ABUSE PREVENTION AND MITIGATION POLICIES FOR THE TLDS .KOELN / .COLOGNE

A. Purpose of this document

dotKoeln GmbH works in close cooperation with the registry backend provider for .koeln and .cologne, RyCE GmbH to establish thorough and effective methods to prevent abuse of .koeln or .cologne domain names, .koeln/.cologne registrant data or the associated infrastructure, as well as to mitigate any impact from such abuse (should it occur despite the preventive measures). In order to achieve this, the dotKoeln GmbH and RyCE GmbH deploy extensive organizational and technical measures; these are described in the following.

B. Rapid Takedown Policy for Cases of Malicious Activity

The dotKoeln GmbH (and RyCE GmbH as its technical provider) are committed to closely collaborate with law enforcement authorities and security agencies in order to take quick action in case a .koeln or .cologne name is reported to be involved in malicious activity. For this purpose, a "Rapid Takedown Policy" is established that

- Identifies cases of malicious activity,
- Defines ways for the registry to be notified of such activity (e.g. via a dedicated web site, e-mail address or phone hotline),
- Defines clear and consistent procedures to quickly stop the malicious activity (after the activity was confirmed and impact of the measures has been assessed),
- Defines related service levels (e.g. with respect to the maximum time the registry may take to respond to takedown requests),
- Defines rules regarding the notification of involved parties (registrant, administrative contact, technical contact, registrar, informant, the public),
- Defines ways to appeal against any measures taken,
- Defines how cases covered by the policy need to be documented and reported.

In this context, cases of malicious activity may include (but are not limited to)

- Wrong, invalid or harmful DNS setup (e.g. pointers to false IP addresses),
- Use of trademarked or otherwise reserved names without proper rights,
- Use of the domain in actions that affect the stability and security of the Internet (e.g. in Denial of Service (DoS), Distributed Denial of Service (DDoS) attacks or botnets),
- Use of the domain for the distribution of malware (such as computer viruses, worms, Trojan horses, spyware or rootkits),
- Use of the domain for phishing or scamming,
- Use of the domain for spamming (affecting e-mail or other forms of electronic messaging),
- Maintaining invalid registrant contact data in the domain.

- Where applicable, the policy includes metrics and thresholds for finding quantitative indications of malicious conduct.

Procedures to stop malicious activity may include (but are not limited to)

- Notifying the domain's sponsoring registrar, specifying a deadline until which the activity needs to be ceased,
- Notifying the domain's registrant, administrative or technical contact directly (again specifying a deadline until which the activity needs to be ceased),
- Locking the domain and putting it on hold in order to prevent changes to the domain and to remove it from the .koeln/.cologne zone ("takedown"),
- Deleting the domain name and blocking it from further registration if need be.

Escalation rules (defining which steps are to be taken in which order and conditions for moving on to the next, more drastic measure) are part of the policy. Since removing a domain name from the .koeln or .cologne zone usually has serious consequences (such as rendering web sites and e-mail addresses utilizing the domain name unusable), the dotKoeln GmbH (and RyCE GmbH as its technical provider) will, in accordance with the policy, exercise extreme caution with regard to any takedown decision. At the same time, the dotKoeln GmbH is aware that malicious activity potentially affects a large number of Internet users, which sometimes warrants drastic measures.

The Rapid Takedown Policy aims at finding appropriate measures, taking the interests of all involved parties into consideration. The Rapid Takedown Policy will be announced to both .koeln/.cologne registrars and .koeln/.cologne registrants and be part of the Registry-Registrar Agreement (RRA) and the .koeln/.cologne registration terms.

For cases of phishing, the dotKoeln GmbH will work closely with all relevant Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) of the area to develop an anti-phishing-specific simplified Rapid Takedown Policy. The goals will be to:

- Get all CERTs and CSIRTs of the area (at least, but open to other CERTs) accredited as authorized interveners,
- Develop criteria and checklists for domain names eligible for rapid suspension,
- Develop a secured communications method between the authorized interveners and the dotKoeln GmbH including an affidavit form.

