Cache Poisoned Denial of Service (English translation)

Cache Poisoned Denial of Service - Author not stated, cpdos.org.

- Published: date not stated
- Original: <https://cpdos.org/>
- Preserved from: https://cpdos.org/ (live) on 2026-08-09
- Licence: unknown

Content (translated into English)

Machine translation of `cpdos-org-cache-poisoned-denial-service.md`, which holds the source's own words. Code, payloads, type names, URLs and CVE identifiers were masked before translating and restored after, so they are byte-identical to the original.

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

CPDoS: Cache Poisoned Denial of Service

What is CPDoS?

Cache-**P**oisoned **D**enial-**o**f-**S**ervice (**CPDoS**) is a new class of web cache poisoning attacks aimed at disabling web resources and websites.

How does it work?

The basic attack flow is described below and depicted in the following figure:

-

An attacker sends a simple HTTP request containing a **malicious header** targeting a victim resource provided by some web server. The request is processed by the intermediate cache, while the malicious header remains unobtrusive.

-

The cache forwards the request to the origin server as it does not store a fresh copy of the targeted resource. At the origin server, the request processing provokes an **error** due to the malicious header it contains.

-

As a consequence, the origin server returns an **error page** which gets stored by the cache instead of the requested resource.

-

The attacker knows that the attack was successful when she retrieved an error page in response.

-

Legitimate users trying to obtain the target resource with subsequent requests...

-

...will get the cached error page instead of the original content.

[image: image]

With CPDoS, a malicious client can block any web resource that is distributed via Content Distribution Networks (CDNs) or hosted on proxy caches. Note, that **a single crafted request** is sufficient to restrain all subsequent requests from accessing the targeted content.

Which CPDoS variations exist?

We detected three variations of CPDoS:

-

HTTP Header Oversize (HHO)

-

HTTP Meta Character (HMC)

-

HTTP Method Override (HMO)

HTTP Header Oversize (HHO)

An HTTP request header contains vital information for intermediate systems and web servers. This includes cache-related header fields or meta data on client supported media types, languages and encodings. The HTTP standard does not define any size limit for HTTP request headers. As a consequence, intermediate systems, web servers, and web frameworks define limits by their own. Most web servers and proxies such as Apache HTTPD provide a request header size limit of around 8,192 bytes to mitigate, e.g., Request Header Buffer Overflow or ReDoS attacks. However, there are also intermediate systems that specify limits larger than 8,192 bytes. For instance, the Amazon Cloudfront CDN allows up to 20,480 bytes. This semantic gap in terms of request header size limits can be exploited to conduct a cache poisoning attack which can lead to a denial of service.

HHO CPDoS attacks work in scenarios where a web application uses a cache that accepts a larger header size limit than the origin server. To attack such a web application, a malicious client sends a `HTTP GET` request including a header larger than the size supported by the origin server but smaller than the size supported by the cache. To do so, an attacker has two options. First, she

crafts a request header with many malicious headers as shown in the following Ruby code snippet. The other option is to include one single header with an oversized key or value.

```
require 'net/http'
uri = URI("https://example.org/index.html")
req = Net::HTTP::Get.new(uri)

num = 200
i = 0

# Setting malicious and irrelevant headers fields for creating an oversized header
until i > num  do
        req["X-Oversized-Header-#{i}"] = "Big-Value-00000000000000000000000000000000"
        i +=1;
end

res = Net::HTTP.start(uri.hostname, uri.port, :use_ssl => uri.scheme == 'https') {|http|
        http.request(req)
}
```

The figure below shows an HHO CPDoS attack flow in which a malicious client sends a request created by the above code snippet. The cache forwards this request including all headers to the endpoint since the header size remains below the size limit of 20,480 bytes. The web server, however, blocks this request and returns an error page, as the request header exceeds its header size limit. This error page with status code `400 Bad Request` is now stored by the cache. All subsequent requests targeting the denialed resource are now provided with an error page instead of the genuine content.

[image: HRS attack]

The video demonstrates the HHO CPDoS attack with an example web application hosted on Cloudfront. In the attack, embedded web resources are selectively replaced by error pages rendering first some parts of the web page and finally the entire page unavailable.

HTTP Meta Character (HMC)

The HTTP Meta Character (HMC) CPDoS attack works similar to the HHO CPDoS attack. Instead of sending an oversized header, this attack tries to bypass a cache with a request header containing a harmful meta character. Meta characters can be, e.g., control characters such as line break/carriage return (`\n`), line feed (`\r`) or bell (`\a`).

