RICKERT.LAW

Rickert Rechtsanwaltsgesellschaft mbH ■ Colmantstraße 15 ■ 53115 Bonn

Hamburg District Court
Sievekingplatz 1
20355 Hamburg

Your sign:	310 O 99/21	Attorney:	RA Thomas Rickert
Our sign:	REDACTED	E-mail:	kanzlei@rickert.net

per beA

Bonn, 31.08.2021

Proceedings

REDACTED ./. Quad9 Foundation

310 O 99/21

filed on behalf of and by proxy for the defendant

Opposition

Rickert Rechtsanwaltsgesellschaft mbH

Rechtsanwälte
Thomas Rickert[1]
Patrick Jardin[2]
Carsten Toß[2]
Roman Wagner[4]
Jan Lutterbach[2]
Matthias Bendixen[3]
Nicolas Golliart[3]
Lena Wassermann[3]
Christian Kirchberger[2]
Sandra Schulte[3]
Jasmin Eul

Kanzlei
Colmantstraße 15
53115 Bonn
Tel.: +49.228.74 898.0
Fax: +49.228.74 898.66
www.rickert.law

HRB 9269
AG Bonn

Geschäftskonto
Commerzbank AG
IBAN: DE81 3804 0007 0241 4480 00
BIC: C0BADEFF380

Deutsche Bank AG
IBAN: DE20 3807 0059 0053 1012 00
BIC: DEUTDEDK380

Anderkonto
Commerzbank AG
IBAN: DE55 3804 0007 0241 4480 80
BIC: COBADEFF380

[1]Geschäftsführender Gesellschafter
[2]Senior Associate Partner
[3]Associate Partner
[4]Of Counsel

to the preliminary injunction issued by the resolution dated May 12, 2021.

It is requested,

to annul the preliminary injunction and reject the underlying application.

It is further requested,

to suspend the execution of the preliminary injunction without the provision of security.

Justification

The ban imposed by the order is unjustified. The respondent is not liable as an interferer. The respondent was not informed of a specific infringement of the law. Even if proper notice had been given, the respondent is not liable as an interferer on account of its privileged status under the German Telemedia Act (German Telemedia Services Act), since the respondent did not make an adequate and causal contribution to making the music album "REDACTED" available to the public, and due to the disproportionate nature of the claim. The preliminary injunction should be lifted.

I. Facts

1. No active legitimation / no rights of use of the applicant

The applicant's place of business is in Munich. The applicant claims that it is the owner of the (exclusive) rights of use with regard to the music REDACTED.

The applicant does not substantiate its right to bring an action. In particular, it does not submit any written evidence showing that it has been granted the exclusive rights of use to the works at issue in the proceedings and the right to pursue legal action.

In this respect, it is disputed that the applicant has the right to act as the owner of the exclusive rights of use within the meaning of Section 31 German Copyright Act with regard to the album "REDACTED by the music group " REDACTED". The applicant does not state which rights of use it holds in the said work.

2. The respondent

2.1 Charitable foundation

The respondent is a charitable foundation under Swiss law, which is financed by donations and does not pursue any commercial purposes.

Supporting documentation: Internet excerpt from the Commercial Register Office of the Canton of Zurich, as **Annex AG 1**.

With regard to the reputation of the respondent, it should be mentioned that the City of London Police, for example, recommends the use of the respondent's service and discusses its advantages and use.

Supporting documentation: Screenshot of the City of London Police publication at http://news.cityoflondon.police.uk/r/945/ibm__packet_clearing_house_and_global_cyber_allia, a translation can be submitted later if necessary, as **Annex AG 2**.

2.2 Technical service

2.2.1 DNS service of the respondent

The respondent operates so-called recursive resolvers as an independent DNS service.

It provides its service exclusively in the public interest and without profit motive.

The aim of the respondent is to provide a service which prioritizes the data protection of the user. Since a query is made via a DNS resolver every time a website is visited by entering a Uniform Resource Locator (URL) in the browser, the data accruing there, including that attributable to a person, is of economic interest and is regularly commercialized by other parties.

Supporting documentation: Affidavit of REDACTED, **as annex AG 3**.

The respondent, on the other hand, does not log any user data and does not create profiles of users.

Supporting documentation: Affidavit REDACTED and translation from English into German, **as annex AG 4**.

Protecting users from unwanted collection and processing of their data is in the public interest.

2.2.2 Domain Name System / Recursive Resolver

The Domain Name System (DNS) is commonly compared to a telephone directory in which the names of subscribers are assigned to the respective telephone numbers. In the DNS, alphanumeric domains are associated with numeric IP addresses.

However, the telephone directory comparison does not fully explain the role of the respondent's DNS service. Imagine three people, the first of whom wants to know a phone number ("user"), the second of whom is halfway to the phone book ("recursive resolver") and the third of whom holds the phone book in their hands or manages the phone book entry ("authoritative DNS server"). In this analogy, the respondent has the role of the second person, who neither knows the first nor the third person and is not related to them and, moreover, has neither influence over nor knowledge of who is behind the requested telephone number. This second person merely passes on the requested information. The defendant thus only passes on the inquiries and their answers. The content behind the telephone number is neither understood nor analyzed by the defendant.

An elaboration upon the telephone directory analogy is required in that there exists nothing analogous to a central telephone directory, rather a directory service provides information on where a telephone directory entry can be found. In the second step, the query is more like the query of a telephone directory service in companies, where information is not obtained for a central telephone number, but rather information about potentially thousands of extensions of individual connections, behind which persons or devices are located.

Another peculiarity is that some "telephone directory operators", i.e. operators of authoritative name servers, want their information to remain in the memory of the second party for a certain time ("Time to Live" or "TTL"), i.e. so that users' queries can be answered without having to retransmit their queries to the authoritative DNS server each time.

DNS queries can be answered in two ways - authoritatively or recursively.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

When answering DNS queries authoritatively, information is obtained from a local zone file specified by the owner of the zone.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

Authoritative DNS queries are answered by authoritative name servers, which are the source of information on how DNS queries are to be resolved. Thus, it is the authoritative name servers that associate domains or hosts with an IP address. For each domain, there is only one authoritative source of records. If the authoritative name server record is deleted, the domain in question no longer resolves.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

Recursive DNS resolvers, on the other hand, exist in thousands. Almost every Internet service provider operates recursive DNS resolvers. In Germany, there are around 800 public recursive resolvers operated by ISPs. In addition, there are many more non-public recursive DNS resolvers, which are operated in corporate networks, for example.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

According to evaluations by the Shadowserver project (https://scan.shadowserver.org/dns/), 16,623 public recursive DNS resolvers were identified in Germany on August 30, 2021.

Supporting documentation: Copy printout of the website, as **annex AG 5**.

In accordance with technical standards, the respondent stores the request unchanged for as long as the Time to Live specified by the domain owner. A longer or otherwise configured intermediate storage by the respondent does not take place. Consequently, no content is cached, but only the IP address for a time frame specified by the authoritative name server, so that the DNS resolver can respond more quickly to the next request for the IP address and load upon the authoritative DNS server is relieved.

The DNS caching described above is done in accordance with "Request for Comments" (RFCs) 1034, 1035, 1123, 2181, 2308. The RFCs are documents that describe and define the technical foundations of the Internet and are managed by the IETF (Internet Engineering Task Force).

Supporting documentation: Affidavit of REDACTED and translation from English into German, **as annex AG 4**.

2.2.3 Summary: DNS service of the respondent

In summary, the automatically running DNS service of the respondent:

- does not provide any authoritative information,
- only passes through DNS queries and responses from each side to the other and
- a temporary storage of the answers only takes place in accordance with the applicable technical standards.

2.3 No contractual relationship between requestor or domain holder and respondent

Insofar as the use of the term "customers", for example on p. 2 of the order dated May 12, 2021, was intended to indicate that the defendant maintains contractual relationships with the requesters of its service, this is false. Requestors use the respondent's service via a simple configuration in their network settings. This requires neither the consent of the respondent nor the acceptance of any contractual conditions.

In fact, it also happens that requestors use the respondent's service unawares, when this is configured by their network administrator. However, there are also many requestors who deliberately choose the respondent's service in order to protect their privacy and to use the Internet safely.

The respondent therefore does not have any contractual relationships with the requestors or the authoritative DNS operators. This applies both in the direction of the operators of services

or content with regard to which DNS queries are resolved via the respondent's system and with regard to companies or persons or technical infrastructures that trigger DNS queries.

2.4 No blocking of the offending URIs possible

The defendant has no way of gaining knowledge of the services or content provided under a domain or third-level domain (such as abc.example.de) or directories (such as example.de/abc).

The automatically running DNS service can query and pass on IP addresses for domains, but not for directories or individual elements, i.e. "Uniform Resource Indicators" (URIs).

It is therefore not technically possible to block URIs.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

Blocking is only technically possible at domain level (such as domain.de or abc.domain.de). This consequently means that all URIs under the domain in question are also blocked. Implementation of the requirement of the court order is only possible by completely blocking the requests for the domains REDACTED and REDACTED and everything they contain.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

2.5 Effects of blocking on the system and the system's responses

The technical blocking of users from the territory of the Federal Republic of Germany required to implement the order is not technically provided for in the respondent's system.

In addition, the blocking of queries to the aforementioned domains, which is necessary to fulfill the requirement of the order, leads to considerable resource consumption in the respondent's technical infrastructure, to performance losses in the systems, and to longer response times for all queries to the affected systems.

Supporting documentation: Affidavit of REDACTED and translation from English into German, as **Annex AG 4**.

In the course of regular operation, process restarts are often necessary to restore a server in the event of faults. Until the restart is completed, the respective server cannot serve traffic. For a representative server that uses the implemented blocking, the inclusion of blocking technology increases the time to validate the configuration and restart the process from 0.203 seconds to 0.605 seconds. This resulted in a tripling of aborted requests during troubleshooting, which negatively impacts the perception of reliability of our service.

During a one-hour comparative performance test, disabling the custom-built blocking feature without a process restart for a single server resulted in an immediate increase from an average

of 2,700 to 3,300 responses per second. At the same time, CPU utilization dropped by 10-15% during the test period compared to an equivalent load in the hour before. This shows that the addition of this blocking technique results in higher resource utilization and a lower number of responses per server, and the potential for aborted queries under high load.

In order to build a system which implementats of the court order with an acceptable impact on performance, approximately 6 person-months of development effort would need to be expended and an additional developer and, if necessary, system administrator would need to be hired. Support staff would need to be trained on the new technology. Furthermore, processes would have to be introduced that are not technical but legal in nature.

Supporting documentation: Affidavit of REDACTED and translation from English into German, as **annex AG 4**.

In this respect, the implementation of the order, in any form, leads to a considerable burden for the respondent, which endangers its existence.

Manipulating the Domain Name System so that DNS queries are answered incorrectly can be done by various technical means ("REFUSED", "SERVFAIL" or "NXDOMAIN").

The failure of a recursive resolver results in the user switching transparently and unknowingly to a different resolver that gives them an answer. This is due to the fact that the DNS requires that at least two name servers be configured to ensure that DNS queries are answered even if one of the registered recursive DNS resolvers fails.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

The "REFUSED" response would result in inquirers not continuing to use the respondent's system because it refuses to respond. Implementing this technically dubious interpretation of the court order would jeopardize the operation and existence of the respondent.

The respondent implements the operative part of the preliminary injunction by responding to a DNS query for the disputed domain with "SERVFAIL". This means that a DNS query is no longer answered correctly with the consequence that no more IP addresses are returned.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

Typically, the users' DNS clients are configured in such a way that, after receiving a "SERVFAIL" response, they then search for a DNS resolver that can correctly answer the specific request. Normally, however, the next request following this command is then directed back to the respondent's infrastructure, so there is no immediate loss of customers to worry about.