Names reported by authorized interveners will be suspended regularly during business hours, but after 24 hours at the latest. This system should expand to a global authorized interveners list. In this regard, the dotKoeln GmbH will work with the Anti-Phishing Working Group and other initiatives in order to develop and complete their proposed Accelerated Take Down proposal, which is still in beta stage.

a. Specifics for .koeln and .cologne

In addition to the above, the following applies. According to dotKoeln GmbH abusive behavior comprises

- Trademark infringement
- Lack of legitimate interest
- Proof of bad faith

Cases of trademark infringement will in any case be handled in compliance with the resolution processes set out by ICANN and through the respective service providers. Therefore the definition of trademark infringement also rests upon ICANN. A legitimate interest is considered as given if:

- The registrant has used the name in relation with the offer of goods or services or has verifiably made respective preparations prior to the announcement of the dispute resolution proceeding
- The registrant is a company, organization or natural person that is generally known under this name, even though no registered right exists
- The registrant uses the name in a legitimate, non-commercial or fair manner without causing user confusion or corrupting the name's image

Many of these guidelines are also in line with ICANN's perception. Lastly, dotKoeln GmbH will declare a registrant to act in bad faith if:

- It becomes evident that the registrant acquired the domain name mainly with the purpose of selling, renting or in any other form assigning the domain to the proper owner or a public institution
- The domain name was registered in order to prevent the proper owner or a public institution from using this name as a domain name
- The domain name was primarily registered with the goal of disturbing the professional or organizational activity / activities of a competitor
- The domain name is used in order to attract Internet users to one's own website with the goal of profit maximization.

b. Policies for handlings complaints regarding abusive behavior

Requests and complaints submitted via the contact form will be received by dotKoeln GmbH as well as the technical service provider. Thereby, the technical service provider will immediately become informed as to the problem brought forward.

dotKoeln GmbH expects the respective registrars to handle complaints by registrants or third parties. Thus, dotKoeln GmbH will redirect incoming complaints to the respective registrar who services the allegedly abusive registrant.

dotKoeln GmbH commits to redirect complaints within one working day (Monday through Friday) upon receipt. In return registrars are also obligated to contact the complainant within one working day upon receipt of the complaint from dotKoeln GmbH.

In handling complaints, dotKoeln GmbH will obligate registrars to adhere to the relevant resolution procedures set out by ICANN, i.e. the Uniform Domain Name Dispute Resolution

Policy (UDRP) and the Uniform Rapid Suspension (URS).This means that in cases of trademark infringement the registrar shall inform the claimant that he/she can file a claim with the respective service providers and provide the relevant contact information. dotKoeln GmbH will then implement all decisions made throughout the resolution process.

Depending on the type of complaint, a proper court proceeding or an extrajudicial conciliation between the two parties will be enforced. This however will only take place as long as there is no special resolution process set out by ICANN. The decision whether a court proceeding or an extrajudicial conciliation will take place will depend on the registrar's as well as the contending party's wish.

c. Resolutions for abusive behavior

dotKoeln GmbH will lock domains within 24 hours in two cases:

- A proper court or an arbitration committee has declared that the respective domain name is defamatory or racist or is in breach of public law. As soon as dotKoeln GmbH receives the verdict, the domain name will be locked within 24 hours and will remain suspended from further registration.
- dotKoeln GmbH receives a "Notice of Complaint" from a URS Provider. This process is further elaborated upon in the answer to question 29 "Rights Protection Mechanism". Besides locking domains in certain cases, dotKoeln GmbH will withdraw any domain if instructed to do so by relevant service providers (e.g. URS Provider), a proper court or an arbitration committee. The final decision will in any case be with the mentioned decision-making bodies.

C. Abuse Point of Contact

To ensure that the dotKoeln GmbH gets notified of any cases of abuse as quickly and easily as possible, an area of the public web site www.nic.koeln operated by the dotKoeln GmbH for the .koeln and .cologne TLD will be dedicated to the reporting of such cases. The web page establishes a single point of contact where abuse cases can be reported (abuse@nic.koeln). Every case reported will raise a high-priority ticket within the support staff's ticket system, examined immediately and treated in accordance with the Rapid Takedown Policy.

