.GEA Acceptable Use and Anti-Abuse Policies

GEA Group Aktiengesellschaft ("registry operator") is committed to the stable and secure operation of .GEA. Abusive use of domain names creates security and stability issues for registries, registrars and registrants – as well as for Internet users. Therefore registry operator requires that registrants for .GEA domain names adhere to this Acceptable Use and Anti-Abuse Policy ("AUP").

Registry operator will address abusive behavior in .GEA consistent with this AUP. Registry operator provides an abuse point of contact through the e-mail address (abuse@nic.gea) posted on the registry operator website found at www.nic.gea.

Violations of the registry operator policies would be treated as abuse. .GEA domain names shall not be used to transmit, distribute, disseminate, publish or store any information that is in violation of any applicable law or regulation or is defamatory, abusive, obscene, indecent, or harassing, or that threatens or encourages injury to persons or property or infringement of the lawful rights of any party. Specifically, the following are deemed, without limitation, as violations:

1. **Spamming.** The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of web sites and Internet forums. Unsolicited emails advertising legitimate and illegitimate products, services, and/or charitable requests and requests for assistance are also considered as spam.
2. **Phishing (and various forms of identity theft).** Fraudulent web services and applications meant to represent and/or confuse or mislead Internet users into believing they represent services or products for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.
3. **Pharming and DNS Hijacking.** Redirection of DNS traffic from legitimate and intended destinations, by compromising the integrity of the relevant DNS systems. This leads unsuspecting Internet users to fraudulent web services and applications for nefarious purposes, such as illegally gaining login credentials to actual legitimate services.
4. **Distribution of Viruses or Malware.** Most typically the result of a security compromised web service where the perpetrator has installed a virus or software meant to infect computers attempting to use the web service in turn ("Malware"). Infected computers are then security compromised for various nefarious purposes such as gaining stored security credentials or personal identity information such as credit card data. Additionally compromised computers can sometimes be remotely controlled to inflict harm on other internet services.
5. **Child Pornography.** Child pornography refers to images or films (also known as child abuse images) and, in some cases, writings depicting sexually explicit activities involving a minor.
6. **Hacking.** Hacking constitutes illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of other individuals. Also includes any activity that might be used as a precursor to an attempted system penetration.
7. **Using fast flux techniques.** A methodology for hiding multiple source computers delivering malware, phishing or other harmful services behind a single domain hostname, by rapidly rotating associated IP addresses of the sources computers through related rapid DNS changes. This is typically done at DNS zones delegated below the level of a TLD DNS zone.
8. **Running botnet command and control operations.** A Botnet is a significant coordinated net of compromised (sometimes tens of thousands) computers running software services to enact various forms of harm – ranging from unsanctioned spam to placing undue transaction traffic on valid computer services such as DNS or web services. Command and control refers to a smaller number of computers that issue or distribute subsequent commands to the Botnet. Compromised botnet computers will periodically check in with a command and control computer that hides behind a list of date triggered, rotating domain registrations, which are pre-loaded in the compromised computer during its last check-in.
9. **Illegal Pharmaceutical Distribution.** Distribution and promotion of drugs, locally within a nation or overseas, without prescription and appropriate licenses as required in the country of distribution are termed illegal.
10. **Other Violations.** Other violations that will be expressly prohibited under the registry operator policies, include:
    - Maintaining inaccurate contact details on the WHOIS

- Network attacks
- Libelous or defamatory content adjudicated by a competent court of law
- Illegal Adult/Pornographic content
- Content that violates any privacy right
- Internet relay chat servers (“IRCs”) IRC bots
- Distribution of malicious tools promoting or facilitating hacking, unsolicited bulk emails or SMS, fake anti-malware products, phishing kits, unauthorized data banks violating individual privacy rights

Reservation of Rights

The registry operator expressly reserves the right to deny, cancel, suspend, lock or transfer any domain name registration that it deems necessary in its discretion: (i) to protect the integrity and stability of the registry operator; (ii) to comply with any applicable laws, government rules or requirements, requests of law enforcement; (iii) in the event a domain name is used in violation of these policies and any other policies regarding .GEA, (iv) domain name use is abusive or violates this AUP, or third parties rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark; and (v) in compliance with any dispute resolution process, or to avoid any liability, civil or criminal, on the part of registry operator and its affiliates, licensors subsidiaries, officers, directors and employees.