DECISION

The Data Protection Authority decides on the data protection complaint by G. H. (complainant) dated 10 April 2022 against nic.at GmbH (respondent), represented by Haider, Obereder, Pilz Rechtsanwält:innen GmbH, for violation of the right to confidentiality as follows:

- The complaint is dismissed as unfounded.

Legal basis: Art. 4 subpara. 1, Art. 6 para. 1 lit. c, Art. 51 para. 1, Art. 57 para. 1 lit. f as well as Art. 77 para. 1 of Regulation (EU) 2016/67 9 (General Data Protection Regulation, hereinafter: GDPR), OJ L 119 of May 4, 2016, p. 1; §§ 18 para. 1 as well as 24 para. 1 and para. 5 of the Data Protection Act (DSG), BGBl. . I No. 165/1999 as amended; §§ 2, 9, 14, 15 and 23 of the Network and Information Systems Security Act (NISG), BGBl. I No. 111/2018 as amended.

STATEMENT OF REASONS

A. Parties' submissions and procedural background

1. In his complaint of April 10, 2022, the complainant stated that, due to the General Data Protection Regulation (GDPR), the whois query provided by the respondent nic.at GmbH would not, in principle, publish any data of natural persons, regardless of whether they were domain holders or the technical contact (tech-C) of a domain. The complainant's domain ".....at" had been registered in 2002 by a "private person" (natural person). The complainant considered this to be a violation of his right to privacy because CERT.at GmbH, as a subsidiary of nic.at GmbH, had accessed personal data (name, address, telephone number, etc.) of the complainant and domain holder of ".....at" without his permission or knowledge by means of the Whois database.

The complaint was settled with a data protection declaration from the respondent, information on requests for information addressed to the respondent and information on the responsibility of CERT.at.

2. In its statement of April 28, 2022, the respondent, represented by a lawyer, stated, in summary, that the respondent nic.at GmbH is the Austrian registry for the administration of all internet domains under the top-level domain ".at". The respondent had been established by means of an official decision of the Federal Chancellor as an operator of essential services within the meaning of Section 16 of the Network and Information Security Act (NISG). CERT.at GmbH is a subsidiary of nic.at GmbH. CERT.at GmbH fulfills the function of the (Austrian) national "Computer Emergency Response Team (CERT)" within the meaning of Section 15 (3) NISG. This task had originally been assigned to nic.at GmbH and was transferred to CERT.at GmbH as part of a corporate demerger for the purposes of absorption. The transfer of the CERT activity to CERT.at GmbH was confirmed by the Federal Chancellery, the competent NIS authority, after the corporate demerger had been carried out. The central task of CERT (according to the NISG) is to ensure IT security in the national environment, which also includes the ".at" zone. According to the legal regulation of § 14 para. 2 NISG, the CERT would in any case be responsible for the following tasks:

- Receiving reports of risks, incidents or security incidents in accordance with §§ 19, 21 para. 2 and 23 para. 1 and 2;
- Forwarding reports (Z 1) to the Federal Minister of the Interior;
- Issuing early warnings, alerts and recommendations for action, as well as publishing and disseminating information on risks, incidents or security incidents;
- Initial general technical support in responding to a security incident;
- Monitoring and analyzing risks, incidents or security incidents, as well as assessing the situation;
- Participating in the coordination structures according to § 7 and participating in the CSIRTs network.

CERT.at GmbH is the (Austrian) national computer emergency response team, which was set up in 2008 by the Federal Chancellery (BKA) in cooperation with nic.at as a project at nic.at GmbH. As such, CERT.at is the point of contact for IT security in Austria. Since 2019, CERT.at GmbH has also been the national CERT under the NISG. It works closely with the Federal Chancellery, operators of essential services, critical infrastructure and relevant state institutions, among others. CERT.at GmbH networks other CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) from the critical infrastructure and information and communication technology (ICT) sectors and issues warnings, information on specific problems and tips for companies and private individuals. In the event of attacks on ICT at the national level, CERT.at GmbH coordinates the response to the incident and informs the respective network operators and the responsible local security teams.

The CERT.at team primarily responds to acute security threats and incidents. In this way, CERT.at can be considered an "internet fire brigade" for all of Austria, operating in its field of activity, conducting ongoing monitoring, sharing information, networking nationally and internationally, and responding to threats. Ultimately, CERT.at GmbH is also responsible for preventive measures, such as early detection, preparation for emergencies, public relations and consulting. CERT.at GmbH sees itself as a point of contact for security-related ICT incidents in Austria and thus serves as a trustworthy and recognized information hub.

However, the domain owners are not placed under general suspicion, as insinuated by the complainant, but the sole aim of CERT's activities is the legally prescribed protection of Internet users from potential attacks and damage. In accomplishing these tasks, CERT.at GmbH is supported by nic.at GmbH. As an operator of an essential service, nic.at GmbH has also concluded a service agreement with CERT.at GmbH, under which CERT.at GmbH has undertaken to provide nic.at GmbH with services to secure the Internet infrastructure in Austria, in particular to provide services to prevent security-critical incidents in the ".at" zone (see Section 14 (6) NISG).

The processing objected to by the complainant relates to the support provided by nic.at GmbH to the activities of CERT.at GmbH in the routine scan of all domains ending in ".at" by the respondent. This scan is used to detect two specific, widespread security vulnerabilities and is carried out across the board in order to identify possible security risks at an early stage and to alert those affected to the existing danger. This activity corresponds to the statutory task and the task assigned to CERT.at GmbH by official notification.

In order to facilitate the technical implementation of these tasks assigned to nic.at GmbH and CERT.at GmbH by law, official notification and contract, nic.at GmbH provides CERT.at GmbH with a list of all domains ending in ".at". The list provided contains only domain names and under no circumstances the identity of any domain holders. The use of the list enables a seamless scan of the associated websites and is therefore necessary to detect all security risks relevant to the Austrian zone (".at").

Before the actual scan for vulnerabilities, the start page for the domains is retrieved first in order to obtain basic information about the existence of a web server and a presented TLS certificate. From a technical point of view, however, this is not "rummaging" but nothing more than a simple visit to the website, i.e. a call to the start page linked to the respective domain. For reasons of transparency, CERT.at GmbH leaves a signet in the log files (automatically created by the site operator) each time it visits, which is how the complainant was able to become aware of the visit in the first place. The complaint refers to these accesses.