[image: image]

An unaware cache forwards such a request to the origin server without blocking the message or sanitizing the meta characters. The origin server, however, may classify such a request as

malicious as it contains harmful meta characters. As a consequence, the origin server returns an error message which is stored and reused by the cache.

HTTP Method Override Attack (HMO)

The HTTP standard provides several HTTP methods for web servers and clients for performing transactions on the web. `GET`, `POST`, `DELETE` and `PUT` are arguably the most used HTTP methods in web applications and REST-based web services. Many intermediate systems such as proxies, load balancers, caches, and firewalls, however, do only support `GET` and `POST`. This means that HTTP requests with `DELETE` and `PUT` are simply blocked. To circumvent this restriction many REST-based APIs or web frameworks such as the Play Framework 1, provide headers such as `X-HTTP-Method-Override`, `X-HTTP-Method` or `X-Method-Override` for tunnel blocked HTTP methods. Once the request reaches the server, the header instructs the web application to override the HTTP method in the request line with the one in the corresponding header value.

```
POST /items/1 HTTP/1.1
Host: example.org
**X-HTTP-Method-Override: DELETE**

HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 62

Resource has been successfully removed with the DELETE method.
```

The code snippet shows a request that can bypass a security policy that prohibits `DELETE` requests by using the `X-HTTP-Method-Override` header. On the server-side this `POST` request will be interpreted as a `DELETE` request.

These method overriding headers are very useful in scenarios when intermediate systems block distinct HTTP methods. However, if a web application supports such a header and also uses a web caching system like a reverse proxy cache or CDN for optimizing performance, a malicious client can exploit this constellation to conduct a CPDoS attack. The figure below illustrates the principle flow of an HTTP Method Override Attack (HMO) CPDoS attack using the `X-HTTP-Method-Override` header.

[image: HRS attack]

Here, the attacker sends a `GET` request with an `X-HTTP-Method-Override` header containing `POST`. A vulnerable cache interprets this request as a benign `GET` request targeting the resource https://example.org/index.html. The web application, however, will interpret this request as a `POST` request, since the `X-HTTP-Method-Override` header instructs the server to replace the HTTP method in the request line. Accordingly, the web application returns a response based on `POST`. Let's assume that the target web application doesn't implement any business logic for `POST` on

/index.html. In such cases, web frameworks like the Play Framework 1 return an error message with the status code `404 Not Found`. The cache assumes that the returned response with the error code is the result of the `GET` request targeting https://example.org/index.html. Since the status code `404 Not Found` is allowed to be cached according to the HTTP Caching RFC 7231, caches store and reuse this error response for recurring requests. Each benign client making a subsequent `GET` request to https://example.org/index.html will receive a stored error message with status code `404 Not Found` instead of the genuine web application's start page.

The video below demonstrates an HMO attack on a web application. Here, the attacker uses the Postman tool to block the start page from being accessed.

Impact

The map below shows the impact of CPDoS attacks on CDNs. Once the error page is injected, the CDN distributes it to many other edge cache server locations around the world. The map illustrates how far the error page is distributed to several edge locations within the CDN. The [image: image] icons show the affected locations displaying the error page. Fortunately, not all edge servers are infected by this attack which is shown by the [image: image] icons. This icon denotes the locations where clients receive the genuine page. The [image: image] icon shows the location of the origin server and the [image: image] icon displays the attacker's locations.

The first figure shows the affected regions in Europe and some parts of Asia when sending a CPDoS attack from Frankfurt, Germany to a victim origin server in Cologne, Germany. The second one illustrates the poisoned regions in the USA when executing a CPDoS attack from Northern Virginia, USA to the same victim origin server in Cologne, Germany. [image: image]

[image: image]

This analysis has been conducted with TurboBytes Pulse and the speed testing tool of KeyCDN. Both services provide a testing environment covering a lot of test agents scattered around the world.