Ultimately, however, the query is not blocked entirely, but forwarded to another recursive DNS resolver. The implementation of DNS blocking leads to inquirers being forwarded to recursive DNS resolvers that do not offer the malware protection provided by the respondent's service.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

A third option that is relevant here is the "NXDOMAIN" command, as used by the respondent for malware filtering. When the client asks for a malicious host, the respondent's resolver refuses to respond with the IP address using "NXDOMAIN", preventing the client from connecting to the malicious target. The request is thus terminated. However, responding to queries with "NXDOMAIN" is reserved for responding to queries about malicious domains and cannot be used to block, for example, the domains in dispute.

Inquirers and industry experts expect the respondent to comply with DNS standards, which in current implementations do not include mechanisms for specifying the reason for a particular response. They have advocated the use of "SERVFAIL" to avoid confusing filtered malicious domains ("NXDOMAIN", authority bit not set) with domains at issue here ("SERVFAIL"). The main difference between the two response types is that the requestors ask for malicious domains to be filtered, but have not made such a request for domains subject to a blocking order according to RFC 8914 4.17 and 4.18 (4.18 is in part a contribution by the respondent that was included in the RFC) – a standard for filtering domains – that has not yet been adopted or implemented in software due to its recency (10/23/2020).

Supporting documentation: Affidavit of REDACTED and translation from English into German, as **annex AG 4**.

Adding list entries other than those to malicious code would cause users to fear that content permitted at their location would not be available. If the lists used to increase IT security were "watered down" in this respect, the service characteristic of increasing the protection of users would be eroded. The consequence would be that the respondent's service would lose its attractiveness and a loss of users could be expected.

Supporting documentation: Affidavit of REDACTED and translation from English into German, as **annex AG 4**.

2.6 The use of filter lists (filtering) is not comparable with manual setup of DNS blocking.

The applicant has submitted that the respondent can set up DNS blocking simply because it includes filter lists of sources of malware in its system. However, the technical and legal implications of these actions are fundamentally different.

The respondent offers its service, including malware protection, in a globally uniform manner. To filter malicious domains, the respondent therefore also uses globally-uniform filter lists, which result in the respective domains being inaccessible to all users of the respondent worldwide.

On a global level, there are various organizations that maintain and keep updated lists of websites or servers that pose a threat to the security of the end devices of the requesting parties because they contain malicious code. These may be sources of phishing, botnets,

pharming or malware, for example. The lists used by the defendant are provided by organizations specializing in this area, such as abuse.ch or CERTs.

Supporting documentation: Affidavit of REDACTED and translation from English into German, as **annex AG 4**.

What the lists subscribed to and used by the defendant have in common is that the harmful offers listed there are undesirable or illegal globally and regardless of a specific jurisdiction. Moreover, the unlawfulness of the offers can be determined on its own. In this respect, the use of filter lists does not require any legal review competence or human resources.

Contrary to the assumption in the order and the submission of the applicant, the respondent does not check any of these offers, but uses these lists without checking them. It is up to the inquirers to decide whether they want to use this service, which increases network security, or not.

However, the respondent has the option of removing items from the list by creating exception rules if an entry in the filter list is found to be unjustified by way of exception. This restores the accessibility of wrongfully filtered offers.

Supporting documentation: Affidavit of REDACTED and translation from English into German, as **annex AG 4**.

A limitation of the filtering of harmful offers to certain countries, to certain user groups or regions is neither intended nor necessary due to the nature of the listed offers. The worldwide equal treatment of list entries of harmful offers also explains that a corresponding functionality to differentiate list entries per country does not exist in the respondent's system. The implementation of a DNS blocking limited geographically to a certain territory is not possible by including an entry in the filter list.

2.7 No sufficient indication by the applicant of infringement by REDACTED

Neither the letter of advice from the applicant's agent dated 23.03.2021 (Annex AST 4) nor the warning letter dated 26.03.2021 (Annex AST 6) were duly served to the respondent.

2.7.1 No receipt of the notice letter of 23.03.2021

The notice letter from the representative of the applicant dated 23.03.2021 was not properly received by the respondent.

It is denied that the applicant sent the notice letter dated 23.03.2021 to the respondent by post. The respondent did not receive such a letter by mail.

Supporting documentation:

1. Affidavit of REDACTED, as **annex AG 6**.
2. Affidavit of REDACTED, as **annex AG 7**.

Nor did the notice letter of 23.03.2021 get duly delivered to the respondent by e-mail.

After service of the order, the respondent reconstructed that the applicant used the e-mail address support@quad9.net. This is an e-mail address set up for technical inquiries about the respondent's service. All messages sent to this email address are automatically sent to the respondent's Zendesk vendor ticketing system. The Zendesk product has its own spam filters and related policies that cannot be turned off by users. Zendesk automatically creates tickets from the incoming e-mails not recognized as spam for further processing by support staff. One such ticket was created only for an e-mail dated 03/26/2021.

Supporting documentation: Affidavit of REDACTED and translation from English into German, as **annex AG 4**.

This suggests the suspicion that further e-mails from Zendesk were classified as spam and not brought to the attention of the support staff. The respondent therefore only became aware of the content of the applicant's information letter of 23.03.2021 when it was served with the decision order.

For cases with legal implications, the respondent operates an industry-standard e-mail address (RFC2142) at abuse@quad9.net that is set up specifically for abuse reports, i.e., also for reports of illegal conduct.

Supporting documentation:

1. Screenshots of websites https://www.peeringdb.com/net/17212, Whois-RWS, ipinfo and ipasn, as **annex AG 8,**

2. Affidavit of REDACTED, as **annex AG 3.**

The contact options are published at the sources mentioned above, i.e. so for the respondent also the abuse contact. The applicant should have known this. In this e-mail inbox intended for abuse cases, there is no significant spam filtering, so that the knowledge of the mail via this channel can be assumed as safe. The respondent takes abuse reports seriously and messages received via this channel are forwarded directly to management and processed there.

Supporting documentation: Affidavit of REDACTED and translation from English into German, as **annex AG 4**.

2.7.2 No receipt of the warning letter dated 26.03.2021

2.7.2.1 No receipt in advance by e-mail

The applicant states that it issued a warning to the respondent in a letter dated March 26, 2021. It claims that an expert opinion on the copyright-infringing content on the disputed domain was attached to the letter. According to Exhibit AST 6, no expert opinion was attached

to the letter, as it is not included in the attachment. The letter also does not contain an attachment note.

The warning letter was also not effectively served to the respondent. The respondent only discovered after service of the order that the e-mail dated March 26, 2021 was received in the respondent's support mailbox and a ticket was created. This was not processed further. The respondent suspects that it was ignored by support staff who are no longer employed by Quad9, likely because the email was thought to be a phishing attempt. It is part of the training for support staff not to open attachments unless there is evidence that the user is sending an attachment recognizably in good faith. Since the respondent's service is free of charge, there is no obligation to reply to inquirers, so an unanswered ticket does not automatically attract attention.

In addition to a footer, the e-mail sent by the applicant's counsel contained only the text "For immediate attention, warning urgent matter!" and an attachment in pdf format.

Supporting documentation:

1. Copy email dated 03.26.2021, as **annex AG 9.**

2. Affidavit of REDACTED and translation from English into German, as **annex AG 4**.

In the case of e-mails from unknown sources, the board member of eco Verband der Internetwirtschaft e.V. and cybersecurity consultant Mr. REDACTED also states in his affidavit that, for security reasons, it is urgently recommended not to open attachments to e-mails from unknown sources in order to prevent your own computer from being infected with malware.

"The security policy of companies should stipulate as a fundamental security aspect when receiving emails that no attachments from unknown senders should be opened. This procedure is part of every successful security certification (IT-Grundschutz, ISO 27001) and corresponds to the general recommendations of experts, such as the German Federal Office for Information Security or Heise Security:

> "The BSI therefore strongly advises against opening the attachment of e-mails from unknown senders." (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Infizierte-Systeme-bereinigen/infizierte-systeme-bereinigen_node.html.)
>
> "The most important principle for secure e-mail handling is therefore never to open a file attachment that you have not requested. " (Heise Security, https://www.heise.de/security/dienste/Dateianhaenge-472901.html)

Exceptions to this should only be made if the sender can be clearly identified and verified, e.g. by using signed emails.

For contact via central addresses (noc, abuse, hostmaster), all relevant information should be included in the body of the e-mail. For file attachments, binary files (.exe., .zip, .pdf) should be avoided to ensure processing by the recipient. “

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

2.7.2.2 No receipt by mail to the authorized recipient

The warning letter of 26.03.2021 sent by the applicant was not received by the authorized representative of the respondent by mail. The receipt of the letter is disputed.

Supporting documentation:

1. Affidavit of REDACTED, as **annex AG 6**.
2. Affidavit of REDACTED, as **annex AG 7**.

The authorized service agent for the respondent for all correspondence received at the Swiss address Werdstrasse 2 in 8004 Zurich, is the Swiss foundation SWITCH. It is the operator of the Swiss academic network of universities. REDACTED and REDACTED are responsible for managing the respondent's incoming mail. Both have affirmed under oath that there was no incoming mail from the applicant's procedural representative for the respondent. Only the order of the Hamburg Regional Court with the file number 310 O 99/21 was delivered to Werdstrasse 2 in 8004 Zurich and immediately forwarded to the respondent.

Supporting documentation:

1. Affidavit of REDACTED, as **annex AG 6**.
2. Affidavit of REDACTED, as **annex AG 7**.

2.7.2.3 No receipt of the letter dated 08.04.2021

The further warning letter of 08.04.2021 from the attorney of record of the applicant has also not been sent to the respondent. Since the e-mail from the applicant's counsel dated 26.03.2021 did not land directly in the spam folder, a ticket was automatically generated. This generated a ticket number (15321) and sent an automatic message to the applicant's procedural representative that the e-mail had been received and further communication on the matter should be sent in response to this automatically generated e-mail. In response to this automatically sent reply, the applicant's legal representative did not reply, but sent a new e-mail containing the same text as the e-mail of 26.03.2021. The system did not create a ticket for this, so it can be assumed that this e-mail was also discarded by the spam filter.

2.7.3 No sufficient claims raised vis-a-vis other parties involved

The applicant claims that it has made extensive efforts to put an end to the infringing offer, with the involvement of those involved parties that were to be approached with priority. The applicant claims that it cannot determine the data of the operator of the REDACTED website due to a lack of a legal notice on the website. The provision of a legal notice is not required

under every legal system, so that the efforts of the applicant may by no means end with the search for a legal notice.

As already explained, the letters were not received by the respondent. Consequently, it must be assumed that other possible parties involved did not receive any letters of notification either. It is disputed that the other parties received the letters.

It is questionable what efforts the applicant made at all to have the specific infringement, the retrievability of the music album " REDACTED," eliminated by other parties.

The notice letters from the applicant's legal representative relevant to the proceedings were allegedly issued on March 23, 2021. Just three days later, in a letter dated 26.03.2021, the applicant made a claim against the respondent as an interferer by means of a warning with costs. According to the warning letter (Annex AST 6), the applicant requested the operators of the offending domain to delete infringing content for the first time on March 23, 2021. The claim against the respondent and the perpetrators of the asserted infringement thus occurred simultaneously. In this context, the much too short period of time between the notice and the warning is criticized as a precautionary measure.

The applicant's actions suggest that its primary goal is to claim costs from the defendant. At the very least, it must be assumed that any letters of notification sent to the other parties involved were merely pro forma and not issued in a serious effort to remedy the situation or to give the allegedly notified parties sufficient opportunity to remedy the situation.