Even in the event that a security vulnerability is discovered, the scans do not result in the processing of non-public data, such as the identity of the domain owner, but usually only to the reading of the owner of the affected IP address from publicly accessible registers and subsequent information of the owner of the IP address – who does not have to be identical with the domain owner, but is usually an Internet service provider – about the discovered security gap. In the context of the calls of the domain of the complainant, only publicly accessible web addresses had been visited in the interest of the person concerned; no other processing of domain-related data, in particular of owner or content data, had taken place.

The data processing in question (forwarding of a list of all domains under ".at" by nic.at GmbH; storage of this list by CERT.at GmbH) is carried out on the basis of the NISG. CERT.at GmbH has been authorized by the Federal Chancellery in accordance with § 15 para. 3 NISG and commissioned by official notification to act as a national CERT and to carry out the necessary data processing. CERT.at GmbH has been commissioned by nic.at GmbH to fulfil the legally prescribed tasks.

The processing in connection with the activities as a CERT is justified according to Art. 6 para. 1 lit. c, e and f GDPR, because it is necessary to fulfil an obligation imposed by an administrative decision and to carry out a task in the public interest and serves to protect the legitimate interests of both nic.at GmbH and CERT.at GmbH. A data processing agreement between nic.at GmbH and CERT.at GmbH has not been concluded for this purpose, since the processing is carried out in the role of a controller according to the GDPR.

The transfer of the list of all domains under ".at" by nic.at GmbH to CERT.at GmbH is a consequence of its task as an operator of essential services according to § 16 NISG. The processing of these data is provided for by law in accordance with § 14 para. 1 and 7 NISG. According to § 14 (7) NISG, computer emergency response teams are expressly authorized by law as data protection officers in accordance with Art. 4 (7) DSGVO to process personal data in accordance with § 9 (2) to (4) NISG insofar as this is necessary to fulfil the tasks in accordance with § 14 (2) NISG. In addition, the disclosure of the list is necessary to protect the legitimate interests of both nic.at GmbH and CERT.at GmbH; the overriding interests of the data subjects (= domain holders) do not conflict with this. The processing of the list by CERT.at GmbH is ultimately necessary and required to fulfil the tasks of CERT.at GmbH under the legally stipulated service agreement with nic.at GmbH, but in particular to fulfil its statutory obligations as a "CERT" under the NISG, which have been transferred by official decision.

Only publicly accessible URLs would be used in the interest of all Internet users, in particular also in the interest of the operators of the scanned websites. The weighing of interests pursuant to Art. 6 lit f GDPR would undoubtedly favour nic.at GmbH. The complainant's interests in the protection of his data and his fundamental freedoms do not stand in the way of such use, especially since only the domain itself, but not the associated owner data, was passed on and processed. The web addresses can be accessed by anyone, but no "rummaging" through the websites beyond the mere act of accessing them takes place. The purpose of leaving a signet in the log files of the visited page is to provide transparency and information to the site operator about the visit that has taken place.

Together with his statement, the respondent submitted the following enclosures:

- Decision of the Federal Chancellery regarding GZ BKA-188.007/0005-I/8/2019 of January 21, 2020, by which the Respondent was identified as an operator of essential services pursuant to Section 16 NISG, Enclosure ./1;
- Decision of the Federal Chancellery regarding GZ BKA-188.007/0001-I/8/2019 of March 14, 2019, by which the respondent was determined to be the national computer emergency response team pursuant to Art. 15 Par. 3 NISG and Art. 14 Par. 2 NISG, enclosure ./2;
- Agreement on commissioned data processing pursuant to Art. 28 GDPR between the respondent and the Republic of Austria, represented by the Federal Chancellery, dated September 24, 2000, under which the respondent processes personal data on behalf of and in accordance with the instructions of the Federal Chancellery on the basis of the "Agreement on the Establishment and Operation of a Computer Emergency Response Team (CERT) for Austria", Annex ./3;
- Decision of the commercial court of the Regional Court of Salzburg in 51 Fr 1944/21 v-2 of September 15, 2021, from which the spin-off of the "CERT.at" division of the respondent for the purpose of incorporation into CERT.at GmbH emerges, enclosure ./4;
- Confirmation of the Federal Chancellery regarding the transfer of the function of the national computer emergency response team from the respondent to CERT.at GmbH in accordance with § 15 para. 3 NISG dated January 28, 2022, reference number 2022-0.068.104, enclosure ./5;
- Service agreement between the respondent as the client and CERT.at GmbH as the contractor regarding the cleanliness of the.at zone, services for a secure internet in general, threat intelligence and incident response for the infrastructure of the nic.at group dated December 22, 2021, enclosure ./6.

3. Despite the fact that the statement of the respondent was submitted and the data protection authority granted the opportunity to be heard by the parties, the complainant did not submit any further comments by letter dated September 2, 2022.

B. Subject of the complaint

The subject of the complaint is whether the respondent violated the complainant's right to confidentiality by

- transmitted the domain ".....at" to CERT.at GmbH and
- granted access to personal data (name, address, telephone number, ...) of the complainant and domain owner of ".....at" without his permission or knowledge by means of the Whois database.

C. Findings of fact

1. The complainant is the domain owner of the domain ".....at".

Assessment of evidence: This is evident from the present complaint filed by the complainant on April 10, 2022 ("The domain '.....at' was registered as a 'private individual' (natural person) (~2002)...") as well as from the complaint filed by the same complainant against CERT.at GmbH, which is the data protection authority under GZ D124.0585/22 and here in particular from the correspondence between the complainant and CERT.at GmbH (Wolfgang Rosenkranz, Team Leader CERT.at) dated March 10, 2022 ("On Thu Mar 10 09:59:38 2022, gh@.....at wrote: Dear Sir or Madam! Please remove the domain: .....at from your scans.").

2. The domain .....at was registered in the name of the complainant as a natural person in approximately 2002. This means that the respondent is aware of the complainant's first and last name as well as his contact details, namely postal address and an e-mail address.