CPDoS vulnerability overview

This overview summarizes what pair of web caching system and HTTP implementation is vulnerable to what CPDoS attack. More details are described in the paper which can be downloaded below. **Note, that the table below illustrates the results from our research experiments conducted in February 2019. In the meantime, the affected organizations have taken precautions to mitigate CPDoS attacks. The majority of the CPDoS vulnerabilities has been addressed by the respective organizations. Click on the info icons in the table or see the section Vendor Responses to CPDoS for more details.**

HTTP ImplementationCache	Apache HTTPD	Apache TS	Nginx	Squid	Varnish	Akamai	Azure	CDN77	CDNSun	Cloudflare	CloudFront	Fastly	G-Core Labs	KeyCDN	StackPath
Apache HTTPD + (ModSecurity)										HHO, HMC					
Apache TS															
Nginx + (ModSecurity)															

| | | | | | | | | | | HHO | | | | | | IIS | | | | | (HHO) | (HHO) | | (HHO) | | (HHO) | HHO, HMC | (HHO) | | | | | | Tomcat | | | | | | | | | | | HHO | | | | | | Squid | | | | | | | | | | | | | | | | | | | | Varnish | | | | | | | | | | | HHO, HMC | | | | | | Amazon S3 | | | | | | | | | | | | | | HHO | | | | | | Google Cloud Storage | | | | | | | | | | | | | | | | | | | | | | Github Pages | | | | | | | | | | | HHO, HMC | | | | | | Gitlab Pages | | | | | | | | | | | HMC | | | | | | Heroku | | | | | | | | | | | HHO | | | | | | ASP.NET | | | | | (HHO) | (HHO) | | (HHO) | | (HHO) | (HHO), (HMC) | (HHO) | | | | | | BeeGo | | | | | | | | | | | HMC | | | | | | Django | | | | | | | | | | | (HHO), (HMC) | | | | | | Express.js | | | | | | | | | | | HMC | | | | | | Flask | | | | | | (HMO) | | | | | HMO, (HHO), (HMC) | | | | | | Gin | | | | | | | | | | | HMC | | | | | | Laravel | | | | | | | | | | | (HHO), (HMC) | | | | | | Meteor.js | | | | | | | | | | | HMC | | | | | | Play 1 | | | | | HMO | HMO | | HMO | | HMO | HHO, HMO | HMO | | | | | | Play 2 | | | | | | | | | | | HHO, HMC | | | | | | Rails | | | | | | | | | | | (HHO), (HMC) | | | | | | Spring Boot | | | | | | | | | | | HHO | | | | | | Symfony | | | | | | | | | | | (HHO), (HMC) | | | | | |

Mitigations

One of the main reasons for HHO and HMC CPDoS attacks lies in the fact that a vulnerable cache illicitly stores responses containing error codes such as `400 Bad Request` by default. This is not allowed according to the HTTP standard. The web caching standard only allows to cache the error codes `404 Not Found`, `405 Method Not Allowed`, `410 Gone` and `501 Not Implemented`. Hence, caching error pages according to the policies of the HTTP standard is the first step to avoid CPDoS attacks.

Content providers must also use the appropriate status code for the corresponding error case. For instance, `400 Bad Request` which is used by many HTTP implementations for declaring an oversized header is not the suitable status code. IIS even uses `404 Not Found` when a specific header is exceeded. The right error code for an oversized request header is `431 Request Header Fields Too Large`. According to our analysis, this error message is not cached by any web caching systems.

Another effective countermeasure against HHO and HMC CPDoS attacks is to exclude error pages from caching. One approach is to add the header `Cache-Control: no-store` to each error page. The other option is to disable error page caching in the cache configuration. CDNs like CloudFront or Akamai provide configuration settings to do so.

A Web Application Firewalls (WAF) can also be deployed to mitigate CPDoS attacks. However, WAFs must be placed in front of the cache in order to block malicious content before they reach the origin server. WAFs that are placed in front of the origin server can be exploited to provoke error pages that get cached either.

For more details on possible mitigations and countermeasures, please read our paper.

Paper

For more details on CPDoS attacks, you are welcome to read our research paper. A preprint can be downloaded below.

Hoai Viet Nguyen, Luigi Lo Iacono, and Hannes Federrath **Your Cache Has Fallen: Cache-Poisoned Denial-of-Service Attack** 26th ACM Conference on Computer and Communications Security (CCS) 2019

Abstract Bibtex Download

Abstract

Web caching enables the reuse of HTTP responses with the aim to reduce the number of requests that reach the origin server, the volume of network traffic resulting from resource requests, and the user-perceived latency of resource access. For these reasons, a cache is a key component in modern distributed systems as it enables applications to scale at large. In addition to optimizing performance metrics, caches promote additional protection against Denial of Service (DoS) attacks.