2.7.3.1 No claims raised vis-a-vis the registry

No claim was made by the applicant against the commercially operated registry of the domain REDACTED. Domains ending in ".to", the country code extension for Tonga, are administered by Tonic Domain Corporation, which is headquartered in the USA. According to its website, the registry can be reached at the following address: Tonic Domains Corp, P.O. Box 42, Pt San Quentin, CA 94964, U.S.A.

Supporting documentation: Screenshot from the website of the registry Tonic at https://www.tonic.to/faq.htm, as **Annex AG 10.**

The registry Tonic writes on its website:

"...any activities deemed by Tonic to be inappropriate or illegal may be removed from the .TO zonefile without notice to the registrant."

The registry thus reserves the right to prevent the resolution of an infringing domain.

Supporting documentation: Screenshot from the Tonic registry website at https://www.tonic.to/faq.htm, as **annex AG 10**.

Tonic maintains a contractual relationship with the domain owner of REDACTED and, in this respect, can also implement contractual sanctions "at the source" and thus globally prevent the functionality of the domain.

There is no evidence that the applicant contacted the registry Tonic to block the domain. However, this does not exhaust the possibilities to contact the domain holder in the context of Tonic.

The "FAQs," the registry's frequently asked questions and answers, also state:

> *"When you attempt to register a name that is already registered, the web page that is returned has a link that sends your contact email address to the registrant. Whether they choose to reply to your email or not is up to them."*

Supporting documentation: Screenshot from the Tonic registry website at https://www.tonic.to/faq.htm, as **annex AG 10**.

If an attempt is made to register a domain that has already been registered, the e-mail address will be sent to the domain holder on request with the request to establish contact, this way the domain holder can be contacted. There is also no evidence that the applicant has made use of this possibility.

The reference to the fact that no Whois data can be determined is also insufficient. The applicant has not shown that it has requested information about the domain holder's data from the registry.

With the entry into force of the GDPR, a large number of registries worldwide have changed their practice and no longer publish personal data in the public Whois. Rights holders as well as other interested parties in non-published registration data are in this respect referred to inquiries with the registries or registrars.

Supporting documentation: Affidavit of REDACTED, as **annex AG 3**.

2.7.3.2 No claims raised vis-a-vis the registrar

A registrar is an organization or company that performs domain registrations. Many registries do not allow the registration of domains directly, but only via registrars. The applicant has not shown whether in the present case the domain was registered via a registrar and whether a registrar was contacted in order to prevent the domain from being resolved or to have the domain deleted.

2.7.3.3 No Sufficient Assertion of a Right to Information vis-a-vis the Payment Service Provider

The operators of the offending domain accept payments via the provider " REDACTED". This provider must necessarily have either the identity or at least information about it from the

operators of the disputed domain in order to be able to forward funds that could have been requested. The factual submission of the applicant does not indicate that the payment service provider was approached in a sufficiently clear and substantiated manner. In addition, the receipt of the letter has not been proven.

2.7.4 No Sufficient Submission of Facts on the Illegality of the Offer

The recommendation of the Clearing House for Copyright on the Internet (CUII) of March 9, 2021 on the implementation of DNS blocking with regard to REDACTED also only came to the attention of the respondent when the petition was forwarded by the petitioner's counsel, i.e., after the order had been issued.

The Audit Committee's statement that there has been a clear infringement by the provision of links by the operators of REDACTED is disputed.

In order to upload information to the REDACTED platform, it is necessary for the user to set up an account –- with a user name and password – and provide an e-mail address. A download link uploaded by a user is then placed online. However, according to the registration conditions of the REDACTED platform, users are prohibited from committing copyright infringements via the platform.

Supporting documentation: Screenshot of the terms of use of the REDACTED website at REDACTED, **attached AG 11**.

These statements suggest that copyright infringements are not tolerated by the operators of the REDACTED. It is inexplicable why the applicant did not include the expert opinion of CUII in the course of the initial contact in order to enable the alleged infringement to be traced and remedied promptly.

2.7.5 Initial acknowledgement by order of 12.05.2021

After all this, it is clear that the respondent was first made aware of the process as a whole when the order of the Hamburg Regional Court was served on May 12, 2021. Subsequently, the respondent had the matter examined from a legal and factual point of view and then took the technical measures available to it within a reasonable period of time in order to restrict the content that allegedly infringed the rights of the applicant. Consequently, the respondent acted within the time limit and cannot be held liable as an interferer by way of injunction proceedings, as the applicant did not send the respondent either the letter of 23.03.2021 or the allegedly subsequent warning letters. This omission is to the detriment of the applicant.

3. Receipt of the application for a preliminary injunction

The applicant makes a credible case by means of the affidavit of Mr. REDACTED (Annex AST 3) that it became aware of the infringement on March 11, 2021. The application for a temporary injunction was received by the court on April 12, 2021.

II. Legal Assessment

A. Inadmissibility

The application for a preliminary injunction is inadmissible.

1. Hamburg Regional Court not locally competent

The Regional Court of Hamburg does not have local jurisdiction pursuant to § 32 German Civil Procedural Code.

The jurisdiction of the court in preliminary injunction proceedings follows the jurisdiction for a - hypothetical - main action pursuant to Sec. 937 (1) in conjunction with Sec. 943 (1) Alt. V. m. § 943 para. 1 Alt. 1 German Civil Procedural Code (see Vollkommer, in: Zöller, German Civil Procedural Code, 32nd ed. 2018, § 919 margin no. 9).

A tort within the meaning of Section 32 German Civil Procedural Code in the case of an alleged infringement of copyright or related rights by making the subject matter of protection publicly available via a website takes place in Germany if the rights asserted are protected in Germany and the website is publicly accessible in Germany (see BGH, judgment of April 21, 2016 - I ZR 43/14 - An Evening with Marlene Dietrich, juris para. 18). In order to establish jurisdiction, it is sufficient to conclusively allege facts on the basis of which a tortious act committed in the jurisdiction is established. The provisions on local jurisdiction (§§ 12 et seq. German Civil Procedural Code) also indirectly regulate the demarcation between the jurisdiction of German and foreign courts (see BGH, judgment of 02.03.2010 - VI ZR 23/09, juris marginal no. 7 with further references).

The applicant bases her claims on the fact that the music album in dispute was made publicly accessible via the website mentioned in the tenor of the injunction under the URLs specified in the application without the applicant's consent and that these could be accessed in Germany. However, according to the correct opinion of the AG Hamburg, an infringement of rights on the territory of the Federal Republic of Germany does not establish universal jurisdiction of all courts in the Federal Republic of Germany:

> *"Even if there may be a senate of the BGH in the context of press law that shares the thesis of the omnipotent jurisdiction of all courts of the republic in cases of the kind at issue here, it is sufficiently clear from other case law of the BGH that there are also BGH senates that attach decisive importance to teleological considerations and the conclusions from the constitutional requirement of the statutory judge. There does not yet appear to be any established case law in this respect. A relevant decision of the BVerfG is also not yet apparent. For example, the Federal Court of Justice has noted for the comparable problem in establishing international jurisdiction of German courts in the context of copyright infringements that "there is much to be said for limiting an*

otherwise existing multiplicity of jurisdictions to those in whose area of jurisdiction a conflict of interests may actually have occurred" (AG Hamburg, judgment of January 30, 2014 - 22a C 100/13).

Since the defendant does not maintain a place of business within the Federal Republic of Germany, filing the application for injunctive relief at the applicant's place of business would be a relevant ground for jurisdiction.

There is no connection to Hamburg as a place of jurisdiction from any point of view. The applicant's choice of venue is an abuse of rights. An abuse of rights is assumed if a targeted selection of the venue aims at disadvantaging the defendant (see OLG Brandenburg, judgment of November 28, 2016 - 1 U 6/16, juris, marginal no. 34).

The Munich Higher Regional Court ruled that there is no reason for an injunction if the applicant waits more than one month before applying for an injunction after becoming aware of an infringement of the law:

"A publisher who has knowledge that works protected by copyright, including works of which it holds the rights, are being made available illegally to the public on an Internet portal, and who lacks any prospect of success in taking action against the portal operator and/or its host provider, is acting in a manner detrimental to urgency if it does not apply for an injunction against the access provider within one month of obtaining this knowledge. The period of urgency does not begin anew with the knowledge of the infringement of the rights with regard to each new work made publicly accessible."

The assumption of urgency may be precluded by conduct on the part of the applicant from which it can be inferred that he himself does not regard the matter as urgent. According to the established case law of the senates of the Munich Higher Regional Court responsible for the fields of intellectual property and copyright law, urgency can no longer be assumed if an applicant waits longer than one month from the time he becomes aware of the infringing act and the person of the infringer before applying for a preliminary injunction (OLG München, judgment of 02.02.2019 - 29 U 3889/18).

The one-month period expired - even taking into account the official release - which is why there was no longer any urgency at the time the application was submitted.

Due to the applicant's place of business, Munich would be a justified place of jurisdiction. The Munich Regional Court, which has local jurisdiction, would have denied the grounds for the injunction in accordance with the opinion of the Munich Higher Regional Court. Accordingly, the local court location of Hamburg was chosen by the applicant with the intention of deliberately disadvantaging the defendant.

2. inadmissible application

2.1 Undetermined application

The application is not sufficiently specific within the meaning of Section 253 (2) no. 2 of the German Code of Civil Procedure.

Pursuant to Section 253 (2) no. 2 of the German Civil Procedural Code, an application for a prohibition may not be worded so vaguely that the subject matter and scope of the court's decision-making power (Section 308 (1) sentence 1 of the German Civil Procedural Code) are not recognizably delimited, the defendant therefore being unable to defend itself exhaustively and ultimately leaving the decision as to what the defendant is prohibited from doing to the court enforcing the judgment. The use of general terms in the application for an injunction to designate the act to be prohibited "making available to the public" is not sufficient if the contribution of which the defendant is accused is not apparent. The defendant is accused in the justification of the application of an act of support for making available to the public. In the motion of the application, however, the defendant is claimed to be the perpetrator. The application for an injunction therefore does not refer to a "Stoererhaftung" (interferer liability), it refers to an act of the defendant by providing hyperlinks. The parties will agree that the defendant does not set hyperlinks. The fact that the applicant assumes interferer liability on page 12 of the application does not relativize an incorrect version of the motion. On the contrary, this cannot be used for interpretation, since the justification for the application contradicts the motion. The court is also of the opinion that the motion does not sufficiently set out the conduct to be refrained from, since the "correction of the application" by the court shows that the motion of the applicant is undefined. The applicant's "clarification" of the motion after the court's indication is also not sufficiently specific.

2.2 Inadmissible amendment of the motion

Furthermore, the "correction of the motion" by the court is to be regarded as an amendment of the motion which exceeds the scope of a permissible correction of the motion. The concretization made by the court in the application, which describes the actual action, only reveals which action to be omitted is demanded from the respondent.

B. Unfoundedness

The application for a preliminary injunction is unfounded.

1. No claim

The applicant is not entitled to any claim against the respondent.

1.1 No right of the applicant to bring an action

The applicant does not have the right to sue.

In the event of an infringement of copyrights and neighboring rights, the author or the holder of an exclusive right alone has the right to take action. Pursuant to Sections 2 (1), 7 German Copyright Act, copyright protection is originally vested in the person who personally produces

the work. Pursuant to Sections 97 et seq. German Copyright Act, the owner of an exclusive right of use to the respective work is also entitled to assert claims. If rights have been granted to another person as the rightful user, the extent to which these rights have been transferred is decisive for the right to sue. In this context, the right to bring an action extends as far as the exclusive rights of use in terms of space, subject matter and time (Dreier/Schulze/Specht German Copyright Act 5th ed., Section 97 no. 19).