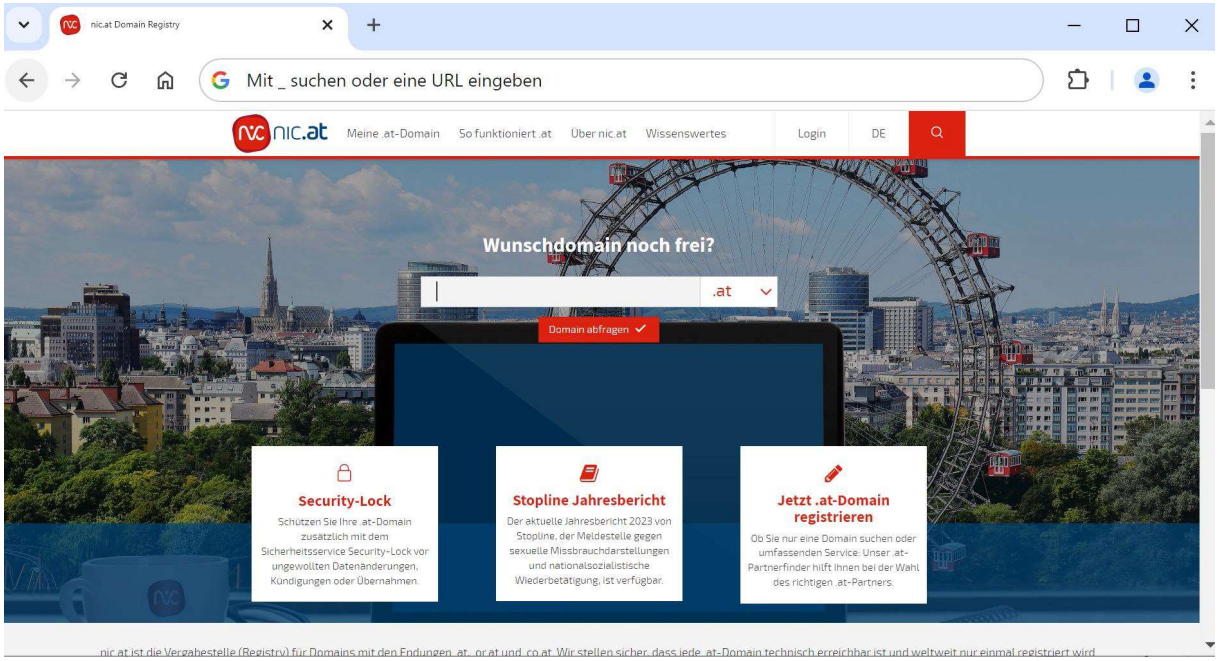
Assessment of evidence: This can be seen from the complainant's complaint of April 10, 2022 ("The domain '.....at' was registered as a 'private individual' (natural person) (~2002)") and from the data protection declaration submitted by the complainant together with his complaint and the data protection declaration of the respondent, which was retrieved ex officio on September 4, 2024 (see point 1.2, https://www.nic.at/de/wissenswertes/rechtliche-hintergruende/datenschutzerklaerung)

3.a. The respondent nic.at GmbH is the official (Austrian) registry for all domains with the top-level domain ".at" (as well as ".co.at" and ".or.at").

3.b. The Respondent is an operator of essential services (namely as an operator of authoritative DNS servers pursuant to § 10 para. 1 no. 2 lit. b of the Ordinance on Network and Information System Security (NISV) and as an operator of a TLD name registry pursuant to § 10 para. 1 no. 2 lit. c NISV) within the meaning of § 16 NISG.

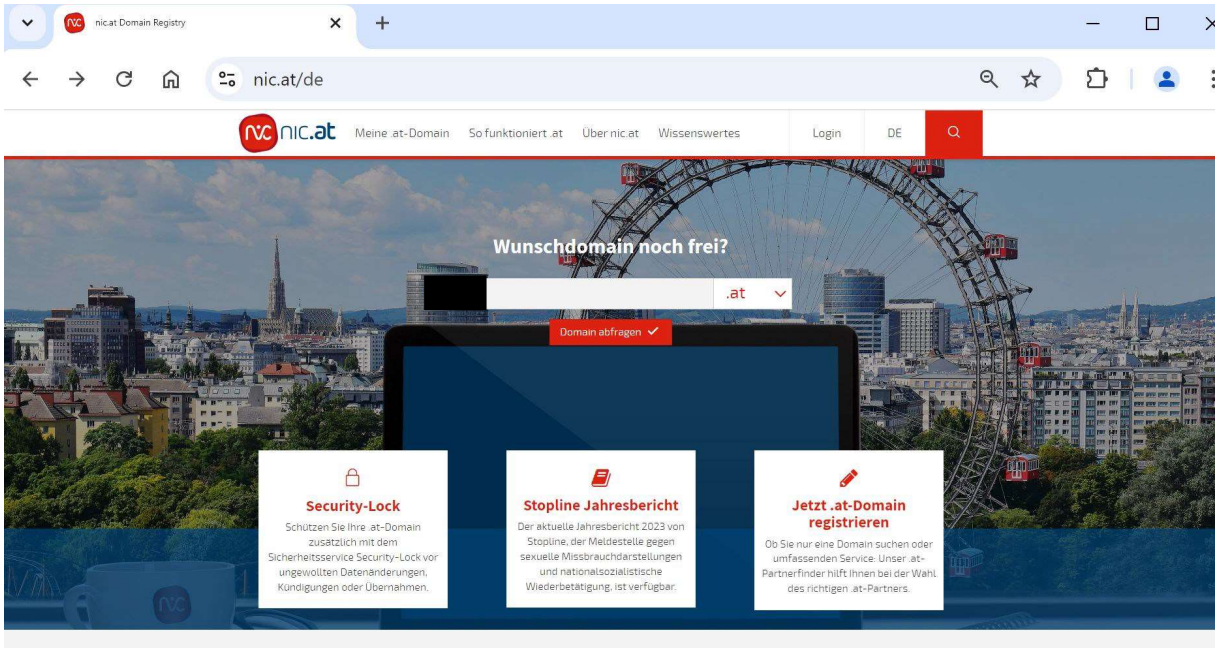
Assessment of evidence: This is evident from the response of the respondent dated April 28, 2022 and from the enclosure ./1, the decision of the Federal Chancellery regarding GZ BKA-188.007/0005-I/8/2019 dated January 21, 2020, by which the respondent is designated as an operator of essential services (namely as an operator of authoritative DNS servers pursuant to § 10 para. 1 no. 2 lit. b of the Network and Information System Security Ordinance (NISV) and as an operator of a TLD name registry pursuant to § 10 para. 1 no. 2 lit. c NISV) pursuant to § 16 NISG.