In this paper we introduce and analyze a new class of web cache poisoning attacks. By provoking an error on the origin server that is not detected by the intermediate caching system, the cache gets poisoned with the server-generated error page and instrumented to serve this useless content instead of the intended one, rendering the victim service unavailable. In an extensive study of fifteen web caching solutions we analyzed the negative impact of the Cache-Poisoned DoS (CPDoS) attack---as we coined it. We show the practical relevance by identifying one proxy cache product and five CDN services that are vulnerable to CPDoS. Amongst them are prominent solutions that in turn cache high-value websites. The consequences are severe as one simple request is sufficient to paralyze a victim website within a large geographical region. The awareness of the newly introduced CPDoS attack is highly valuable for researchers for obtaining a comprehensive understanding of causes and countermeasures as well as practitioners for implementing robust and secure distributed systems.

```
@inproceedings{conf/ccs2019/nguyen,
    author = {H.V. Nguyen and L. Lo Iacono and H. Federrath},
    title = {{Your Cache Has Fallen: Cache-Poisoned Denial-of-Service Attack}},
    booktitle = {{26th ACM Conference on Computer and Communications Security (CCS)}},
    year = {2019},
    url = {https://doi.org/10.1145/3319535.3354215},
    abstract = {{Web caching enables the reuse of HTTP responses with the aim to reduce the number of requests that reach the origin server, the volume of network traffic resulting from resource requests, and the user-perceived latency of resource access. For these reasons, a cache is a key component in modern distributed systems as it enables applications to scale at large. In addition to optimizing performance metrics, caches promote additional protection against Denial of Service (DoS) attacks.

    In this paper we introduce and analyze a new class of web cache poisoning attacks. By provoking an error on the origin server that is not detected by the intermediate caching system, the cache gets poisoned with the server-generated error page and instrumented to serve this useless content instead of the intended one, rendering the victim service unavailable. In an extensive study of fifteen web caching solutions we analyzed the negative impact of the Cache-Poisoned DoS (CPDoS) attack---as we coined it. We show the practical relevance by identifying one proxy cache product and five CDN services that are vulnerable to CPDoS. Amongst them are prominent solutions that in turn cache high-value websites. The consequences are severe as one simpl
    request is sufficient to paralyze a victim website within a large geographical region. The awareness of the newly introduced CPDoS attack is highly valuable for researchers for obtaining a comprehensive understanding of causes and countermeasures as well as practitioners for implementing robust and secure distributed systems
    }}
}
```

Talks

On November 14th, 2019, we will give a talk on CPDoS attacks at the CCS 2019. For more information, please take a look at the CCS' agenda: https://sigsac.org/ccs/CCS2019/...

HHO, HMC and HMO are not the only CPDoS variations. In March 2019, Nathan Davison has detected a CPDoS variation which use CORS headers. Also, Nathan posted a blog post on using the Connection header to conduct a CPDoS attack.

Moreover, James Kettle has published a blog article discussing other variations of CPDoS attacks on real world websites. James is Head of Research at PortSwigger Web Security. He wrote many blog articles on practical web cache poisoning vulnerabilities as well as a new variation of HTTP Request Smuggling denoted as HTTP Desync Attacks.

Coverage

www.hostingadvice.com *March 30, 2020* **Researchers Identify a New Cache Poisoning Attack Impacting CDNs That Could Block Web Resources and Sites** https://www.hostingadvice.com/blog/researchers-identify-new-cache-poisoning-attack/

nathandavison.com *February 24, 2020* **Cache poisoning DoS in CloudFoundry gorouter (CVE-2020-5401)** https://nathandavison.com/blog/cache-poisoning-dos-in-cloudfoundry-gorouter

Golem.de *October 23, 2019* **Cache attacks can cripple websites** https://www.golem.de/news/cpdos-angriff-cache-angriffe-koennen-webseiten-lahmlegen-1910-144575.html

The Hacker News *October 23, 2019* **New Cache Poisoning Attack Lets Attackers Target CDN Protected Sites** https://thehackernews.com/2019/10/cdn-cache-poisoning-dos-attack.html

ZDNet *October 23, 2019* **CPDoS attack can poison CDNs to deliver error pages instead of legitimate sites** https://www.zdnet.com/article/cpdos-attack-can-poison-cdns-to-deliver-error-pages-instead-of-legitimate-sites/