D. Prevention of Domain Name Tasting and Domain Name Front Running

The life cycle of a .koeln or .cologne domain name includes a 5-day Add Grace Period (AGP) during which a newly created domain name may be deleted with a refund of the domain fee. This is common practice and corresponds to the policies of almost all existing generic top level domains.

However, in the past the Add Grace Period has been abused for practices such as domain name tasting and domain name front running. Domain name tasting means that domains were created simply for the purpose of testing whether revenue can be generated by e.g. creating a web page with advertisements for the domain; if this was found feasible within the first few days, the domain

was retained, otherwise it was deleted within the add grace period for a full refund, i.e. the domain was "tasted" for potential revenue without any payment to the registry. Domain name front running refers to the practice of pre-registering domain names somebody has merely expressed interest in (e.g. by searching for them on the WHOIS web frontend of a registrar) with the purpose of reselling the domain to that person (at an inflated price) afterwards; again, the Add Grace Period has been abused for this purpose, since a registrar could do that without any cost (if the unsold domain was deleted before the end of the add grace period).

In 2008, ICANN introduced the so-called "AGP Limits Policy" (http://www.icann.org/en/tlds/agp-policy-17dec08-en.htm) which addresses these and other issues resulting from the Add Grace Period. As the registry operator for the .koeln and .cologne TLD, RyCE GmbH will fully implement this policy by restricting Add Grace Period refunds to registrars according to the limits specified by the policy. At the end of every month, the registration system's billing module will determine every registrar's net domain adds and check whether the add grace period refunds granted during that month exceed the permissible number according to the policy; if this is the case, additional charges to the registrar's account will be initiated to effectively revert the excessive refunds.

Any exemption requests by registrars, whether they were granted (as permitted by the policy) or rejected, are documented, and such documentation will be maintained and made available for review by ICANN on request. The registry's monthly report to ICANN will contain per-registrar information on the granted add-deletes, as well as additional columns regarding the exemption requests.

The related report columns are (with column header names in parentheses):

- Number of AGP deletes ("domains-deleted-grace")
- Number of exemption requests ("agp-exemption-requests")
- Number of exemptions granted ("agp-exemptions-granted")
- Number of names affected by granted exemption request ("agp-exempted-domains")

E. Prevention of Domain Name Sniping (Grabbing)

Domain name sniping (also known as "grabbing") is another common abuse pattern; the name refers to the practice of trying to re-register potentially interesting domain names immediately after they are deleted (sometimes by accident, or because a registrant failed to renew the domain with his registrar in time).

Since .koeln and .cologne domains are (per registry policy) automatically renewed when they reach their expiration date, no explicit renewals by registrars are required to prevent a domain name from being deleted when they expire. Registrars need to explicitly delete domains in order to release them for re-registration. This substantially reduces opportunities for domain name sniping.

However, registrars may still send unintended domain deletions, i.e. due to clerical errors or miscommunication with the registrants. Even for these cases, measures against domain sniping are in place. Starting in 2002, registries have begun to implement an ICANN proposal, the so-called "Redemption Grace Period" (RGP, http://www.icann.org/en/registrars/redemption-proposal-

14feb02.htm). The proposal recommends introducing a 30-day period after a name's deletion during which the name is removed from the TLD zone (in order to give the registrant the chance to take notice of his name's deletion) but is still eligible for being restored by the previous registrar/registrant. Supporting the RGP significantly reduces chances for domain grabbers to obtain inadvertently deleted domains, since a registrant gets 30 days to notice the mistake and to restore the domain before it becomes available for re-registration.

The Registration System used by RyCE GmbH to operate the .koeln and .cologne TLD supports the Redemption Grace Period as proposed by ICANN and implements it in full compliance with RFC 3915 ("Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)").

F. Prevention of Orphaned Glue Records

According to the definition found in the "SSAC Comment on the Orphan Glue Records in the Draft Applicant Guidebook" (http://www.icann.org/en/committees/security/sac048.pdf), a glue record becomes an "orphan" when the delegation point NS record (the "parent NS record") that references it is removed while retaining the glue record itself in the zone. Consequently, the glue record becomes "orphaned" since it no longer has a parent NS record. In such a situation, registrars and registrants usually lose administrative control over the record, and the record's attribution to a certain registrar may become unclear, which makes it a potential vector for abuse.

The glue record policy in effect for the .koeln and .cologne TLD avoids this situation entirely by disallowing orphan glue records altogether. The technical implementation within the Registration System and its associated zone generation process ensures this by the following measures:

- As a general principle, glue records are only created if they are really necessary, i.e. only in the case where a name server (e.g. "ns.example.koeln") is used for the delegation of a superdomain of its own name, e.g. "example.koeln" in this example. If the same name server is used for e.g. "example2.koeln", no glue record is created.
- A host object within the TLD (like "ns.example.koeln") cannot exist without its parent domain ("example.koeln"). Any attempt to create the host "ns.example.koeln" will be rejected by the SRS if
- the domain "example.koeln" doesn't already exist or is not sponsored by the registrar creating the host. Likewise, the domain "example.koeln" cannot be deleted by the registrar if subordinate hosts like "ns.example.koeln" still exist. These subordinate hosts have to be deleted before the domain itself may be deleted; if such hosts are used in delegations for other .koeln/.cologne names, these delegations in turn have to be removed before the host may be deleted.
- If a domain name is put on hold (e.g. as a consequence of the Rapid Takedown Policy described above), this not only means that the delegation for the name itself is removed from the zone; it also means that any occurrences of NS records referencing a name server that is subordinate to the domain are also removed from other .koeln or .cologne domains, along with any accompanying glue records. The same of course holds true should the domain name have to be deleted entirely by the registry.

Consequently, no glue records can exist for a certain domain in the .koeln or .cologne zone after that domain is put on hold or deleted as part of abuse prevention or mitigation procedures.

It should be noted that this policy may lead to other domains (not directly involved in the abuse case) being affected by the takedown if they were delegated to a name server subordinate to the offending domain. Depending on their overall DNS architecture, such domains may become unreachable or less reachable after the delegation point is removed. While this could in theory be avoided by a less rigid orphan glue record policy, the overall benefit of adopting the strict policy described above is deemed higher than the potential damage to domains using a DNS infrastructure depending on an offending domain name.

G. Preventing Use of Trademarked, Reserved, Invalid, Illegal or otherwise Unsuitable .koeln/.cologne Names

The dotKoeln GmbH takes extensive measures to protect the legal rights of others (such as trademark holders) with regard to .koeln and .cologne domain names. This includes

- Conducting a Sunrise phase to allow trademark holders to secure names related to their trademarks prior to GA,
- Accessing a Trademark Clearinghouse to validate trademarks presented by registrants,
- Offering a Trademark Claims Service, at least during the first 90 days of general availability,
- Taking precautions against phishing and pharming and
- Committing to full compliance with established Dispute Resolution and Suspension Procedures, including the Uniform Rapid Suspension (URS), the Trademark Post-Delegation Dispute Resolution Procedure (TrademarkPDDRP), and the Uniform Domain Name Dispute Resolution Policy (URDP).

In order to prevent from domain name registrations which are defamatory, racist or in breach of public law, dotKoeln GmbH in collaboration with the Cologne City Council has compiled a list of names and terms which will be blocked. These names and terms will not be available for registration over the entire registry lifespan, i.e. at least for ten years. If however, a domain name happens to be registered which is defamatory, racist or in breach of public law the above mentioned process will set in and the respective name will be added to the existing list of blocked names.