The applicant's submission that a copy of the back cover of the CD " REDACTED on which the applicant is identified by the P-notice as the exclusive owner of the rights of the phonogram producer, is not sufficient for the presumption under Sections 85 (4), 10 (1) German Copyright Act. The reason is that even according to the provisions of Art. 11 of the Rome Convention on the affixing of the P-notice, it is not ensured that the company named in the P-notice is actually the owner of the phonogram producer right.

1.2 Liability privilege pursuant to Sections 8 (1), 9 of the German Telemedia Act (German Telemedia Services Act)

Contrary to the opinion of the court, the respondent can invoke a liability privilege for service providers pursuant to Sections 8 (1), 9 German Telemedia Services Act, at least in analogous application. A liability of the respondent for injunctive relief is excluded according to §§ 8 para. 1 sentence 2, 9 in conjunction with §§ 8 para. 1 sentence 2, 9 in conjunction with § 8 para. 1 sentence 2 German Telemedia Services Act. Section 8 (1) sentence 2 German Telemedia Services Act.

1.2.1 Applicability of the German Telemedia Services Act

The exclusions of liability pursuant to §§ 7 et seq. German Telemedia Services Act are applicable in the present case. The defendant is a service provider within the meaning of § 2 No. 1 German Telemedia Services Act. Accordingly, a service provider is any natural person or legal entity that provides its own or third-party telemedia for use or provides access for use. The term "service provider" in the German Telemedia Services Act is based on the E-Commerce Directive (Directive 2000/31/EC) and is to be interpreted uniformly as an autonomous term under EU law. In Art. 2 lit. b of the E-Commerce Directive, "service provider" is defined as any natural or legal person offering an information society service. The term "information society service" is also an autonomous concept of Union law, which is legally defined in Art. 1(1)(b) of Directive (EU) 2015/1535 as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient". This applies to the service provided by the respondent. The respondent provides a service at the individual request of its users, which consists of resolving the domain into a numerical IP address and transmitting it. The fact that the respondent provides this service free of charge is irrelevant. For one thing, the fact that the respective users pay a fee is not decisive for the consideration. It is sufficient if the service is financed otherwise, for example through advertising or, as in the present case, through donations (ECJ, judgment of September 15, 2016, Case C-484/14 - *McFadden,* paras. 41, 43). Secondly, the legal definition of Directive (EU) 2015/1535 is based on the fact that the services are "normally" provided for remuneration.

This applies to the operation of a DNS resolver, the operation of which is regularly provided for remuneration. As explained above, a large number of Internet users use the preset DNS resolver of their Internet service provider, which offers this service as part of its contractually owed service and business model compensated by corresponding contract rates.

In Annex 1, Directive (EU) 2015/1535 also lists an example of services that do *not* fall under this definition. DNS services are not mentioned in Annex 1.

This result is consistent with the case law of the Federal Court of Justice on the interpretation of the term "service provider" in the Telemedia Services Act. According to the case law of the Federal Court of Justice, the term "service provider" must be interpreted functionally. The service provider must enable the dissemination or storage of information through its instructions or control over computers and communication channels and must appear to third parties as a provider of services (BGH, judgment of October 15, 2020 - I ZR 13/19, marginal no. 16 with reference to Spindler in Spindler/Schmitz, German Telemedia Services Act, 2nd ed. § 2 marginal no. 28). This applies to the respondent. The respondent operates computers under its control and disseminates information by passing on DNS queries. For its users who use the respondent's service, the respondent acts as a provider of services to the outside.

Unlike the registrar, which the Federal Court of Justice did not classify as a service provider within the meaning of Section 2 No. 1 of the German Telemedia Act (German Telemedia Services Act) because it merely carried out the administrative processing of the domain registration, the defendant's interferer liability in the present case is linked to a contribution that is made in each case during the relaying of the retrieval of the disputed domain (Federal Court of Justice, judgment of October 15, 2020 - I ZR 13/19, para. 16). The respondent, unlike the registrar, is therefore itself involved in the technical provision of access (BGH, judgment of October 15, 2020 - I ZR 13/19, marginal no. 17). The automated resolution of domain names into IP addresses is required for each retrieval of the domain. After the one-time connection of the domain, the registrar is no longer involved in subsequent retrievals.

1.2.2 Defendant has privileged liability pursuant to Section 8 (1) of the German Telemedia Act (German Telemedia Services Act)

The applicant may invoke the liability privilege pursuant to Section 8 (1) sentence 1 German Telemedia Services Act. Pursuant to Section 8 (1) sentence 1 of the German Telemedia Act (German Telemedia Services Act), service providers are not responsible for third-party information that they transmit in a communications network or to which they provide access, subject to the conditions set out in sections 1 –3, and may not be held liable for damages or injunctive relief pursuant to Section 8 (1) sentence 2 of the German Telemedia Services Act.

The service of the respondent fulfills the requirements of Section 8 (1) sentence 1 2nd alt German Telemedia Services Act, as it provides its users with access to third-party information. As an independent DNS resolver, the respondent provides a service that gives its users access to the services available under the domains queried in each case. Only when the respondent's

service transmits the answers determined in this way to the user's browser by querying the IP addresses do the users gain access to the respective websites.

The assessment of whether the liability privilege pursuant to Section 8 (1) sentence 1 2nd alt. German Telemedia Services Act is relevant, the concrete retrieval path must be taken into account. In its legal assessment of the respondent's contribution, the court focuses on the retrievability of illegal content via the specific retrieval path using the respondent's DNS resolver. For this retrieval path, the resolution of the domain names into IP addresses constitutes a provision of access. This is because if the specific DNS settings were retained and the DNS resolver of the respondent were used, it would not be possible to access the respective websites under the domain names entered in the browser.

This is also consistent with the findings of the court, which describes the respondent's business model as "giving access to the Internet". The court correctly states that the information published on the REDACTED website would only be accessible to the respondent's users by means of the resolution of IP address into domain names provided by the respondent. Without the resolution of the domain name into the IP address, the respondent's users are denied access to websites, as the court further states. Even according to these findings, the respondent's service consists of providing access to information. It is not shown or evident that the term "provision of access" within the meaning of Section 8 (1) sentence 1 2nd alternative of the German Telemedia Services Act must be understood narrowly in the sense that it only covers the direct opening of access to certain information. The term "providing access" already expresses linguistically that also such contributions, which do not open the access directly, but make possible by providing access, are to be privileged. If, as in the present case, a chain of service providers is used to provide access to information, in which each service provider automatically provides access to the next service provider, all service providers in this chain are privileged pursuant to Section 8 of the German Telemedia Services Act (MüKo StGB, 3rd ed. 2019, Vorbem. Zu § 7 German Telemedia Services Act Rn. 49).

The case law on the responsibility of the registry of the top-level domain .de, DENIC eG, is also based on a broad concept of mediation:

> *"The name server service provided by the plaintiff ensures the assignment of domain names to the associated IP addresses of the computer from which the content accessed by the user by entering the domain name is to be retrieved. [...] It thus (in the broader sense) provides access to information held on servers by third parties."* (VG Düsseldorf, judgment of 29.11.2011 - 27 K 458/10).

The meaning and purpose of the exclusion of liability pursuant to Article 12 of the E-Commerce Directive and Section 8 (1) of the German Telemedia Act (German Telemedia Services Act) require the application of the exclusion of liability to the service of the respondent. According to recital 42 of the E-Commerce Directive, the exclusion of liability for mere conduit serves to protect service providers who merely provide a technical infrastructure but have no control over the information they transmit or to which they provide access. This is intended to ensure that service providers whose services are in principle desirable and technologically neutral are

not threatened by excessive liability risks. These teleological considerations apply to DNS resolvers whose business model consists of providing a technical service central to the functioning of the Internet and who have no control over the information to which they provide access. Accordingly, DNS service providers - and explicitly alongside top-level domain registries - are included as operators of essential services in Art. 4 No. 4 in conjunction with. Annex 2 of the NIS Directive (Directive (EU) 2016/1148). From a systematic point of view, it would also be contradictory if services such as DNS resolvers could not benefit from the exclusion of liability under Section 8 (1) of the German Telemedia Services Act and were liable under more stringent conditions than, for example, access providers, who are indisputably covered by the exclusion of liability under Section 8 (1) of the German Telemedia Services Act. DNS resolvers are more distant from the infringing information than access providers, since they do not even transmit the information.

As already explained, access providers also regularly operate recursive DNS resolvers. If one did not want to include the logically mandatory upstream step of the DNS query in the technical facts of the provider of a telemedia service, this would render the privileges, which are largely motivated by criteria of reasonableness, worthless, since the providers would then be exposed to liability risks not in their capacity as access providers, but in their capacity as providers of a recursive DNS resolver.

This result is supported by the European Commission's draft regulation on a single market for digital services (Digital Services Act - DSA) and amending Directive 2000/31/EC. The European legislator transfers the liability privileges of the E-Commerce Directive into the DSA with the same wording. Recital 27 of the draft DSA clarifies that DNS services can make use of the liability privileges:

> "*Since 2000, new technologies have been developed to provide better availability, effectiveness, speed, reliability, capacity and security of systems for the transmission and storage of data on the Internet, resulting in an increasingly complex online ecosystem. In this regard, it should be recalled that providers of* ***services to provide and facilitate the underlying logical architecture and smooth functioning of the Internet, including auxiliary technical functions,*** *may also benefit from the disclaimers set out in this Regulation, provided that their services are classified as "mere transit", "caching" or "hosting".* ***Such services*** *may* ***include*** *wireless local area networks (WLANs****), DNS services****, the services of top-level domain name registries and certification authorities issuing digital certificates, or content delivery networks that provide or enhance functions of other switching service providers. Services for communications purposes and the technical means for providing them have also evolved significantly, leading to the emergence of online services such as Internet voice telephony (VoIP), messaging services, and Web-based e-mail services, where communications are enabled through an Internet access service. These services are also eligible for disclaimers if they are classified as "pass-through only," "caching," or "hosting.* " (emphasis of the undersigned).

This proposal clarifies that all services, including auxiliary technical functions for the logical architecture of the Internet, including explicitly DNS services, can in principle benefit from a liability privilege. The wording "should be recalled" and the retention of the wording of the E-Commerce Directive make it clear that the European legislator merely clarifies in recital 27 that DNS service providers also fall under the exclusion of liability for mere conduit under the current legal situation. According to recital 27, the privileged service providers also include those who offer auxiliary technical functions. The accompanying legislative materials to the draft DSA also make it clear that the term "DNS services" also includes recursive DNS resolvers. In its Inception Impact Assessment for the DSA, the European Commission refers to its report on the "Legal analysis of the intermediary service providers of non-hosting nature" (available at: https://op.europa.eu/de/publication-detail/-/publication/3931eed8-3e88-11eb-b27b-01aa75ed71a1/language-en/format-PDF/source-179885922), in which recursive DNS resolvers are explicitly mentioned as part of DNS services (p. 46).

The respondent's service also meets the other requirements of Section 8 (1) sentence 1 nos. 1 - 3 German Telemedia Services Act, namely that it does not initiate the transmission, does not select the addressee of the transmitted information and does not select or modify the transmitted information. Contrary to the view of the applicant, the privilege under Section 8 (1) of the German Telemedia Services Act also does not cease to apply because the respondent uses filter lists (Application, p. 17). The ECJ has ruled that the use of voluntary measures to combat infringements by service providers may not lead to the loss of the liability privileges of the E-Commerce Directive (ECJ, judgment of 22.6.2021, C-682/18 and C-683/18 - Youtube/Cyando, para. 109). The ECJ has clarified with regard to the hosting provider privilege pursuant to Art. 14 E-Commerce Directive that the voluntary application of technical measures by the service provider to combat infringements does not result in the service provider playing an "active role" because it would otherwise be excluded from the liability privilege pursuant to Art. 14 E-Commerce Directive (ECJ loc. cit.). Accordingly, voluntary technical measures to combat infringements by service providers pursuant to Section 8 of the German Telemedia Services Act may not lead to the loss of the liability privilege.