Bleeping Computer *October 23, 2019* **New CPDoS Web Cache Poisoning Attacks Impact Sites Using Popular CDNs** https://www.bleepingcomputer.com/news/security/new-cpdos-web-cache-poisoning-attacks-impact-sites-using-popular-cdns/

Cyware *October 23, 2019* **New 'CPDoS' Web Cache Poisoning Attack Impacts Content Delivery Networks (CDN)** https://cyware.com/news/new-cpdos-web-cache-poisoning-attack-impacts-content-delivery-networks-cdn-440ffccc/

Security Affairs *October 23, 2019* **Exploring the CPDoS attack on CDNs: Cache Poisoned Denial of Service** https://securityaffairs.co/wordpress/92859/hacking/cpdos-attack-cdns.html

The Media HQ *October 23, 2019* **CPDoS attack can poison CDNs to deliver error pages instead of legitimate sites** https://themediahq.com/cpdos-attack-can-poison-cdns-to-deliver-error-pages-instead-of-legitimate-sites/

Reblaze *October 23, 2019* **CPDoS – A new DoS attack on the rise** https://www.reblaze.com/blog/cpdos-new-dos-attacks-rise/

SensorsTechForum *October 24, 2019* **Cache Poisoned Denial of Service (CPDoS) Attacks Used Against Content Delivery Networks** https://sensorstechforum.com/cpdos-attacks-cdn/

Naked Security *October 24, 2019* **Vulnerability in content distribution networks found by researchers** https://nakedsecurity.sophos.com/2019/10/24/researchers-find-vulnerability-in-content-distribution-networks/

ACM TECHNEWS *October 24, 2019* **CPDoS Attack Can Poison CDNs to Deliver Error Pages Instead of Legitimate Sites** https://cacm.acm.org/news/240392-cpdos-attack-can-poison-cdns-to-deliver-error-pages-instead-of-legitimate-sites/fulltext

Security Week *October 24, 2019* **Researchers Warn of New Cache-Poisoned DoS Attack Method** https://www.securityweek.com/researchers-warn-new-cache-poisoned-dos-attack-method

Cybers Guard *October 25, 2019* **Experts Warn of the Latest Cache-Poisoned Method of Attack** https://cybersguards.com/experts-warn-of-the-latest-cache-poisoned-method-of-attack/

Vendor Responses to CPDoS

Play Framework *March 14, 2019* **Define allowed methods used in 'X-HTTP-Method-Override'** https://github.com/playframework/play1/issues/1300

Microsoft *June 11, 2019* **CVE-2019-0941 | Microsoft IIS Server Denial of Service Vulnerability** https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0941

Amazon Web Services *September 7, 2019* **How CloudFront Processes and Caches HTTP 4xx and 5xx Status Codes from Your Origin** https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HTTPStatusCodes.html

Akamai *October 23, 2019* **CPDOS POISONING ATTACK** https://blogs.akamai.com/2019/10/cpdos-poisoning-attack.html

Cloudflare *October 24, 2019* **Cloudflare response to CPDoS exploits** https://blog.cloudflare.com/cloudflare-response-to-cpdos-exploits/

CDN77 *October 23, 2019* **Our statement regarding today's article published by @TheHackersNews CDN77 is not vulnerable to CPDoS attacks.** https://twitter.com/CDN77com/status/1186971315217092612

Verizon Digital Media *October 28, 2019* **CPDoS attack update** https://www.verizondigitalmedia.com/blog/cpdos-attack-update/

Contact

[image: ...]

Hoai Viet Nguyen

[](mailto:viet.nguyen@th-koeln.de)

[image: ...]

Luigi Lo Iacono

[](mailto:luigi.lo_iacono@th-koeln.de)

Legal Disclosure

Information in accordance with section 5 TMG

TH Köln - University of Applied Sciences F07/IMP Data and Application Security Group Gustav-Heinemann-Ufer 54 50968 Cologne

Represented by

Prof. Dr. Luigi Lo Iacono

Contact

Telephone: 0221/8275-2527 Email: luigi.lo_iacono at th-koeln.de Website: das.th-koeln.de

Person responsible for content in accordance with 55 Abs. 2 RStV

- Hoai Viet Nguyen
- Luigi Lo Iacono

Indication of source for images and graphics

Bomb, Recycle, and Server and icons made by Freepik from www.flaticon.com

404 icon made by DinosoftLabs from www.flaticon.com

Cloud icon made by Smashicons from www.flaticon.com

Explosion icon made by Good Ware from www.flaticon.com

Disclaimer

Accountability for content The contents of our pages have been created with the utmost care. However, we cannot guarantee the contents' accuracy, completeness or topicality. According to statutory provisions, we are furthermore responsible for our own content on these web pages. In this context, please note that we are accordingly not obliged to monitor merely the transmitted or saved information of third parties, or investigate circumstances pointing to illegal activity. Our obligations to remove or block the use of information under generally applicable laws remain unaffected by this as per §§ 8 to 10 of the Telemedia Act (TMG).

