Stellungnahme des Registranten nach Ziffer 5. Der Registrant bzw. die Registry wird bei ihrer Entscheidung insbesondere auch die bisherige Anzahl von gemeldeten Missbrauchsfällen bezüglich des betroffenen Registranten berücksichtigen.

7. Sonstiges

a. Weitergehende Schadensersatz- und/oder Freistellungsansprüche des Registrars bzw. der Registry bleiben unberührt.

b. Unbeschadet der vorstehenden Regelungen bleibt den Parteien die Nutzung sonstiger Streitschlichtungsverfahren bzw. die Beschreitung des ordentlichen Rechtsweges vorbehalten.