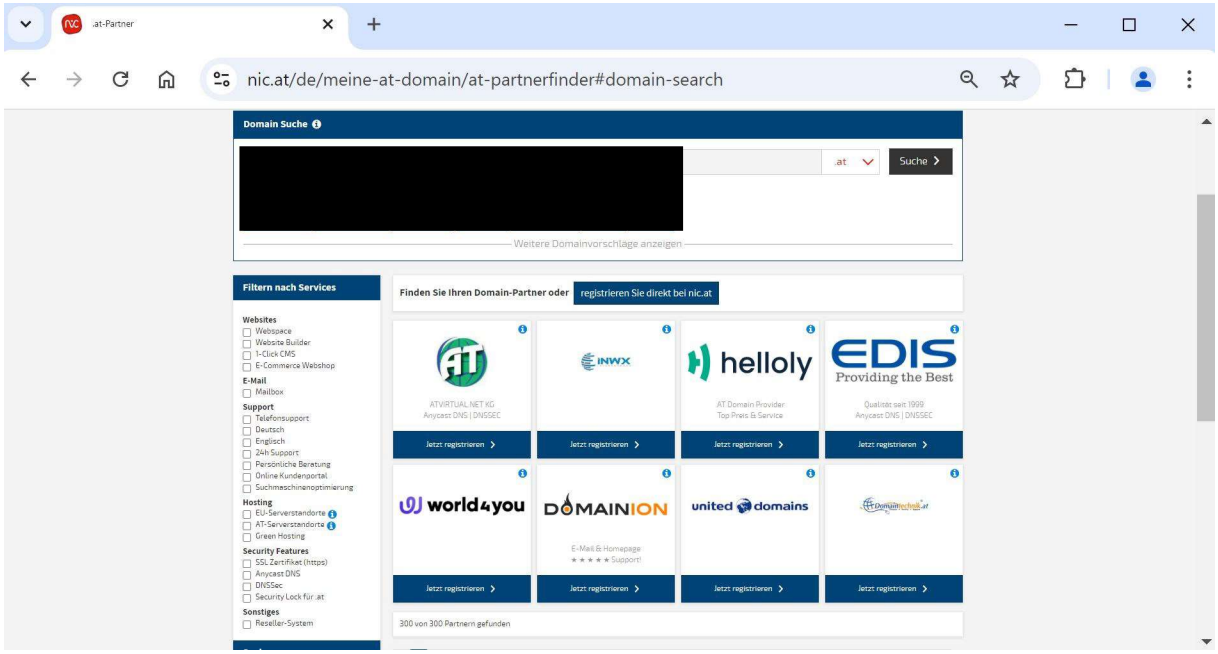
4. The respondent operates the website "www.nic.at", which can be used to query domains (see white box under the text "Wunschdomain noch frei?", in which the domain can be entered and red box "Domain abfragen" below it) and to find out whether a desired domain is still available ("Wunschdomain noch frei?").



Evaluation of evidence: This is evident from the official query of the respondent's website “www.nic.at” on September 4, 2024.

5. The query of the complainant's domain “.....at” on the respondent's website “www.nic.at” leads – as can be seen below – to the result that the domain “.....at” is already taken.





Assessment of evidence: This is evident from the ex officio query of the domain ".....at" on the website "www.nic.at" on September 4, 2024 (see "Unfortunately, the domain .....at is already taken").

6. The respondent also offers a whois query on its website "www.nic.at".

Assessment of evidence: This is the result of an official query of the respondent's website https://www.nic.at/de/meine-at-domain/domain-suche/whois#result on September 4, 2024.

7. The Whois is a public directory of registered.at domains that used to display all owner and contact data for all.at domains. Due to the applicability of the GDPR, the search options have been restricted as follows:

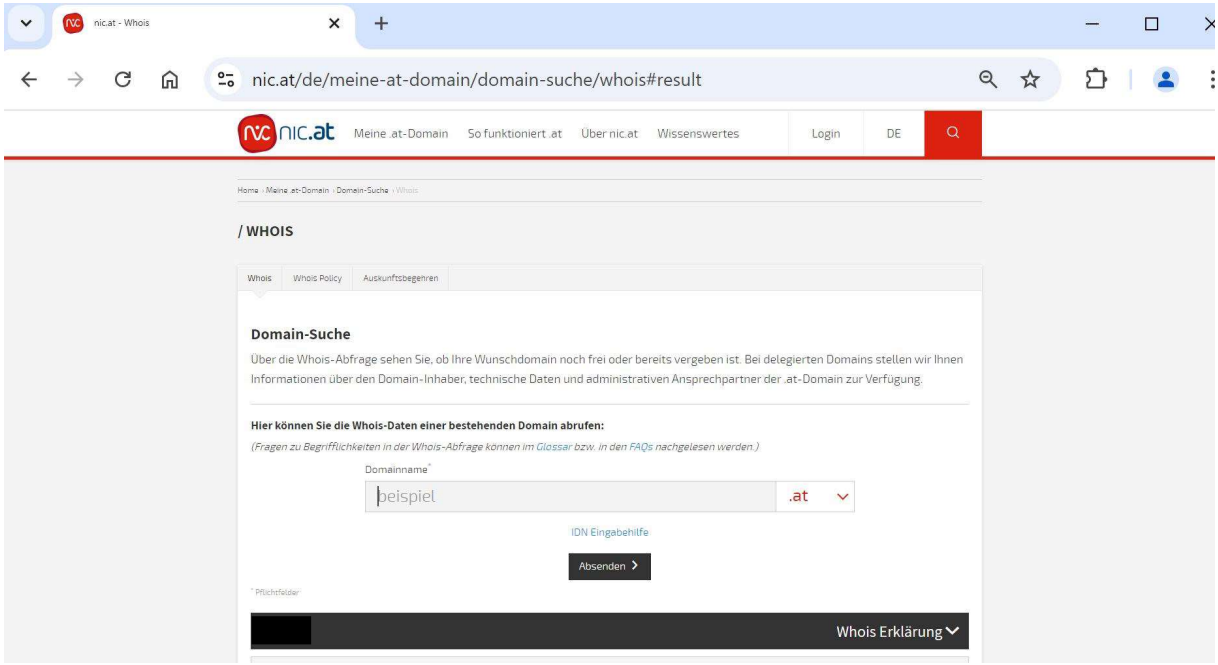
The owner data of legal entities continue to be published in the Whois.