Accountability for links Responsibility for the content of external links (to web pages of third parties) lies solely with the operators of the linked pages. No violations were evident to us at the time of linking. Should any legal infringement become known to us, we will remove the respective link immediately.

Copyright Our web pages and their contents are subject to German copyright law. Unless expressly permitted by law (§ 44a et seq. of the copyright law), every form of utilizing, reproducing or processing works subject to copyright protection on our web pages requires the prior consent of the respective owner of the rights. Individual reproductions of a work are allowed only for private use, so must not serve either directly or indirectly for earnings. Unauthorized utilization of copyrighted works is punishable (§ 106 of the copyright law).

Privacy Policy

- F. Rights of Data Subjects

A. Name and Address of the Controller

The controller within the meaning of the EU General Data Protection Regulation (GDPR), other national data protection laws, and other data protection provisions is:

TH Köln Data and Application Security Group Prof. Dr. Luigi Lo Iacono Betzdorfer Str. 2 50679 Cologne Tel: +49 221-8275-2527 Email: luigi.lo_iacono@th-koeln.de Website: cpdos.org

B. Name and Address of the Data Protection Officers of TH Köln

Walter Keens Claudiusstraße 1 50678 Cologne Tel: +49 221 8275 3108 Email: datenschutzbeauftragter@th-koeln.de

Bernadette Schmitz Claudiusstraße 1 50678 Cologne Tel: +49 221 8275 3994 Email: datenschutzbeauftragter@th-koeln.de

C. Supervisory Authority for Data Protection Matters

State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia (LDI NRW) Kavalleriestr. 2-4 40213 Düsseldorf Telephone: 0211/38424-0 Fax: 0211/38424-10 Email: poststelle@ldi.nrw.de

D. General Information on Data Processing

1. Scope of the Processing of Personal Data

As a rule, TH Köln processes the personal data of website users only to the extent necessary to provide a functional website and its content and services. The personal data of website users is generally processed only on the basis of consent that has been granted. An exception applies in cases where it is not possible, for factual reasons, to obtain prior consent and the processing of the data is permitted by law.

1. Legal basis for the processing of personal data

Insofar as TH Köln processes personal data on the basis of consent that has been granted, Art. 6(1)(a) GDPR constitutes the legal basis.

Where personal data is processed because this is necessary for the performance of a contract to which the data subject is a party, the legal basis is Art. 6(1)(b) GDPR. This also applies to processing activities that are necessary in order to take steps prior to entering into a contract.

Insofar as the processing of personal data is necessary for compliance with a legal obligation to which TH Köln, as a public-law corporation, is subject, Art. 6(1)(c) GDPR serves as the legal basis.

Where the vital interests of the data subject or of another natural person require the processing of personal data, Art. 6(1)(d) GDPR constitutes the legal basis.

If processing is necessary to safeguard a legitimate interest of TH Köln or a third party, and the interests, fundamental rights, and fundamental freedoms of the data subject do not override the former interest, the legal basis is Art. 6(1)(f) GDPR.

1. Data erasure and retention period

The personal data of the data subject is erased or blocked as soon as the purpose for which it was stored no longer applies. The data may also be retained if this has been provided for by the European or national legislature in European Union regulations, laws, or other provisions to which TH Köln is subject. The data is also blocked or erased when a retention period prescribed by the aforementioned provisions expires, unless the data must continue to be stored for the conclusion or performance of a contract or to comply with a retention obligation.

E. Provision of the website and creation of log files

1. Description and scope of data processing

Each time our website is accessed, TH Köln automatically collects data and information from the computer system of the device accessing it.

The following data is collected:

- The users' IP address
- The date and time of access
- Websites accessed by the users' system via our website
- The users' operating system
- Information about the browser type and version used
- Websites from which the users' system reaches our website
- The users' internet service provider

The data is also stored in the log files of TH Köln's systems. This data is not stored together with other personal data of the users.