1.2.3 Applicability of § 9 German Telemedia Services Act to caching

Insofar as the respondent caches results of recursive name resolution, it is privileged from liability pursuant to Section 9 German Telemedia Services Act. The DNS caching described above represents an automatic, temporary caching that serves the sole purpose of making the transmission of third-party queries to other requesters more efficient. The respondent does not store any content, but rather the DNS query results on the name server operator’s instructions.

Contrary to the opinion of the applicant, the liability privilege according to § 9 German Telemedia Services Act is also applicable to the service of the respondent. The respondent has neither knowledge nor control over the "information" stored with it. The fact that the respondent uses the implementation of security lists to filter malware from the DNS query does not mean that it actively influences the cached DNS query results. The respondent stores in the cache the resolution of a DNS query that is frequently made and therefore its behavior in storing it is technical, automatic and passive.

Pursuant to Section 9 Sentence 1 No. 5 German Telemedia Services Act, service providers are not responsible for third-party information that they store for a user, provided that they act promptly to remove stored information within the meaning of this provision or to block access to it as soon as they become aware that the information has been removed from the network at the original point of origin of the transmission or that access to it has been blocked or that a court or administrative authority has ordered its removal or blocking. None of these conditions are met.

1.3 No Interferer Liability of the Respondent

If, notwithstanding the above, the court should assume that the defendant is liable, there is nevertheless no interferer liability.

1.3.1 No Adequate-Causal Contribution of the Respondent to the Alleged Copyright Infringement

The provision of the respondent's service does not constitute an adequate-causal contribution to the copyright infringement alleged by the applicant. In the present case, the making available to the public has been completed without any contribution by the defendant. The applicant submits that the music album in question is made publicly accessible by providing hyperlinks to another website under the disputed domain for downloading. The operation of the DNS resolver of the defendant is not causal for this copyright infringement. This is because the making available to the public occurs through the setting of hyperlinks on the disputed website, or by making content available for download on the third-party website. The act of making available to the public pursuant to Section 19a German Copyright Act is fulfilled at the moment when the subject matter of the protection is made available for download on a website on the Internet. The relevant act is the making available of protected content, which in Internet cases is completed, among other things, as soon as the content can be retrieved from a website. The actual retrieval of the work is irrelevant (Wandtke/Bullinger, Urheberrecht, 5th ed. 2019, § 19a marginal no. 10).

The act of making available to the public is thus already completed at the moment the subject matter of protection is published on the website, irrespective of actual retrievals. The sound recordings in dispute became retrievable at the moment the hyperlinks were published or made available for download, regardless of the use of the DNS resolver of the defendant. Internet users can access the website via numerous DNS resolvers other than that of the defendant, for example via that of its Internet service provider or other providers. The "concrete form of commission" (application p. 13) is not the retrieval of the sound recordings, but their provision. For the realization of making available to the public, it is not necessary that a specific DNS resolver be used to resolve the domain name.

Nor is the retrievability without the use of the respondent's service an irrelevant hypothetical causal event. First, the contribution of the defendant is not the event giving rise to liability. This lies in the making available on the objected website and occurs without a contribution by the respondent. The making available to the public would be committed, even if the DNS resolver

of the defendant would not exist. Secondly, even if one focuses on the specific retrieval, not every hypothetical causal course is irrelevant. In the decision on which it relies in the judgment on the *registrar's interferer liability,* the Federal Court of Justice makes it clear that the relevance of hypothetical causal sequences is a question of individual assessment that is answered differently in different constellations:

> "Whether the reserve cause is relevant and leads to an exoneration of the tortfeasor is a question of evaluation, which is answered quite differently for different groups of cases (see BGHZ 29, 207, 215; Staudinger/Medicus, BGB 12th ed. § 249 Rdnr. 99ff; Larenz, Schuldrecht I 13th ed. § 30 I in each case m.w.N.). The realization that an only hypothetically effective reserve cause cannot eliminate the causality of a cause that has become effective in reality is not limited to the law of damages" (BGH, judgment of 07.06. 1988, IX ZR 144/87, juris marginal no. 12).

However, the contribution of the respondent is not comparable to that of the registrar. Unlike the registrar, who makes the accessibility of the website under the domain name possible in the first place through the connection (BGH, GRUR 2021, 63 para. 19 - Störerhaftung des Registrars), the website is accessible under the domain name using any DNS resolver. Unlike the use of a DNS resolver, the registrar's contribution is not arbitrarily interchangeable and thus plays a central role in making the website accessible.

Finally, contrary to the applicant's opinion, no adequate causal contribution by the respondent can be derived from the case law of the Federal Supreme Court on the interferer liability of access providers. The applicant only incompletely reproduces the decision of the Federal Court of Justice on the interferer liability of the access provider. In paragraph 25 of the decision on the "Stoererhaftung *des Access Providers" (interferer liability), referred to by the* applicant, the Federal Court of Justice stated:

> By procuring the access, the defendant, according to the correct assessment of the Court of Appeal, made an adequate causal contribution to the copyright infringement found by the Court of Appeal. According to recital 59 of Directive 2001/29/EC, the term "intermediary" used in the Directive refers to any person who transmits a third party's infringement of a protected work on a network. Infringement in this sense includes making an object of protection available to the public (ECJ, GRUR 2014, 468 para. 31 - UPC Telekabel). Since the provider of Internet access services, by granting network access, makes possible the transmission of such an infringement on the Internet between its customer and a third party, the service provider is necessarily involved in any transmission, so that its access services are used to infringe copyright within the meaning of Art. 8 III RL 2001/29/EC (cf. ECJ, GRUR 2014, 468 Rn. 32, 40 - UPC Telekabel)." (BGH GRUR 2016, 268 marginal no. 25 - Access Provider's Breach of Duty of Care).

The BGH thus clarifies that the contribution of the access provider was adequate-causal because the access provider is necessarily involved in the transmission of illegal content in its network. This is not the case with the service of the defendant. The respondent is not, a fortiori

not necessarily, involved in the transmission of unlawful information. The making available to the public through the setting of hyperlinks is completed independently of the use of the service of the respondent (see above). The applicant also does not transfer the sound recordings thus made publicly accessible to third parties. Its service merely consists of answering the DNS queries.

Finally, it is contradictory for the applicant to state, on the one hand, that the contribution of the respondent - like that of an access provider - consists in the fact that it provides access to a network that enables transmission and, on the other hand, to deny the respondent the liability privilege under Section 8 (1) sentence 2 of the German Telemedia Act (German Telemedia Services Act), which is linked to that very act.

1.3.2 No violation of reasonable monitoring obligations

The defendant does not meet the requirements of interferer liability, as it has not breached any reasonable duties of care. According to the case law of the Federal Court of Justice, interferer liability for content on the Internet that is claimed to be infringing is subject to different requirements depending on the function and activity of the defendant (BGH, judgment of October 15, 2020, I ZR 13/19, marginal no. 21). Since interferer liability cannot be extended unduly to third parties who have not themselves carried out the unlawful interference, the liability of the interferer requires a violation of obligations of conduct. The extent of these obligations is determined by whether and to what extent the party held liable as a "Stoerer" can reasonably be expected to carry out an inspection (BGH, loc.cit., marginal no. 13).

In principle, the defendant is not subject to any testing and monitoring obligations with regard to the information to which it provides access. According to the case law of the Federal Court of Justice (BGH), testing and monitoring obligations for the operators of technically neutral Internet services regularly only arise after a reference to a specific infringement (in summary for registries, Admin-C, host providers, access providers and registrars: BGH, loc. cit., para. 22 ff.). The substantiation and specificity of the notice of an infringement is again subject to graduated requirements, which depend, among other things, on whether the activity of the respective service provider is in the general interest, whether it is provided with the intention of making a profit, whether it is connected with the storage of the illegal information, whether the efficient performance of the tasks is impaired by the legal examination of the notice and whether there are parties closer to the infringement (BGH, loc. cit., paras. 22 et seq., 29). In the case of DENIC eG, the Federal Court of Justice ruled that even if DENIC had been notified of an infringement, it had only a limited duty to carry out investigations. Only in the case of infringements that are easily recognizable, either because they have been proven by a legally binding title or because the infringement is so clear that it must be obvious without any investigation, does DENIC have concrete duties of care. According to the case law of the Federal Court of Justice (BGH), DENIC's obligations are limited to these particularly substantiated notices, because it performs a task in the general interest free of charge (BGH, loc. cit., para. 22). In contrast, the registrar's liability is subject to less stringent requirements, since the registrar performs a task in the public interest by handling the domain registration, but does so with the intention of making a profit. Therefore, in the case of the registrar, the

reference to a clear and readily ascertainable infringement is sufficient to trigger verification obligations (BGH, loc. cit. para. 28 - 30.). In any case, the notice must contain all requirements for the claim (BGH, loc. cit. para. 35). According to the case law of the Federal Court of Justice, the requirements for the notice in the case of a registrar and a non-commercial registry differ with regard to the requirements for the recognizability of the recognizability of the infringement. For the commercially acting registrar, the infringement must be clearly and readily ascertainable, whereas for the non-commercial registry the standard is stricter to such an extent that the infringement must either be apparent from a legally binding title or be obvious.

No less stringent standard can apply to the respondent than to DENIC eG. The respondent participates in a task in the general interest, since it contributes to the smooth flow of DNS queries. It provides this service free of charge and offers its users protection against malicious software while complying with applicable data protection regulations and safeguarding the users' privacy. Just like DENIC eG, the respondent provides a purely technical task that is neutral in terms of content. More stringent requirements must be applied to the respondent's duties of care compared to DENIC eG, also because DENIC eG "only" has domains ending in ".de" in its administration, whereas the respondent processes DNS queries for thousands of Top Level Domains and hundreds of millions of domains may be affected.

A duty of care on the part of the respondent can only arise from references based on a legally binding title or in the case of infringements where the nature of the asserted infringement is evident from the content itself. As with regard to the filter lists used by the respondent, an obvious, imposing infringement can be assumed in this context if it concerns generally, globally undesirable infringements that are intrinsic to the content. The blocking lists concern malware, viruses, botnets, phishing sites, stalkerware and other types of content that are globally illegal. There is no room for interpretation here. In contrast, infringements that depend on alleged rights holder representations, lack of licensing or similar circumstances, which are subject to the private autonomy and contractual arrangements of the respective parties, are not apparent to the respondent and cannot reasonably be checked to determine whether the alleged infringer may be authorized after all.

To the extent that the measure requested by the applicant results in a domain no longer being accessible worldwide, the notice would have to enable the respondent to determine the requirements for blocking information in all affected jurisdictions. Otherwise, the respondent would be forced to carry out such a time-consuming legal examination, which would make it impossible for it to perform its duties. In addition, there is the need to vet the identity of the respective claimants in order to avoid blocking requests from unauthorized parties.

Even if one applies the standard developed by the Federal Court of Justice for DENIC eG and assumes that the defendant has a duty of care on the condition that it receives a notice that enables it to ascertain an infringement without further investigation, for example by means of a legally binding title or because the illegality is recognizable from the content itself, a breach of the duty of care cannot be considered in the present case.