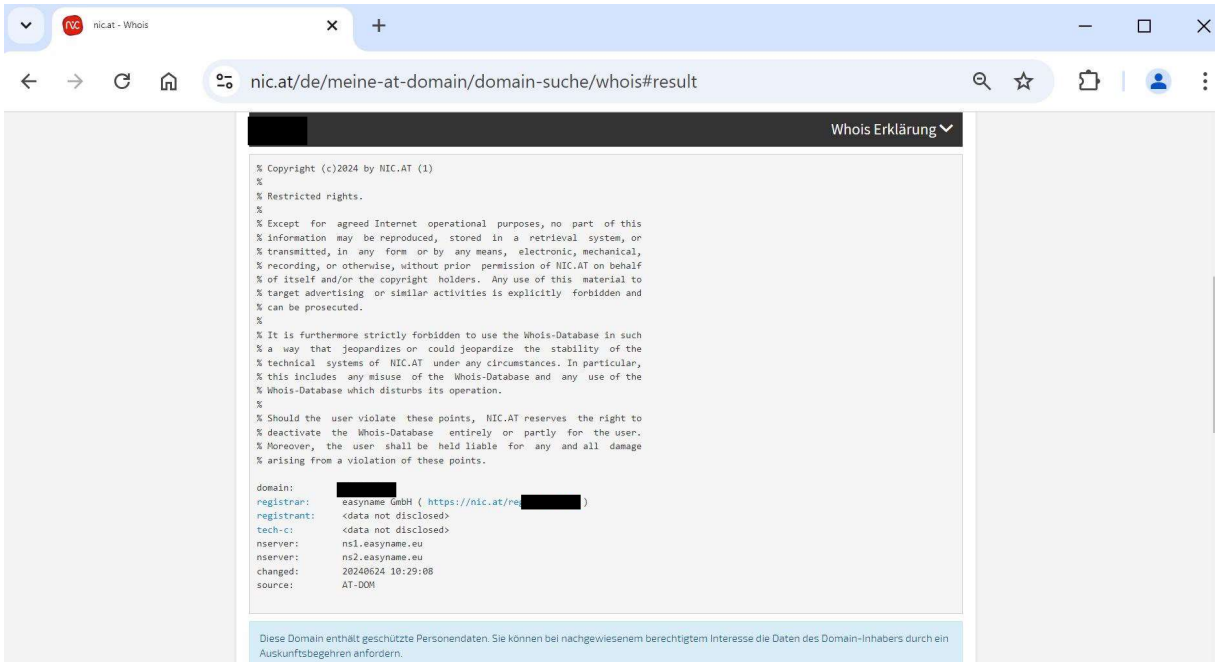
The owner data of natural persons are generally no longer published in the Whois. Owner data of natural persons only appear in the Whois at their express request. Disclosure of this owner data in individual cases is based solely on a specific request for information from a third party who must demonstrate a legitimate interest.

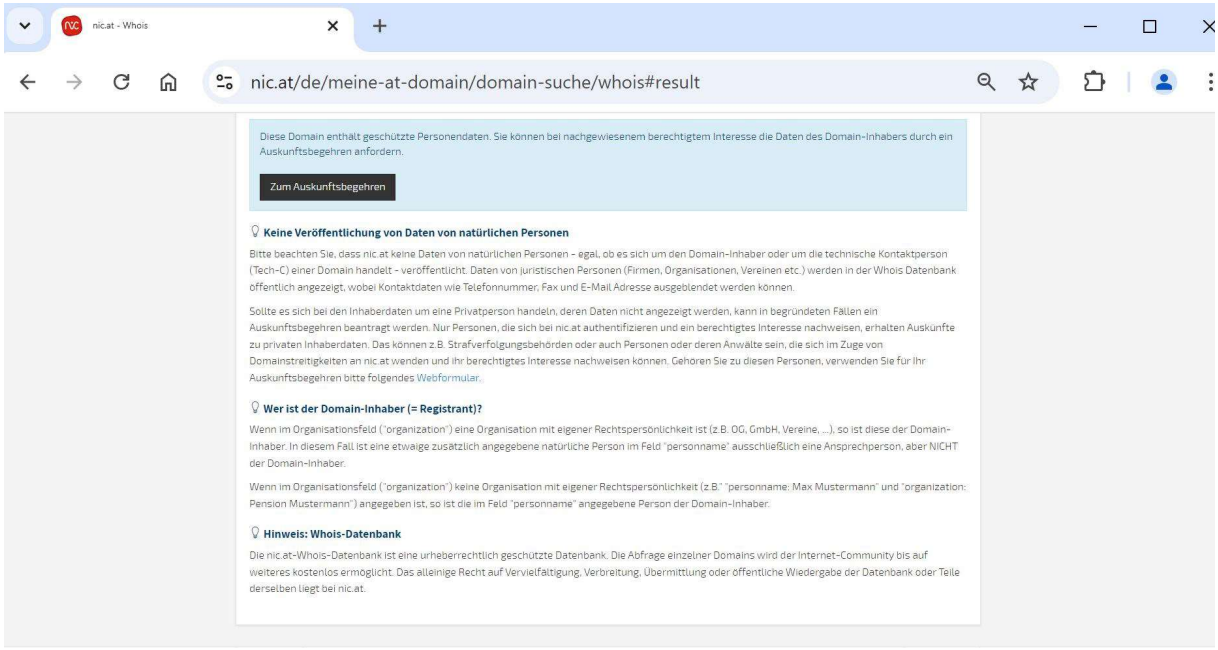
Assessment of evidence: This is evident from the data protection declaration of the respondent, which was submitted by the complainant together with his complaint and which was retrieved ex officio on September 4, 2024 (see point 1.9, Whois https://www.nic.at/de/wissenswertes/rechtliche-hintergruende/datenschutzerklaerung).

8.a. The whois query offered by the respondent for the domain ".....at" leads - as can be seen below - to the result that the registrar of the domain ".....at" is "easyname GmbH".

8.b. The registrant and domain holder of the domain ".....at", on the other hand, is not published as part of the whois query (see "data not disclosed"). The technical contact person (tech-c) for the domain ".....at" is also not published as part of the whois query (see also "data not disclosed").


nic.at - Whois
nic.at/de/meine-at-domain/domain-suche/whois#result
nic.at
Meine .at-Domain
So funktioniert .at
Über nic.at
Wissenswertes
Login
DE
Home › Meine .at-Domain › Domain-Suche › Whois
/ WHOIS
Whois
Whois Policy
Auskunftsbegehren
Domain-Suche
Über die Whois-Abfrage sehen Sie, ob Ihre Wunschdomain noch frei oder bereits vergeben ist. Bei delegierten Domains stellen wir Ihnen Informationen über den Domain-Inhaber, technische Daten und administrativen Ansprechpartner der .at-Domain zur Verfügung.
Hier können Sie die Whois-Daten einer bestehenden Domain abrufen:
(Fragen zu Begrifflichkeiten in der Whois-Abfrage können im Glossar bzw. in den FAQs nachgelesen werden.)
Domainname*
beispiel
.at
IDN Eingabehilfe
Absenden
* Pflichtfelder
[redacted]
Whois Erklärung