1. Legal basis for data processing

The legal basis for storing the data is Art. 6(1)(a) GDPR.

1. Purpose of data processing

The system must temporarily store the IP address in order to deliver the website to the users' device. For this purpose, the users' IP address must remain stored for the duration of the session.

Data is stored in log files to ensure the functionality of the website. The data also serves to optimize the website and ensure the security of TH Köln’s information technology systems. The data is not analyzed for marketing purposes in this context.

TH Köln’s legitimate interest in data processing pursuant to Art. 6 Abs. 1 lit. f DS-GVO is based on these purposes.

1. Storage Period

The data is deleted as soon as it is no longer required to achieve the purpose for which it was collected. When data is collected to provide the website, this occurs when the respective session

has ended.

When data is stored in log files, this occurs after no more than seven days. In this case, users' IP addresses are deleted or altered so that the accessing client can no longer be identified.

1. Right to Object and Options for Removal

The collection of data to provide the website and the storage of data in log files are strictly necessary for operating the website. Consequently, users have no right to object.

F. Rights of Data Subjects

If your personal data is processed, you are a data subject i.S.d. DS-GVO and have the following rights with respect to TH Köln:

1. Right of Access

You may request confirmation from TH Köln as to whether we process personal data concerning you. If such processing takes place, you may request the following information from TH Köln:

-

the purposes for which the personal data is processed;

-

the categories of personal data that are processed;

-

the recipients or categories of recipients to whom the personal data concerning you has been or will be disclosed;

-

the planned period for which the personal data concerning you will be stored or, if specific information is not possible, the criteria used to determine the storage period;

-

the existence of a right to rectification or erasure of the personal data concerning you, a right to restriction of processing by TH Köln, or a right to object to such processing;

-

the existence of a right to lodge a complaint with a supervisory authority;

-

all available information concerning the source of the data where the personal data was not collected from the data subject;

-

the existence of automated decision-making, including profiling, pursuant to Art. 22 Abs. 1 and 4 DS-GVO and—at least in these cases—meaningful information about the logic involved, as well as the significance and intended effects of such processing for the data subject.

You have the right to request information as to whether the personal data concerning you is transferred to a third country or an international organization. In this context, you may request to be informed of the appropriate safeguards pursuant to Art. 46 DS-GVO in connection with the transfer.

This right of access may be restricted to the extent that it is likely to render impossible or seriously impair the achievement of the research or statistical purposes and the restriction is necessary to fulfill those research or statistical purposes.

1. Right to Rectification

You have a right to rectification and/or completion by TH Köln if the personal data concerning you that is processed is inaccurate or incomplete. TH Köln must carry out the rectification without undue delay. Your right to rectification may be restricted insofar as its exercise is likely to render impossible or seriously impair the achievement of the research or statistical purposes and the restriction is necessary for the fulfillment of the research or statistical purposes.

1. Right to restriction of processing

You may request the restriction of the processing of personal data concerning you under the following conditions:

-

if you contest the accuracy of the personal data concerning you for a period that enables TH Köln to verify the accuracy of the personal data;

-

the processing is unlawful and you oppose the erasure of the personal data and request instead that the use of the personal data be restricted;

-

TH Köln no longer needs the personal data for the purposes of processing, but you require it for the establishment, exercise, or defense of legal claims; or

-

if you have objected to the processing pursuant to Art. 21(1) GDPR and it has not yet been determined whether the legitimate grounds of TH Köln override your grounds.

If the processing of personal data concerning you has been restricted, this data may—with the exception of storage—be processed only with your consent or for the establishment, exercise, or defense of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest of the European Union or of a Member State. If processing has been restricted under the o.g. conditions, TH Köln will inform you before the restriction is lifted.

Your right to restriction of processing may be restricted insofar as its exercise is likely to render impossible or seriously impair the achievement of the research or statistical purposes and the restriction is necessary for the fulfillment of the research or statistical purposes.

1. Right to erasure

- Obligation to erase

You may request that TH Köln erase personal data concerning you without undue delay, and TH Köln is obliged to erase this data without undue delay where one of the following grounds applies:

- The personal data concerning you is no longer necessary for the purposes for which it was collected or otherwise processed.
- You withdraw the consent on which the processing was based pursuant to Art. 6(1)(a) or Art. 9(2)(a) GDPR, and there is no other legal basis for the processing.
- You object to the processing pursuant to Art. 21(1) GDPR and there are no overriding legitimate grounds for the processing, or you object to the processing pursuant to Art. 21(2) GDPR.
- The personal data concerning you has been processed unlawfully.
- The personal data concerning you must be erased in order to comply with a legal obligation under European Union law or the law of the Member States to which TH Köln is subject.
- The personal data concerning you was collected in relation to information society services offered pursuant to Art. 8(1) GDPR.