1.3.2.1 No Receipt of the Notice of Alleged Infringement of Rights

The respondent was not made aware of the circumstances by the applicant because the applicant's agent did not properly send either the letter of advice or the warning letters to the respondent. Receipt, for which the applicant has the burden of presentation and proof, does not exist. In the case of dispatch by e-mail, the applicant bears the burden of proof for the proper receipt of both the letter of notice and a warning letter. The risk of actual receipt in the respondent's mailbox is borne by the applicant. If an e-mail is already sorted out by the server's spam filter, this risk is borne by the sender (Wandtke/Bullinger, Urheberrecht, 5th ed. 2019, § 97a marginal no. 27). If the e-mail is received in the local spam folder, the recipient has no obligation to open attachments, as this may give rise to the suspicion that the attachments have been infected by a virus (Wandtke/Bullinger, loc. cit.).

The attachments in pdf format attached to the e-mail of 26.03.2021 were not opened by the respondent, as it is customary and recommended not to open attachments of mails from unknown senders for security reasons (see 2.7.2.1 above).

The information in the footer does not lead to the impression that the respondent was not dealing with spam. Contrary to the BSI's recommendation (see above), the mail contained a very short text without a formal salutation or information about the content of the attachments.

The overall impression of the e-mail was thus in contradiction to an e-mail in legal matters, which can be expected in the case of a warning letter.

Since the applicant has both out-of-court and in-court experience with such proceedings, it is also reasonable to expect it to address an abuse report to the relevant e-mail address. The respondent cannot be expected, nor can it be demanded, to inspect every incoming e-mail without the use of technical aids to contain spam and e-mails with malicious code. A fortiori, the respondent does not have to take this risk with a support e-mail address the purpose of which is to answer questions about the system.

According to the applicant's submission, the warning letter sent by ordinary mail was also not received by the respondent. If the applicant uses the postal service to transport the warning letter, the postal service acts as the applicant's agent in this respect, so that in such a case the applicant is responsible for a fault of the postal service pursuant to Section 278 sentence 1 of the German Civil Code (Bürgerliches Gesetzbuch - BGB) if mail is lost in transit (see BGH, judgment dated January 21, 2009 - VIII ZR 107/08).

Furthermore, it is questionable why the notice was only sent by e-mail and the warning letter by letter post. If the applicant had wanted to ensure that the letters were received, it could have sent a registered letter or an e-mail with read confirmation. The applicant must accept responsibility for the uncertainties thus created, as they fall within its sphere of risk.

The respondent first became aware of the asserted infringement through the court order. It responded within a reasonable period of time, without acknowledging any legal obligation, by blocking the domain.

1.3.2.2 No sufficiently substantiated notice

Assuming that the respondent had received the letter of notification or the warning letter, they would not contain a sufficiently substantiated reference to an infringement of rights that would have enabled the respondent to establish beyond doubt, without having to conduct investigations, that the blocking of the entire REDACTED domain would be legally permissible and required due to the infringement of rights asserted by the applicant. A notice that can trigger the defendant's duty of care must contain all information that enables the defendant to understand the legality of the blocking request without further investigation and beyond doubt. It is therefore not sufficient for the applicant to make a plausible case for an individual infringement; it must set out the requirements for the asserted blocking of the entire domain.

This includes, in particular, references to the fact that the domain in question contains predominantly infringing content and that the right holder has unsuccessfully taken action against parties closer to the infringement (BGH, judgment of October 15, 2020, I ZR 13/19, marginal no. 35). According to the case law of the Federal Court of Justice (BGH), a DNS block can only come into consideration if lawful content is not significant in relation to the unlawful content on the respective website (BGH loc. cit.). In addition, a blocking obligation can only be considered if the rights holder has previously taken unsuccessful action against parties closer to the infringement, including reasonable measures to uncover the identity of the operator of the website by involving state investigative authorities or private investigators (BGH GRUR 2016, 268, 275, marginal no. 87 - Stoererhaftung des Access Providers).

The information contained in the notification and warning letter (Annexes AST 4 and AST 6) does not meet these requirements. The notification letter does not contain any information about the unsuccessful action of the applicant against parties closer to the infringement. It cannot contain this information, as the applicant, according to the notification letter, contacted the operators of the disputed domain and its host provider for the first time at the same time as the notification letter was sent on March 23, 2021.

Furthermore, the applicant has not sufficiently substantiated the overall proportion between lawful and infringing contents of the disputed domain. Neither has it submitted a judicial title nor a comparable reference from which the respondent should have been aware of the illegality of the information without having to make inquiries. Neither the recommendation of the examination board nor the expert opinion (Annex AST 2 and AST 16) were properly attached to the letters. On the basis of this, the respondent cannot satisfy itself with the necessary certainty of the legality of the blocking request. The respondent would not have been able to comprehend whether the results of this examination were correct or whether it had been carried out at all.

The expert opinion (Annex AST 6) and the recommendation of the Examination Committee (Annex AST 16) also fail to satisfy the substantiation requirements. Neither the expert opinion nor the recommendation of the Examination Committee are documents that originate from a state-recognized body whose assessment can be equated with a judgment or an official order. The expert opinion fails to take into account the fact that the website in question contains links

as well as a discussion forum, which contains a large amount of lawful content. It is therefore questionable whether the very small sample of 80 items of content can be meaningful at all in view of the large number of items of content available. The recommendation of the Examination Committee cannot be comprehended by the respondent because the statistical analysis report to which the recommendation refers is not attached to the recommendation. Furthermore, the recommendation does not state how far and why the examination committee follows the methodology of the statistical analysis report.

Finally, the applicant has not provided any sufficiently substantiated information in the warning letter about unsuccessful actions against other parties. In any case, irrespective of the other deficits addressed below, the applicant does not show that it has taken the reasonable measures required by the case law of the Federal Court of Justice to determine the identity of the website operators. In particular, it does not show that it has initiated state or private investigations. Thus, even if the respondent had entered into a legal examination, it would not have been able to establish with the requisite certainty that the subsidiarity was ensured.

1.3.3 Recourse to the defendant excluded due to subsidiarity

In the present case, recourse against the defendant is excluded under the aspect of subsidiarity. The applicant has not substantiated that it has made all reasonable efforts to take action against the perpetrator of the infringement or other parties involved who are closer to the perpetrator.

Interferer liability is generally not subsidiary to perpetrator liability, provided that interferer liability offers more effective legal protection because it is not necessary to take action against a large number of infringers (BGH GRUR 2007, 724 para. 13). This is not the case here. In order to stop the making available of the sound recordings in dispute, the applicant would only have had to take action against one of the parties closer to the infringement in order to stop the infringement.

According to the case law of the Federal Court of Justice, the access provider's interferer liability is therefore subsidiary to the recourse against parties closer to the offence for reasons of proportionality:

> "With regard to the fact that the access provider pursues a business model that is approved by the legal system and is neutral with regard to infringements of the rights of third parties, it is reasonable in the context of the examination of the reasonableness of monitoring and blocking measures to demand priority legal action against those parties who – like the operators of objectionable websites – either committed the infringement themselves or contributed to the infringement – like the host provider of the objectionable websites – by providing services. In contrast, the assertion of claims against the access provider can only be considered from the point of view of proportionality if the claim against the operator of the website lacks any prospect of success and would therefore otherwise create a gap in legal protection. This result is also supported by the fact that the operator of the website and its host provider are

> much closer to the infringement than the person who only generally provides access to the Internet." (BGH, GRUR 2016, 268 marginal no. 83 - Breach of Duty of Care of the Access Provider).

Accordingly, the Federal Court of Justice ruled that the registrar could also only be held liable as an interferer, in other words, that interferer liability was ultima ratio:

> "In weighing the fundamental rights involved (see recital 26), account must be taken of the risk that this will result in a disproportionate burden on the registrar and thus jeopardize his business model by accepting his merely subsidiary liability, which only arises when the rightsholder has unsuccessfully taken action against those parties who - like the operator of the Internet site - have themselves committed the infringement or - like the host provider - have contributed to the infringement by providing services, unless such action lacks any prospect of success. The registrar's liability, like that of the Internet access provider, is ultima ratio if copyright protection cannot be effectively ensured by other means (cf. BGHZ 208, 82 marginal no. 83 - Stoererhaftung des Accessproviders)." (BGH, judgment of October 15, 2020, I ZR 13/19, marginal no. 31 - Stoererhaftung des Registrars).

These liability principles are to be applied to the DNS resolver. By providing access to the Internet, the defendant also operates a business model that is approved by the legal system and is neutral with regard to third-party copyright infringements. Like the access provider, the respondent also has no contractual relationships with parties closer to the infringement, such as the operator of the disputed website or its host provider.

The applicant has not demonstrated that it has taken reasonable measures to take recourse against the parties closer to the offence.

1.3.3.1 Applicant has not exhausted reasonable measures to determine the identity of the website operator

The applicant has not taken all reasonable measures to determine the identity of the operators of the website in question. According to the case law of the German Federal Court of Justice (BGH), the rightsholder can be expected to involve state investigative authorities or to conduct private investigations in this context. The mere fact that the identity of the website operator cannot be inferred from the website does not release the rights holder from taking further measures (BGH, GRUR 2016, 268 marginal no. 87 - Störerhaftung des Access Providers). The applicant has not met these requirements. In particular, it has not shown that it has called in state investigating authorities or commissioned private investigations. The applicant submits that the website in question has no imprint, that there is no public Whois entry, and that the operators did not respond to a message to the administrator of the website's forum. The fact that the identity of the operators could not be determined via the website is not sufficient according to the aforementioned decision of the BGH. The absence of a Whois entry does not exempt the operator from taking further measures. The domain on which the BGH's decision on the access provider's interferer liability is based, goldesel.to, and the domain in question in

the present case share the top-level domain .to. The Federal Court of Justice therefore considered it reasonable to take further measures, even if the corresponding top-level domain does not have a public Whois directory.

The applicant is also not exempt from the reasonable initiation of state or private investigations because they contacted the advertising provider "REDACTED" or the payment service provider REDACTED by e-mail. The BGH explicitly mentions the investigative approach via payment service providers as an independent measure in addition to the initiation of investigations (BGH loc. cit.).

Moreover, the requests for information which the applicant has addressed to the above-mentioned service providers do not constitute a suitable attempt to establish the identity of the operators of the offending website. The applicant has not explained by which means of communication it attempted to deliver the letters (Annexes AST 8 and AST 9). In this respect, it is disputed that the letters were received by the respective services. In addition, the wording in the solicitor's letters is not sufficiently clear and in part contradictory. Both letters refer to the fact that the services have a business relationship with the REDACTED website. However, only URLs under another domain, REDACTED, are cited as evidence of the infringement of the applicant's rights. The applicant does not demonstrate that it has the right to bring an action; not even a written power of attorney was attached to the letters. The full address of the applicant is not stated in the heading of the letters. In this respect alone, it was probably not possible for the services to verify the authenticity of the applicant's request for information.

With the letter to " REDACTED" (Exhibit AST 8), the applicant also requests the service " REDACTED " to stop placing advertisements under the domain REDACTED This is not only in contradiction to the previously listed infringements, which refer to a different domain, this request also clearly goes beyond a request for information. The applicant does not explain on what legal basis it bases alleged claims for injunctive relief or for the provision of information. The REDACTED " service can therefore not understand that it should be obliged to hand over personal data on the basis of this sparse and contradictory information, let alone to terminate contractual relationships that may give rise to corresponding recourse claims. In the letter to " REDACTED ", the applicant also does not set out a legal basis for their request for information. The request for information is related solely to the REDACTED domain. Without further information, however, the payment service provider cannot even assign this claim to a donation account. The applicant should at least have named the account to which the request for information is linked. “REDACTED" can therefore not seriously have assumed an obligation to provide information on the basis of this information letter either.

Both letters also provide for a deadline of three days to fulfill the asserted claims. In addition to the deficiencies in substantiation, contradictions and ambiguities in service already explained, the applicant's representative in the proceedings is asserting the rights of further rights holders in numerous other works with the letters from lawyers. In this regard, the letters are contradictory in further aspects (some albums are stated more than once) and the deadline is also so short that the actual and legal review within this period is factually impossible. After all this, the service providers could not assume to be obliged to provide information.