In addition to these specific rights protection measures, the Registration System provides the following general means to make sure that no .koeln or .cologne names are registered which are for other reasons deemed invalid, reserved, illegal, offensive or unsuitable.

a. Rule Engine

For the most part, this is achieved by the deployment of a complex rule engine that checks each registered name at the time of registration for compliance with a configurable set of rules. Among other things, these rules include

- A test to ensure that the domain name has the proper number of labels (which is two for a traditional registry that allows only second level domains to be registered),
- A test to ensure that no hyphens occur in position 3 and 4 of any of the domain's U-labels (to protect "xn--" and future ACE prefixes),
- A test to disallow hyphens at the beginning or end of the name,
- A test to disallow ASCII characters which are neither a letter, nor a digit or a hyphen,
- A test to find invalid IDN characters, i.e. characters not contained in any of the supported IDN tables,
- A test to disallow reserved geopolitical names,
- A test to disallow registry reserved names,
- A test to disallow ICANN reserved names,
- A test to disallow otherwise reserved or unsuitable names.

For the tests checking for reserved names, custom lists of labels can be conveniently maintained by the dotKoeln GmbH to define the disallowed names for each category. Additional categories can also be added as required for enforcing specific policies of the .koeln and .cologne TLD.

The rules are stored in database tables (rather than static configuration files), which means rules can be added, deleted or altered by authorized registry personnel without requiring a shutdown or restart of the .koeln/.cologne SRS. Should eligible parties approach the dotKoeln GmbH (via a registrar) providing sufficient evidence of their eligibility for a specific reserved domain name, the dotKoeln GmbH can enable the chosen registrar to register the domain name for that specific registrant only (circumventing the rule engine check that would otherwise prevent the registration).

b. Compliance with Specification 5 of the Registry Agreement

The rule engine is the central system component ensuring that the dotKoeln GmbH will operate the .koeln and .cologne TLD in full compliance with Specification 5 ("SCHEDULE OF RESERVED NAMES AT THE SECOND LEVEL IN GTLD REGISTRIES") of the Registry Agreement. Unless the dotKoeln GmbH is otherwise authorized by ICANN and the Government Advisory Committee (GAC) in writing, the rule engine for .koeln and .cologne will be set up to prohibit the registration of the labels and label types listed in Specification 5 by registrars.

H. Domain Data Access Control

One important point of attack that may lead to abuse of .koeln or .cologne domains and their associated data is the unauthorised or excessive access to data stored within the .koeln or .cologne repository. This applies to both read access (e.g. via public interfaces such as the port 43/web WHOIS) and write access (such as registrar interfaces like EPP or the web-based Control Panel). The measures taken in the .koeln/.cologne TLD to properly restrict access are laid out in the following.

a. Prevention of WHOIS Data Mining

The port 43/web WHOIS interfaces grant public access to domain, host and contact data. As such they are a potential target for data mining, i.e. the retrieval of large amounts of postal or e-mail addresses for e.g. the purpose of advertising.

The WHOIS implementation provided by the Registration System prevents such data mining attempts, most importantly by the following measures:

- Access to all WHOIS interfaces is rate-limited (when accessed from IP addresses not whitelisted for unlimited access).
- Web interface users seeking access to extended WHOIS search capabilities are required to authenticate by entering login credentials (which are only issued to eligible parties).
- For improved spam protection, E-mail addresses may be displayed as images only in the web-based WHOIS.
- Contact disclosure flags as specified in RFC 5733, the Extensible Provisioning Protocol (EPP) Contact Mapping, are fully supported. This gives registrants enhanced control over the contact fields they want to disclose in the WHOIS. In this respect, the system is configurable and allows restricting the use of EPP contact disclosure settings via rules defined by specific registry policies or legal requirements.

b. Prevention of Unauthorized Data Modifications

Domain data within the .koeln/.cologne TLD is exclusively provisioned by registrars, i.e. registrants have no direct write access to their data within the repository; all their modifications have to be done via the registrar sponsoring the respective domain. In this constellation, registrants need to trust their registrar and will expect that the management of their domain is conducted in a diligent and correct manner. This means that the registry's interfaces used by registrars need to be secured in order to only allow the sponsoring registrar of a domain (and nobody else) to modify domain data.