-

Information to Third Parties If TH Köln has made the personal data concerning you public and is obliged to erase it pursuant to Art. 17(1) GDPR, then, taking into account the available technology and the cost of implementation, it shall take reasonable measures, including technical measures, to inform the TH Köln controllers that process the personal data that you, as the data subject, have requested the erasure of all links to those personal data or of copies or replications of those personal data.

-

Exceptions The right to erasure does not apply insofar as processing is necessary

- to exercise the right to freedom of expression and information;
- to comply with a legal obligation that requires processing under Union or Member State law to which TH Köln is subject, or to perform a task carried out in the public interest or in the exercise of official authority vested in TH Köln;
- for reasons of public interest in the area of public health pursuant to Art. 9(2)(h) and (i) and Art. 9(3) GDPR;
- for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes pursuant to Art. 89(1) GDPR, insofar as the right referred to in section a) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise, or defense of legal claims.

1. Right to Notification

If you have exercised your right to rectification, erasure, or restriction of processing against TH Köln, it is obliged to notify all recipients to whom the personal data concerning you have been disclosed of this rectification or erasure of the data or restriction of processing, unless this proves impossible or involves disproportionate effort. You have the right to be informed by TH Köln about these recipients.

1. Right to Data Portability

You have the right to receive the personal data concerning you that you have provided to TH Köln in a structured, commonly used, and machine-readable format. You also have the right to transmit those data to another TH Köln controller without hindrance from the TH Köln controller to which the personal data were provided, provided that

-

the processing is based on consent pursuant to Art. 6(1)(a) GDPR or Art. 9(2)(a) GDPR, or on a contract pursuant to Art. 6(1)(b) GDPR, and

-

the processing is carried out by automated means.

In exercising this right, you also have the right to have the personal data concerning you transmitted directly from TH Köln to another controller, where technically feasible. The freedoms and rights of others must not be adversely affected by this. The right to data portability does not apply to the processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in TH Köln.

1. Right to Object

You have the right, on grounds relating to your particular situation, to object at any time to the processing of the personal data concerning you that is based on Art. 6(1)(e) or (f) GDPR; this also applies to profiling based on those provisions.

TH Köln will no longer process the personal data concerning you unless it can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or the processing serves the establishment, exercise, or defense of legal claims.

You also have the right, on grounds relating to your particular situation, to object to the processing of personal data concerning you that is carried out for scientific or historical research purposes or for statistical purposes pursuant to Art. 89(1) GDPR.

Your right to object may be restricted insofar as its exercise is likely to render impossible or seriously impair the achievement of the research or statistical purposes and the restriction is necessary for the fulfillment of the research or statistical purposes.

1. Right to withdraw the declaration of consent under data protection law

You have the right to withdraw your declaration of consent under data protection law at any time. The withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal.

1. Automated individual decision-making, including profiling

You have the right not to be subject to a decision based solely on automated processing—including profiling—that produces legal effects concerning you or similarly significantly affects you. This does not apply if the decision

-

is necessary for entering into or performing a contract between you and TH Köln,

-

is authorized by European Union or Member State law to which TH Köln is subject and that law lays down suitable measures to safeguard your rights and freedoms and your legitimate interests; or

-

is made with your explicit consent.

However, these decisions may not be based on special categories of personal data referred to in Art. 9(1) GDPR unless Art. 9(2)(a) or (g) GDPR applies and suitable measures to safeguard your rights and freedoms and your legitimate interests have been taken. In the cases referred to in (a) and (c), TH Köln takes suitable measures to safeguard your rights and freedoms and your legitimate interests, including at least the right to obtain human intervention by TH Köln, to express your point of view, and to contest the decision.

1. Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, your place of work, or the place of the alleged infringement, if you consider that the processing of personal data concerning you infringes the GDPR.

The supervisory authority with which the complaint has been lodged will inform the complainant of the progress and outcome of the complaint, including the possibility of a judicial remedy pursuant to Art. 78 GDPR.