1.3.3.2 Applicant has not exhausted reasonable measures vis-à-vis the host provider

The applicant has also not taken all reasonable measures to end the infringement by taking action against the host provider of the disputed domain. The applicant's lawyer's letter submitted as Annex AST 10 was also not sufficiently substantiated, so that the host provider also did not have to assume an obligation to delete the allegedly infringing content. Here, too, the applicant has not demonstrated its right to bring an action. The complete address of the applicant is also missing from the heading of their lawyer's letter, as is a written power of attorney. Taken as a whole, the letter does not appear to an objective recipient to be an effective request to terminate a contractual relationship with the operators of the disputed website. In addition to the deficiencies in substantiation, there are again contradictions which call into question the impression of seriousness. The letter does not state any legal basis for the alleged claims. Several albums are listed twice for no apparent reason. The letter also contains translation errors, e.g. the representation of REDACTED formulated in German. Without further information on the part of the applicant, the host provider cannot assume that it is obligated to terminate its service to the operators of the disputed website.

1.3.3.3 No identification of a registrar closer to the offence

Although Tonic offers domain registrations directly to its customers, the applicant would have had to show that the domain was registered without the involvement of a registrar and that a claim against the registrar was therefore out of the question. This is due to the fact that mostly domain registrations are made via registrars and registrars are closer to the infringement. On the one hand, the registrar has a contractual relationship with the domain operator. In the absence of knowledge of the contents of the website they connect, they are not in the camp of the website operator, but they are nevertheless connected to them by a contractual relationship. This is not the case with the respondent, who provides a completely technically neutral service. On the other hand, the registrar acts with the intention of making a profit, so that they can be expected to assume greater obligations than the non-commercially acting respondent. Moreover, the termination of the infringement by the registrar is more effective than the blocking by the DNS resolver of the respondent. The deconnection of the domains in question, which is possible for the registrar, does not require technical measures to be installed and regularly updated in a sensitive infrastructure, but only an administrative step. The deconnection only affects the accessibility via the domain, but eliminates it completely. In this respect, it is more effective than DNS blocking by the respondent, which is ineffective in most cases due to the automated use of alternative DNS resolvers and can be circumvented with the necessary technical knowledge via other DNS resolvers.

Information on the unsuccessful recourse against the registrar or on the lack of a registrar would have been necessary in this respect for an effective notice to the respondent.

1.3.4 Defendant's Interferer Liability Excluded due to Disproportionality

The liability principles developed by the ECJ and the Federal Court of Justice in connection with access providers, which the Federal Court of Justice also applies to the registrar, are to

be applied to DNS resolvers. DNS blocking by the DNS resolver follows the same logic as blocking by the access provider, which the latter also performs by configuring the DNS resolver. The service of the DNS resolver is also technically neutral; unlike the registrar or access provider, the respondent even provides this service free of charge in the present case. According to the case law of the ECJ, when assessing whether court orders against access providers are in compliance with Union law, compatibility with the relevant fundamental rights of the EU Charter of Fundamental Rights (GrCh) must be examined (ECJ, GRUR 2014, 468, para. 45 f. - UPC Telekabel). National law must therefore be applied in compliance with the fundamental rights of the Charter and the principle of proportionality (BGH, GRUR 2016, 268 marginal no. 31 - Störerhaftung des Access Providers).

1.3.4.1 Lack of targeting

The measure ordered by the court is disproportionate as it is not strictly targeted.

1.3.4.1.1 No judicial recourse

The claim against the defendant on the grounds of interferer liability amounts to a disproportionate restriction of the freedom of information of the users concerned, as the users of the defendant have no access to judicial recourse.

According to the case law of the ECJ, the lawfulness of a website blocking order from the perspective of freedom of information requires that the national procedural rules enable Internet users to assert their rights in court after the blocking measures taken by the provider have become known (ECJ, GRUR 2014, 468 Rn. 56 - UPC Telekabel). The Federal Court of Justice (BGH) has repeated this and clarified with regard to website blocking by the access provider that national law must enable the affected Internet users to seek legal protection in court (BGH GRUR 2016, 268 marginal no. 57 - Access Provider's Breach of Duty of Care).

This requirement is not met in the present case. The Internet users affected have no legal recourse against the implementation of the block by the defendant. With regard to DNS blocks by the access provider, the Federal Court of Justice has ruled that this requirement can be met by allowing Internet users to assert their rights against the access provider in court on the basis of the contractual relationship existing between them (BGH loc. cit.).

In the present case, there are no contractual claims that would enable the users of the respondent to have the DNS blocking reviewed by the courts.

1.3.4.1.2 DNS block not appropriate

DNS blocking constitutes a disproportionate interference with the freedom of information of the defendant's users. In this respect, the ECJ and the Federal Court of Justice require that blocking measures be strictly targeted, in that they put an end to copyright infringement without depriving Internet users of the possibility of lawfully accessing information (Federal Court of

Justice GRUR 2016, 268 marginal no. 53 - Stoererhaftung des Access Providers). The DNS block imposed on the defendant does not meet these requirements.

Firstly, the appropriateness of the DNS blocking by the respondent already encounters far-reaching concerns. Measures to prevent unauthorized access to protected objects do not have to completely put an end to the infringement, but they must at least prevent unauthorized access to some extent or make it more difficult for Internet users to access the infringing information (BGH loc. cit. para. 48). DNS blocking by the applicant does not satisfy even these minimum requirements. As described above under I.2.5, a DNS query is answered by an alternative DNS resolver after blocking by the respondent. This means that technical circumvention options are not even necessary, since a recursive resolver other than that of the respondent automatically resolves the domain name on the normal retrieval path via the browser.

Secondly, the blocking is not sufficiently targeted, since it affects all content of the disputed domain beyond the asserted infringement of the sound recordings. With regard to the criterion of targeting from the point of view of "overblocking", i.e. the collateral blocking of lawful information, the BGH has ruled that it depends on the overall ratio of lawful to unlawful content on the blocked website and that it must be taken into account whether the amount of lawful content is insignificant (see, for example, BGH loc. cit. para. 55). The expert opinion submitted by the applicant (Annex AST 2) is not meaningful in this respect. The subject of the expert opinion is not the relationship between lawful and unlawful content within the meaning of the aforementioned case law, but the relationship between protected content and public domain or unknown works (Exhibit AST 2, p. 3). The expert opinion does not answer whether the protected contents are infringements. In addition, as explained above under 1.3.1.2, the expert opinion disregards lawful content such as the contributions to the discussion forum in the sample and its weighting and therefore encounters considerable methodological doubts.

Furthermore, there is a lack of targeting also because the respondent almost arbitrarily selected one of thousands of providers of recursive resolvers operating in Germany alone.

Finally, the service can never implement selective DNS blocks only for users in Germany. The applicant's statement that a worldwide blocking of the domain is legally irrelevant cannot be followed.

Due to the worldwide blocking effect, there is an increased risk that access to information that is lawful in other jurisdictions will be prevented. Irrespective of whether the infringing content accessible via the disputed domain is also illegal in the jurisdictions of the TRIPS member states, the question to be assessed is whether the respective jurisdictions would have permitted judicial recourse against the respondent. Court orders against DNS resolvers have so far remained isolated cases internationally (see Schwemer, Copyright Content Moderation at Non-Content Layers, in: Rosati, Handbook of European Copyright Law (2021), p. 11). Action against DNS resolvers is not possible in other jurisdictions, for example, due to the proportionality and subsidiarity considerations outlined above under other jurisdictions. Even in Switzerland, where the respondent has its registered office, it is highly unlikely that the

present court order could have been issued. The Swiss Federal Supreme Court has ruled that under Swiss law, access providers cannot be held liable for setting up DNS blocks based on copyright infringements for lack of a contribution to the infringement (Federal Supreme Court, ruling of February 4, 2019, 4A_433/2018). This must apply a fortiori to DNS resolvers whose contribution to the infringement is even less than that of the access provider. The worldwide blocking effect can therefore lead to a legal consequence occurring that is not provided for under other legal systems or, as in the case of Switzerland, is expressly excluded. Thus, a court order in one jurisdiction would have the effect of nullifying legal provisions of another jurisdiction. This result cannot be intended outside of international agreements by which the contracting states accept this legal consequence. Blocking orders against infringing websites must therefore be limited territorially to the area for which the infringement is claimed.

The applicant's arguments on the worldwide blocking effect (application, p. 15) do not justify its reasonableness. The applicant first points out that the notice-and-takedown procedure also has a worldwide effect. This is not comparable to the establishment of a DNS block. This is because the notice-and-takedown procedure leads to the targeted removal of a single piece of illegal content, while setting up a DNS block leads to the inaccessibility of an entire domain. These procedures are not legally comparable and are accordingly treated in the legal literature as opposing, not complementary approaches ("delete instead of block," see for example MMR Aktuell, 303415).

Insofar as the applicant relies on the decision of the ECJ in *Glawischnig-Piesczek ./. Facebook Ireland Ltd, it* must be clarified that the ECJ merely ruled that Directive 2000/31/EC does not prevent a court from issuing blocking orders with international effect insofar *as this is permissible under international law* (ECJ, judgment of 03.01.2019, C-18/18 - Glawischnig-Piesczek, para.51). With regard to the extraterritorial effects of injunctions issued by Member State courts, the decision is limited to the terse statement that the E-Commerce Directive does not provide for a territorial limitation of the measures. However, the Member States must ensure that the measures they issue are compatible with international law (loc. cit. para. 52). Accordingly, whether an injunction with extraterritorial effect is permissible under international law must first be determined in each individual case. However, the applicant does not submit any evidence on the admissibility of a worldwide effect of the order under international law.

The fact that the respondent cannot implement the requested blocking limited to the territory of Germany means that this order is disproportionate. The applicant should have turned to the national access providers, which, due to their territorial market limitation and their much larger market shares than the respondent, are in a position to prevent the infringement both more specifically and more effectively.

1.3.4.2 Disproportionate interference with the entrepreneurial freedom of the defendant

The obligation to implement the DNS blocking disproportionately impairs the respondent's right to entrepreneurial freedom pursuant to Art. 16 GrCh and Art. 12 (1) GG. According to the established case law of the Federal Court of Justice, service providers may not be required to take measures that endanger their business model or make their activities disproportionately

difficult (Federal Court of Justice GRUR 2007, 890 = NJW 2008, 758 - Jugendgefährdende Medien bei eBay). Therefore, the administrative, technical and financial effort that the defendant must incur in order to implement the DNS block must also be taken into account when weighing up fundamental rights (BGH GRUR 2016, 268 marginal no. 37 - Access Provider's Breach of Duty of Care).

In the case of the defendant, it must be taken into account that it acts without the intention of making a profit and merely provides an automatic procedure that enables its users to access the disputed domain. Its passively neutral automatic contribution is not comparable to that of a platform operator, such as that on which the BGH decisions on Internet auction houses were based (also OLG Frankfurt a.M., judgment of January 22, 2008 - 6 W 10/08, GRUR-RR 2008, 93, 94 - Access Provider, there on claims under competition law). There, the court based the question of the reasonableness of obligations on the fact that the operators of the platforms and forums themselves had set the sources of risk for infringements, that it was precisely the content that was important to them, and that there were completely different possibilities for better influencing and controlling the content. In contrast, the defendant has not itself created any new source of danger and, as a neutral technical intermediary, has nothing to do with the content to which it provides access and has no influence on it. It thus has a significantly greater distance to the infringing content, which also narrows down the limits of reasonableness (cf. OLG Hamburg, judgment of December 22, 2010 - 5 U 36/09).