nic.at - Whois
nic.at/de/meine-at-domain/domain-suche/whois#result
[redacted]
Whois Erklärung
% Copyright (c)2024 by NIC.AT (1)
%
% Restricted rights.
%
% Except for agreed Internet operational purposes, no part of this
% information may be reproduced, stored in a retrieval system, or
% transmitted, in any form or by any means, electronic, mechanical,
% recording, or otherwise, without prior permission of NIC.AT on behalf
% of itself and/or the copyright holders. Any use of this material to
% target advertising or similar activities is explicitly forbidden and
% can be prosecuted.
%
% It is furthermore strictly forbidden to use the Whois-Database in such
% a way that jeopardizes or could jeopardize the stability of the
% technical systems of NIC.AT under any circumstances. In particular,
% this includes any misuse of the Whois-Database and any use of the
% Whois-Database which disturbs its operation.
%
% Should the user violate these points, NIC.AT reserves the right to
% deactivate the Whois-Database entirely or partly for the user.
% Moreover, the user shall be held liable for any and all damage
% arising from a violation of these points.
domain: [redacted]
registrar: easyname GmbH (https://nic.at/re[redacted])
registrant: <data not disclosed>
tech-c: <data not disclosed>
nserver: ns1.easyname.eu
nserver: ns2.easyname.eu
changed: 20240624 10:29:08
source: AT-DOM
Diese Domain enthält geschützte Personendaten. Sie können bei nachgewiesenem berechtigtem Interesse die Daten des Domain-Inhabers durch ein Auskunftsbegehren anfordern.



Assessment of evidence: The findings regarding the registrar, the registrant and the fact that the registrant is the domain holder are evident from the official query of the whois query offered by the respondent regarding the domain ".....at" on the website "www.nic.at" on September 4, 2024.

9. The function of the national computer emergency response team pursuant to Section 15 (3) NISG and Section 14 (2) NISG was originally assigned to the respondent.

Assessment of evidence: This is evident from the statement of the respondent dated April 28, 2022, as well as from the enclosure ./2 submitted at the same time, the decision of the Federal Chancellery regarding GZ BKA-188.007/0001-I/8/2019 dated March 14, 2019, by which the respondent was determined to be the national computer emergency response team pursuant to Section 15 (3) NISG and Section 14 (2) NISG, and from the also submitted enclosure ./3, an agreement on commissioned data processing pursuant to Art. 28 GDPR between the respondent and the Republic of Austria, represented by the Federal Chancellery, dated September 24, 2000, by which the respondent processes personal data on behalf of and in accordance with the instructions of the Federal Chancellery on the basis of the "Agreement on the Establishment and Operation of a Computer Emergency Response Team (CERT) for Austria".

10. The function of the national computer emergency response team pursuant to Section 15 (3) NISG and Section 14 (2) NISG has been transferred from the respondent to CERT.at GmbH as part of a demerger under company law.

Assessment of evidence: This can be seen from the enclosure ./4 submitted by the respondent together with its statement of April 28, 2022, a decision of the commercial court Salzburg Regional Court, 51 Fr 1944/21 v-2 of September 15, 2021, showing the spin-off of the "CERT.at" division of the respondent for the purpose of absorption into CERT.at GmbH, as well as enclosure ./5, a confirmation from the Federal Chancellery the transfer of the function of the national computer emergency response team from the respondent to CERT.at GmbH in accordance with Section 15 (3) NISG dated January 28, 2022, GZ 2022-0.068.104, enclosure ./5.

11. CERT.at GmbH is a wholly-owned subsidiary of the respondent nic.at GmbH.

Assessment of evidence: This is evident from the respondent's statement of April 28, 2022, as well as from an ex officio query of the commercial register on August 30, 2024 regarding CERT.at GmbH with the commercial register number 561772k. 12. nic.at GmbH, as an operator of an essential service, has also concluded a service agreement with CERT.at GmbH pursuant to Section 14 (6) NISG, under which CERT.at GmbH has undertaken to provide nic.at GmbH with services to secure the internet infrastructure in Austria, in particular services to prevent security-critical incidents in the ".at" zone.

Assessment of evidence: This also follows from the enclosure ./6 submitted with the present complaint, a service agreement between nic.at GmbH as the client and CERT.at GmbH as the contractor regarding the cleanliness of the.at zone, services for a secure internet in general, threat intel and incident response for the infrastructure of the nic.at group dated December 22, 2021.

13. The following information can be found in the respondent's data protection declaration:

“1.5 Our data recipients

(...)

In order to fulfill its legal and contractual obligations, nic.at also grants its subsidiary CERT.at GmbH access to the Whois database. CERT.at is, among other things, the Austrian national CERT (Computer Emergency Response Team), which is the point of contact for IT security (...)”.

Assessment of evidence: This can be seen from the data protection declaration of the respondent, which was submitted by the complainant together with his complaint and retrieved ex officio by the data protection authority on September 4, 2024 (see https://www.nic.at/de/wissenswertes/rechtliche-hintergruende/datenschutzerklaerung).

14. The respondent has submitted the domain '.....at' to CERT.at GmbH for the purpose of a routine scan. However, the respondent has not provided the name, address or telephone number or other personal data of the complainant to CERT.at GmbH.

Assessment of evidence: This is evident from the statement of the respondent dated April 28, 2022 (see page 5: “In the context of the calls of the complainant's domain, only publicly accessible web addresses were visited in the interest of the person concerned; no other processing of domain-related data, in particular of owner or content data, took place” and “The data processing in question (passing on of a list of all domains under “.at” by nic.at GmbH; storage of this list by CERT.at GmbH) is carried out on the basis of the Network and Information Systems Security Act (NISG)“; see also page 6: ‘The transfer of the list of all domains under ’.at” by nic.at GmbH to CERT.at GmbH is a result of its task as an operator of essential services in accordance with Section 16 NISG.”,). Despite a request from the data protection authority in a letter dated September 2, 2022, to submit a statement in the hearing of the parties, the complainant did not object to the statement of the respondent.

15. CERT.at GmbH scanned the complainant's domain “.....at” in any case on April 7, 2022 at 8:51:53 a.m. “Scanned” means that CERT.at GmbH accessed the ‘.....at’ website and checked it for security vulnerabilities.

Assessment of evidence: This is evident from the complaint filed by the same complainant against CERT.at GmbH, which is logged with the data protection authority under GZ D124.0585/22. The fact that CERT.at GmbH generally scans.at domains also follows from the enclosure ./6 submitted with the present complaint, a service contract between the respondent as the client and CERT.at GmbH as the contractor regarding the cleanliness of the.at zone, services for a secure internet in general, threat intel and incident response for the infrastructure of the nic.at group dated December 22, 2021.

D. From a legal point of view, the following conclusions can be drawn:

D.1. Legal bases

D.1.1. The right to confidentiality

In the present case, the complainant feels that his right to confidentiality has been violated.