The EPP interface provided by the Registration System does this by

- Requiring SSL/TLS on the transport layer,
- Requiring a strong EPP password (minimum length, mandatory digits and non-alphanumerical characters),
- Requiring registrars to supply lists of IP addresses or subnets from which exclusive access will be granted,
- Requiring registrars to use SSL client certificates known to and trusted by the registry, thus providing an additional means of authentication beyond the EPP password.

Likewise, the web-based Control Panel

- Requires SSL/TLS on the transport layer,
- Requires registrars to log in with a user name and password (for which the same rules regarding minimum length, mandatory digits and non-alphanumerical characters apply),

- Requires registrars to supply lists of IP addresses or subnets from which exclusive access will be granted,
- Requires registrars to install SSL client certificates known to and trusted by the registry in their web browsers, thus providing an additional means of authentication beyond the web password.

I. WHOIS Accuracy

Since .koeln and .cologne are operated as so-called "thick registry", the .koeln and .cologne WHOIS displays information about the registrant, as well as the administrative, technical and billing contacts of every domain. In cases of malicious or abusive activity involving a .koeln or .cologne domain, this WHOIS contact information usually is the first and most important source of information, e.g. for law enforcement authorities, to determine the people or organisations responsible for the domain in a timely manner. Consequently, it is deemed very important to maximise the accuracy of contact information stored in the registry repository.

The dotKoeln GmbH (and RyCE GmbH as its technical provider) are therefore committed to take diligent measures to promote WHOIS accuracy, including (but not limited to) the following:

- Contact data completeness policy: The thick registry model used for .koeln and .cologne mandates the association of each domain with exactly one registrant, one administrative contact, one technical contact and one billing contact. The data of all used contacts is stored in the registry repository. While RFC 5733, the Extensible Provisioning Protocol (EPP) Contact Mapping, merely requires contact data to contain a name, a city, a country code and an e-mail address for a syntactically complete EPP request, the .koeln and .cologne TLD policy for contact data mandates the specification of at least one address line (street), a voice phone number and a postal code in addition. This means that, in addition to the XML schema validation conducted by the .koeln/.cologne SRS for every EPP request received from the registrar (which ensures the presence of all RFC-mandated contact data), the SRS also requires these essential fields to be present and will reject requests lacking them with a "parameter value policy error" message. The validation done by the SRS also goes beyond validating against the EPP XML Schema Definitions (XSDs) with respect to field content. For instance, contact e-mail addresses are required to contain an '@' character and a valid domain name; this is not mandated by the XSDs specified in RFC 5733
- Contact data monitoring: On a regular basis, the registry will run automated plausibility audits on the contact data submitted by registrars. Using publicly available databases, contact address lines will e.g. be mapped to cities and zip codes, which are then compared to the ones provided by the registrant. Likewise, phone and fax numbers will be checked for plausibility.
- Domain data change notifications: The Registration System used to operate the .koeln and .cologne TLD can be configured (on a per-registrar basis) registrant and the administrative contact in order to reach multiple people concerned with the domain) after every change made to the domain (i.e. alterations of associated contacts or name servers). When enabled, this feature allows unauthorized or unintended changes to domain and contact data to be detected immediately. This functionality will however need to be deployed after consultation with .koeln/.cologne registrars, since many registrars do

not endorse direct communication between the registry and registrants, i.e. their customers.

- WDRP auditing: In 2003, ICANN adopted the so-called "WHOIS Data Reminder Policy" (WDRP, http://www.icann.org/en/registrars/wdrp.htm) which obliges ICANN-accredited registrars to send yearly WHOIS data reminder notices to registrants. These notices contain the WHOIS data currently on file for the respective domain, as well as instructions for the registrant about ways to correct the data if required. While the dotKoeln GmbH does not intend to replicate this reminder procedure on the registry level, it will establish an auditing process that monitors the WDRP activities of .koeln and .cologne registrars to make sure that WDRP responsibilities are honored.