It must also be taken into account that the respondent offers its service globally and uniformly. Internet users worldwide can use the respondent's service by configuring the respondent's service with the IP address 9.9.9.9. as DNS resolver in their network settings. This distinguishes the present situation from blocking orders against access providers, which form the basis of the court decisions on the Access Provider's Interferer Liability. The DNS resolvers of the access providers only process requests from their contract customers. Access providers can therefore only implement DNS blocking orders to a limited extent geographically, as they only process queries from the territory of their contractual customers. The respondent's system does not provide for geographical differentiation between users' queries. It can only implement DNS blocking by either setting up, configuring and maintaining it at considerable expense through manual costly configuration or by programming a functionality that does not yet exist so that the system is able to implement blocking commands on a geographical basis. As explained above, the respondent is a non-profit foundation that has not yet received any requests to deploy DNS blocking for copyright infringement. The cost of setting up such a system alone could be stifling to the applicant.

The installation of DNS blocks also leads to considerable losses in the performance of the respondent's DNS resolver. These losses jeopardize the respondent's business model. The quality of a DNS resolver is largely determined by its performance, i.e., how quickly the DNS resolver resolves DNS queries. The quality of DNS resolvers is indicated on various Internet portals on the basis of the resolver's performance, i.e. the speed with which it responds to queries (see for example: https://www.dnsperf.com/#!dns-resolvers; DNS resolvers are not even listed here if they take longer than one second to resolve a query). The implementation of DNS blocking for queries from Internet users from the territory of the Federal Republic of

Germany leads to a noticeable slowdown of the service of the respondent for these users (cf. above I.2.5.). The assignment of requests to a specific IP address and their geographical assignment to the territory of the Federal Republic of Germany involves considerable technical effort, since each request to the respondent's service must be checked to determine whether the requesting IP address can be assigned to the territory of the Federal Republic of Germany and must be answered with appropriate blocking commands. If the performance of the respondent's service falls significantly behind that of other public DNS resolvers, it is to be expected that the inquirers will choose another DNS resolver. It must be taken into account that only those Internet users will use the respondent's service who explicitly choose to do so by changing the default network settings and entering the respondent's DNS resolver instead of the default DNS resolver. These users have the technical understanding and interest in the choice of a particular DNS resolver, so that on the one hand they are able to configure an alternative DNS resolver in the network settings and on the other hand there is a high probability that they will switch to another DNS resolver in the event of a corresponding loss of performance.

Finally, the respondent has neither the budget nor the personnel or technical resources to carry out legal checks on the content objected to. This is all the more true because the service is provided globally. It follows that the respondent, which cannot limit the group of inquirers like other providers of Internet services who enter into a contractual relationship with their customers, is not in a position to carry out legal checks. It is potentially exposed to verification obligations regarding infringements of the laws of a wide variety of legal systems. It is de facto impossible for it to investigate and verify in a well-founded manner notice letters whose substantiation corresponds to that of the letters submitted by the applicant. This applies in particular if, as in the present case, the court would still consider the little substantiated information provided by the applicant to be sufficient.

The respondent will not be able to provide its service if it is confronted with a large number of blocking requests in the future – also in view of the aspect or risk of equivalent violations. The respondent will not be able to check and implement these due to the lack of staff capacity. If the recipient does not implement a DNS block because it considers the factual situation to be too thin or is unable to comprehend it, there is a risk of costly warnings or a possibly costly and resource-intensive legal dispute. It is to be feared that many (independent and smaller) providers or even companies that operate their own recursive resolvers will not take this risk, but will implement a DNS block without a deeper examination of the justification, even at the risk of blocking legitimate content.

Before the defendant is exposed to the permanent risk of forfeiture of regulatory fines, it will have to give up its server location in Europe. This will not only be to the detriment of the defendant, but also of its European users. This is because the respondent's service would continue to be available to users from Germany even if the server were located outside the EU, but without being able to guarantee compliance with European data protection standards. In order to promote data protection and data security in the use of DNS by European companies, the EU Commission has launched the "DNS4EU" initiative (https://ec.europa.eu/digital-single-market/en/faq/faq-eu-cybersecurity-strategy-digital-

decade), under which the EU itself will establish a European DNS resolver to enable compliance with European data protection rules and reduce the dependence of EU companies on DNS resolvers in third countries. These efforts would be thwarted if the respondent had to discontinue its service, which already meets the highest data protection standards.

The infringement of the respondent's entrepreneurial freedom outweighs the infringement of the applicant's fundamental right to property. The applicant's legal interests are only insignificantly affected by the retrieval of the disputed domain via the respondent's service. In assessing the severity of the impairment, it must be taken into account in this respect that the applicant has already obtained DNS blocks for the disputed domain from all major German Internet access providers via the recommendation of CUII. For the vast majority of Internet users in Germany, access to the disputed domain is already blocked as a result of the implementation of the CUII recommendation by the access providers involved. The specific retrieval path via the respondent's service is only of minor importance in relation to the actual retrievals of the disputed domain. According to the APNIC evaluation, the usage rate of the respondent on August 30, 2021 is 0.097% in Germany compared to 18.489% of Google.

Supporting documentation: Screenshot statistical analysis of APNIC, available at https://stats.labs.apnic.net/rvrs/QO?o=cXAw1l1s0t10x, as **Exhibit AG 12**.

If the applicant were concerned with effectively preventing access to the disputed domain, it would have to give priority to other DNS resolvers with a larger market share than the respondent, in particular the public DNS resolver of the Google Group. In this constellation, the fundamental rights of the affected parties are to be weighted more in favor of the applicant, since a greater importance of the retrieval path is offset by a lesser economic impairment. In the present case, however, the minor economic importance of the retrieval path via the respondent's service cannot justify the endangerment of its business model.

1.4 Auxiliary request unfounded

The alternatively asserted claim pursuant to Section 7 (4) German Telemedia Services Act is also unfounded. The requirements of reasonableness, proportionality and subsidiarity are expressly set out in Section 7 (4) of the German Telemedia Services Act. These requirements are not met in the present case; in this respect, reference is made to the comments on interferer liability.

2. No ground for injunction

Finally, there is also no reason for the injunction.

This is the case if provisional safeguarding in summary proceedings is necessary to avert a threat to the creditor's interests. There must be circumstances which, in the objective judgment of a reasonable person, give rise to fear that the realization of the individual claim is endangered by imminent change of the existing circumstances (cf. Seiler in: Thomas/Putzo,

German Civil Procedural Code, 39th ed. 2018, § 935 marginal no. 6, § 940 marginal no. 5 with further references).

Even if certain deadlines in this area can only serve as a point of reference, a lack of urgency is generally to be assumed if the injunction creditor, without compelling reasons, allows a period of more than one month from knowledge of the infringement to elapse until the application is filed(OLG Köln, decision dated January 22, 2010 - 6 W 149/09, GRUR-RR 2010, 493 - Ausgelagerte Rechtsabteilung).

According to these principles, the applicant's request for an injunction was not received within the time limit. The applicant has allowed the one-month period to elapse. The applicant itself has submitted and made credible by affidavit of REDACTED (Exhibit AST 3) that it became aware of the infringement on March 11, 2021. The application for a temporary injunction is dated 12.04.2021, i.e. it was written more than one month after the applicant became aware of the infringement and was not received by the court until 14.04.2021.

The question of urgency is not to be assessed in relation to a work (see OLG Munich, judgment of 17.10.2019 - 29 U 1661/19, BeckRS 2019, 25462), because the applicant is not concerned with the blocking of a work, but with the blocking of a DNS query resolution. The measure specifically requested is not directed at a specific property right, but at the fact that access to a domain as a whole is no longer provided and the users of the respondent can consequently no longer access all content of the website linked to the domain. If the asserted claim does not result solely from the infringement of a specific property right, but – as in the present case, among other things, from the overall relationship of lawful and unlawful content of the website subject to the complaint – the question of urgency is also not to be assessed on the basis of the individual property right (so also BGH GRUR 2018, 1044 marginal no. 27 - Dead Island on the question of whether the reference giving rise to the duty of inspection for the interferer liability must be work-related). The applicant has been aware for some time that copyright infringements of its works are continuously committed via the disputed website. The applicant therefore already had the opportunity to claim the requested DNS blocking from the respondent beforehand. Consequently, the applicant did not consider the enforcement of the claim asserted by it to be urgent as a whole. A selective exercise of rights based on the marketing topicality of works would, conversely, not justify an urgent blocking of an entire domain.

Apart from that, even considering the timeliness of the music album, the one-month deadline was not met.

Accordingly, the application for a preliminary injunction is inadmissible and unfounded.

C. Value of the Matter

The value of the injunction dispute is set too high at EUR 100,000. The amount in dispute is to be determined in accordance with §§ 53 GKG (German Court Cost Act), § 3 German Civil Procedural Code. The court decisions issued to date on website blocking show that the number of plaintiffs, the number of infringements asserted, the market significance of the access

provider, and the significance of the blocked website are the decisive factors in determining the amount in dispute.

Based on the total of 12 sound recordings, a maximum amount in dispute of EUR 30,000 would be appropriate in the main proceedings. In a main action with three leading music labels as plaintiffs, which asserted rights to three music albums against a leading German access provider and requested the blocking of the leading website in the area of music file sharing, goldesel.to, the Munich Regional Court I used an amount in dispute of EUR 150,000 as a basis (LG München I, judgment of June 7, 2019, 37 O 2516/18). The BGH's leading decision on the access provider's interferer liability was based on an amount in dispute in the main proceedings of EUR 600,000 (OLG Köln decision on the amount in dispute of December 9, 2011, 6 U 192/11 and lower court LG Köln of October 12, 2011, 28 O 362/10). In these proceedings, four plaintiffs asserted rights to six music albums with a total of 120 tracks against a nationwide access provider against the leading website REDACTED. In its decision on the registrar's interferer liability (OLG Cologne, judgment of August 31, 2018, 6 U 14/18) in the main proceedings, the OLG Cologne based a blocking claim relating to 9 domains of the leading website "The Pirate Bay", in which rights to a multi-award-winning feature film were asserted, on an amount in dispute of EUR 100,000.

Based on this standard, the amount in dispute must be set lower in the present case. Based on the number of sound recordings in the decisions of the Munich Regional Court I and the Federal Court of Justice, a value in dispute of between EUR 50,000 and EUR 60,000 would be appropriate for the main proceedings. However, the amount in dispute must be further reduced in this case considering the fact that the economic significance of the asserted blocking claim is lower due to additional circumstances. The website REDACTED subject to the complaint has significantly lower traffic than the website REDACTED subject to the complaint in the aforementioned proceedings (hits from Germany on goldesel.to in September 2020: 3.06 million, hits on REDACTED in Germany in the same period: approx. 932,000), so that measured against this, the number of accesses to illegal content is also lower by approx. 1/3 and, in the same proportion, the economic significance of the asserted infringement.

Supporting documentation: Copy Roundtable DNS Blocking, list of selected. copyright-infringing websites for submission to the German Federal Cartel Office, p. 8f., available at: https://fragdenstaat.de/anfrage/clearingstelle-urheberrecht-im-internet-und-netzsperren-durch-internetzugangsanbieter-1/615725/anhang/2020-11-16Schreibenincl.Anlagen.pdf, as **Annex AG 13.**

In addition, the number of accesses to the website using the respondent's service is also significantly lower than via nationwide access providers due to its much lower market significance (see 1.3.3.4.3 above, the proportion of Internet users in Germany using the respondent's service on August 30, 2021 was only 0.097% and thus a fraction of the market share of large access providers). Accordingly, the amount in dispute in the preliminary injunction proceedings is to be set at a maximum of EUR 20,000.

Rechtsanwaltsgesellschaft Rickert mbH
durch:

Thomas Rickert, Rechtsanwalt