Pursuant to § 1.1 of the Data Protection Act, everyone has the right to confidentiality of personal data concerning him or her insofar as there is a legitimate interest in such confidentiality. The existence of such an interest is excluded if data is not subject to a claim of confidentiality due to its general availability or because it cannot be traced back to the data subject.

D.1.2. The legal provisions of the Network and Information System Security Act (NISG) in the version published in Federal Law Gazette I No. 111/2018, where relevant, are reproduced here as follows (underlining by the data protection authority):

§ 2. Subject matter and purpose of the Act

This Federal Act lays down measures to achieve a high level of security of network and information systems of operators of essential services in the sectors of

1. energy,

2. transport,

3. banking,

4. financial market infrastructures,

5. healthcare,

6. drinking water supply and

7. digital infrastructure

as well as of providers of digital services and public administration bodies.

§ 9. Data processing

(1) The Federal Chancellor, the Federal Minister of the Interior, the Federal Minister of Defense, the Federal Minister for Europe, Integration and Foreign Affairs and the Computer Emergency Response Teams pursuant to § 14 para. 1 shall be authorized to process the personal data necessary to ensure a high level of security of network and information systems in the performance of their tasks under this Federal Act and to prevent and counter threats to public security data within the meaning of Article 4(2) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter: GDPR), OJ L 119 of May 4, 2016, p. 1, in the version of the correction OJ No. L 314 of 22.11.2016 p. 72, and § 36 of the Federal Data Protection Act (Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten - Datenschutzgesetz - DSG), BGBl. I No. 165/1999, and to transmit them to each other and to the members of OpKoord.

(2) This is the following personal data:

1. of participants and their organizational units, which are necessary to enable and in the course of participation in the coordination structures for organizational purposes;

2. of persons associated with risks, incidents and security incidents for the purpose of discussing and updating the situation report prepared by the Federal Minister of the Interior, discussing the findings obtained in accordance with Section 13 (1) and (2), and supporting the Coordination Committee;

3. of persons who are involved in or affected by a business case.

(3) The Federal Chancellor, the Federal Minister of the Interior and the Federal Minister of Defense are entitled, for the purpose of analyzing and managing risks, incidents and security incidents, to process and transmit the following personal data to each other in addition to the data referred to in paragraph 2:

1. contact and identity data as well as technical data of the reporter and the contact person;

2. contact and identity data as well as technical data of persons associated with a report of a risk, incident or security incident, such as, in particular, victims and attackers.

(4) In order to fulfil their tasks under §§ 4 and 5, the Federal Chancellor and the Federal Minister of the Interior are entitled to process and transmit the following personal data to each other in addition to the data referred to in paragraphs 2 and 3:

1. contact and identity data as well as technical data of operators of essential services, providers of digital services, public administration bodies that have made use of the option under Section 22 (5), computer emergency response teams and competent authorities of other Member States;

2. contact and identity data and technical data of persons associated with a report of a risk, incident or security incident, such as, in particular, victims and attackers;

3. contact and identity data of participants and their organizational units, which are necessary to enable and facilitate participation in EU-wide, international and national bodies for the security of network and information systems;

(…)

§ 14. Tasks and purpose of the computer emergency teams

(1) Computer emergency teams are set up to ensure the security of network and information systems. To this end, the national computer emergency team and sector-specific computer emergency teams support operators of essential services and digital service providers, as well as the public administration computer emergency team (GovCERT), in managing risks, incidents and security incidents.

(2) The CERTs pursuant to subsection 1 shall in any case have the following tasks:

1. receiving reports on risks, incidents or security incidents pursuant to §§ 19, 21 para 2 and 23 para 1 and 2;

2. forwarding reports (no. 1) to the Federal Minister of the Interior;

3. issuing early warnings, alerts and recommendations for action, as well as publicizing and disseminating information about risks, incidents or security incidents;

4. initial general technical support in responding to a security incident;

5. monitoring and analyzing risks, incidents or security incidents, as well as assessing the situation;

6. participating in the coordination structures pursuant to § 7 and participating in the CSIRTs network.

(…)

(6) Computer emergency response teams may also perform the tasks pursuant to subsection 2 nos. 3 to 5 for other entities or persons if they are affected by a risk or incident of their network and information systems.

(7) As controllers under data protection law pursuant to Article 4(7) of the GDPR, the computer emergency response teams are authorized to process personal data pursuant to Section 9(2) to (4) to the extent necessary to fulfill the tasks pursuant to subsection 2.

(…)

Section 15. Requirements and eligibility of a computer emergency response team

(…)

(3) The Federal Chancellor, in agreement with the Federal Minister of the Interior, shall determine that the national computer emergency response team and, upon application, a sector-specific computer emergency response team, fulfills the requirements pursuant to paragraph 1 and is suitable to perform the tasks pursuant to § 14 para. 2. Insofar as a Computer Emergency Response Team is a private institution, it shall be authorized by the Federal Chancellor in agreement with the Federal Minister of the Interior to fulfill the tasks pursuant to § 14 para. 2 subparas. 1 and 2. Computer Emergency Response Teams shall immediately notify the Federal Chancellor of any changes regarding the circumstances that were a prerequisite for determining suitability or granting the authorization. The authorization shall be revoked in its entirety or only with regard to the fulfillment of individual tasks if a prerequisite for the granting of the authorization is no longer met.

(…)

§ 23. Voluntary Reporting

(1) Risks and incidents may be reported by operators of essential services or digital service providers to the computer emergency team responsible for them, which forwards the reports in summary form to the Federal Minister of the Interior.

(…)

(4) The voluntary report need not include the identity of the organization or any information that might lead to its identification. Section 19 subsection (3) shall apply mutatis mutandis.

(5) In order to contribute to ensuring a high level of security of network and information systems, the voluntarily reporting entity pursuant to subsections 1 and 2 may transmit personal data pursuant to Section 9 (3) item 2 to the competent CERT.

D.2. Transfer of the domain ".....at" from the Respondent to CERT.at GmbH

As stated in C.14. and C.15., the respondent transferred the domain ".....at" to CERT.at GmbH for the purpose of a routine scan for security vulnerabilities.

In this context, it should be noted that the scope of data protection law (GDPR and DPA) applies if the processing of personal data within the meaning of Art. 4 no. 1 GDPR is involved. The domain ".....at" does not contain any personal data of the complainant, such as his name. Since the mere domain ".....at" cannot be traced back to the complainant, the domain ".....at" as such does not constitute personal data within the meaning of Art. 4 no. 1 GDPR.

As also stated in C.14., the respondent did not provide CERT.at GmbH with the name, address, telephone number or other personal data of the complainant. Thus, overall, no processing of the complainant's personal data took place. The scope of application of data protection law is therefore not established. The complaint was therefore to be dismissed for this reason alone.

D.3. The provision of access to the complainant's personal data by the respondent to CERT.at GmbH via a Whois query

The complainant also considers his right to privacy to have been violated because the respondent, according to its own data protection declaration (see point C.13.), grants CERT.at GmbH access to the whois database operated by the respondent. However, the complainant was not informed about CERT.at GmbH's access rights.

Although the respondent – as stated under C.7. – does not, in principle, publish any personal data of domain holders (unless this is explicitly requested by domain holders), the domain '.....at' – as stated under C.2. – was registered in approximately 2002 to the complainant as a natural person. Since the registration took place in 2002, long before the GDPR came into force in May 2018, when the data of natural persons were no longer published by the respondent in Whois, it can be assumed that the respondent is in any case aware of the name and contact details of the complainant. If the respondent grants CERT.at GmbH access to the Whois database, the CERT.at GmbH can therefore also access the name and contact details – and thus personal data – of the complainant by means of a Whois database.

It should be noted here that such access to the complainant's personal data constitutes a "processing" of personal data within the meaning of Art. 4 no. 2 GDPR, which also includes, for example, the storage, retrieval and use of personal data.

Now, restrictions on the right to confidentiality are generally permissible under Section 1 (2) of the Data Protection Act if the use of personal data is in the vital interest of the data subject or with his or her consent, in the case of overriding legitimate interests of another or if there is a qualified legal basis.

The GDPR and in particular the principles enshrined therein must be taken into account when interpreting the right to confidentiality (see the decision of the Data Protection Officer of October 31, 2018, GZ DSB-D123.076/0003-DSB/2018).

In particular, in order to be lawful, any data processing must, in addition to the principles of data processing pursuant to Art. 5 GDPR, (at least) fulfill a legal basis pursuant to Art. 6 GDPR (see, for example, ECJ of May 4, 2023; C-60/22, para. 57).

In the present case, the legal basis for accessing the complainant's personal data is Article 6(1)(c) of the GDPR (compliance with a legal obligation).

D.3.1. Legal basis: Article 6(1)(c) of the GDPR (compliance with a legal obligation)

According to Article 6(1)(c) GDPR, processing is lawful if processing is necessary to fulfill a legal obligation to which the controller is subject.

Pursuant to Section 2 NISG, the aim of the NISG is to achieve a high level of security for network and information systems of operators of essential services, including in the digital infrastructure sector.

As stated in 3.b., the Respondent is an operator of essential services (specifically, an operator of authoritative DNS servers and an operator of a TLD name registry) within the meaning of § 16 NISG.

DNS stands for Domain Name System. The DNS works similarly to the internet's telephone book: it manages the assignment between names (namely domain names) and numbers (IP addresses). DNS servers resolve domains (such as “example.at”) into IP addresses (such as “131.130.249.233”) when a DNS query is made.

TLD name registry stands for top-level domain name registry. The top-level domain is the abbreviation at the end of a domain name, e.g. “.at” for the domain name “www.beispiel.at” or “.com” for Domain name “www.example.com”. TLD name – registry refers to a registry or database of all domain names with a specific top-level domain. The Respondent nic.at GmbH is – as stated under C.3.a. – the official (Austrian) registry for all domains with the top-level domain “.at” (as well as “.co.at” and “.or.at”).

As stated under C.9., the function of the national Computer Emergency Response Team pursuant to § 15 para. 3 NISG and § 14 para. 2 NISG was originally assigned to the Respondent.

As further stated under C.10., CERT.at GmbH is now the national Computer Emergency Response Team (CERT) within the meaning of Section 15 para. 3 NISG and Section 14 para. 2 NISG.

The national computer emergency response team, CERT.at GmbH, supports the respondent in ensuring the security of network and information systems (see Section 14 (1) NISG). One of the tasks of the national computer emergency response team is to monitor and analyze risks, incidents or security incidents in accordance with Section 14 (2) (5) NISG. Pursuant to Section 14 (7) NISG, CERT.at GmbH is authorized to process personal data in accordance with Section 9 (2) to (4) NISG, insofar as this is necessary to fulfill the tasks pursuant to Section 14 (2) NISG.

This means that CERT.at GmbH may process personal data in order to fulfill its tasks, such as monitoring and analyzing risks, incidents or security incidents.

As stated under C.14. and C.15., the respondent submitted the domain “.....at” to CERT.at GmbH for a routine scan for security vulnerabilities.

The forwarding of the domain “.....at” to CERT.at GmbH was thus carried out in accordance with § 14 para. 1, para. 2 subpara. 5 in conjunction with § 9 paras. 2 to 4 NISG and was therefore legally covered.

If the complainant feels that his right to privacy has been violated in that the respondent granted CERT.at GmbH access to the complainant's personal data via the Whois database, the following must be stated:

It should be noted that the complainant in the present case has not complained about CERT.at GmbH accessing his personal data beyond accessing the domain “.....at” – which the respondent would have made possible by granting access rights to the Whois database.

Nevertheless, it is noted that the processing of personal data – including the data of the complainant – by the national computer emergency team, CERT.at GmbH, is provided for by law in sections 15, 14 and 9 subsections 2 to 4 NISG. Also, the respondent, as an operator of essential services pursuant to section 23 subsection 5 NISG, is

legally authorized to demand from the national Computer Emergency Response Team to transmit certain personal data – namely contact and identity data as well as technical data of persons associated with a report of a risk, incident or security incident, in particular victims and attackers, in accordance with Section 9 (3) (2) NISG – in order to help ensure a high level of security of network and information systems.

In summary, the processing of personal data by the respondent as an operator of essential services and by CERT.at GmbH as the national computer emergency response team is necessary and therefore lawful due to legal obligations within the meaning of Article 6 (1) (c) GDPR, which arise from the NISG.

Thus, access to the complainant's personal data, which the respondent grants to CERT.at GmbH within the framework of the NISG by means of a Whois query, is also covered by a statutory exception.

For this reason, too, the complaint had to be dismissed.

APPEAL

An appeal against this decision may be lodged in writing with the Federal Administrative Court within four weeks of notification. The appeal must be submitted to the data protection authority and must include

- the designation of the contested decision (GZ, subject)

- the designation of the authority concerned,

- the reasons on which the claim of illegality is based,

- the request, and

- the information necessary to assess whether the appeal has been filed in time.

An appeal against this decision is subject to a fee. [.....]

September 11, 2024

For the Head of the Data Protection Authority: