Republik Österreich
Datenschutz behörde

Barichgasse 40-42
A-1030 Vienna
Tel.:+ 43-1-52152 302568

E-mail:dsb@dsb.gv.at

GZ:D155.018
2020-0.339.292

SachbearbeiterinMag. [redacted]

«Anrede»
«Titel»«Vorname»«Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße»«ON»
«Postleitzahl»«Ort»
«Land»

Data protection complaint (Art. 6 GDPR, Art. 13 GDPR, Art 14 GDPR)
[redacted] (IMI Nr.: A56ID 99607); Case Nr. 112370

by e-mail «emailadresse»

F I N A L D E C I S I O N

The data protection authority decides on the anonymous data protection complaint, received by the Slovenian supervisory authority on 1 February 2020, against [redacted] (opponent) for 1) an infringement of the right to information and 2) an infringement of the right to legality of processing as follows:

— The complaint is dismissed as unfounded.

Legal basis: Art. 6, Art. 12, Art. 13, Art. 14, Art. 51, Art. 56, Art. 57 para 1 lit. f, Art. 60 and Art. 77 GDPR regulation (EU) 2016/679, published in the Journal of the European Union Nr. L 119 from 4th of May 2016, p. 1.

R E A S O N I N G

A. Arguments of the parties and course of proceedings:

1. The austrian data protection authority was notified by the Slovenian supervisory authority according to Art. 56 iVm At.60 GDPR of 28 February 2020 on the basis of an anonymous complaint dated 1. February 2020, that the opponent in his Slovenian branch had monitored the internet use of employees with regard to the visited websites and the amount of data usage as well as their professional e-mails.

The specific statistics on Internet use, including the website domains, were available to employees for their own use. Furthermore, the employees were not informed of such processing in accordance with Articles 13 and 14 GDPR.

2. As this is a cross-border case, the Slovenian supervisory authority placed the case in the "Internal Market Information (IMI) System", which is used in the cooperation procedure to manage **cross-border cases** under the provisions of the GDPR. It turned out that the main establishment of the controller, [redacted], commercial register number [redacted], is at address [redacted], Austria, so that **the Austrian data protection authority is the lead supervisory authority** in this case pursuant to Article 56(1) GDPR. Due to the fact that the opponent [redacted] has further establishments in Member States of the European Union, in particular in Croatia, Hungary and Slovakia, the supervisory authorities of these countries had to be included as concerned supervisory authorities pursuant to Art. 4.22 DSGVO.

3. At the request of the Austrian data protection authority dated 28 February 2020, the opponent stated in its submission from 20 May 2020 that the opponent had obtained its IT infrastructure services from [redacted] (processor) and that this processor had automated personal log files on the proxy server for IT security reasons. Access to the Internet communication of the employees is only permitted for the course of investigations in case of malfunctions or for the detection of security incidents and requires an appropriate authorisation of selected department heads or managing directors. It was correct that the processor recorded the total volume of Internet traffic caused by the opponent's employees, i.e. the amount of data used for the purpose of billing between the opponent and the processor. It is also true that the Internet traffic caused by individual employees on the intranet was represented by a "traffic light system" to the respective employee, but it did not show the websites visited by the user or other content data. This system had been introduced by above-average Internet traffic due to significant problems in the past. Due to the Covid 19 pandemic, the entire traffic light system had now been removed from the opponent's intranet. All employees were informed about the traffic light system by the Group Data Protection Officer. With regard to the "statista" link, the opponent did not at any time commission the alleged monitoring or logging of the employees' websites accessed. The factual logging of the websites accessed was created by the processor for internal reasons and was limited to their employees. For this purpose, the necessary company works agreement had been obtained. Apparently, a misadjustment had led to an employee having accessed his own statistics. However, it was not possible to receive the statistics of another employee. The opponent had prompted the immediate deactivation of the "statista" link for its employees and the deletion of all recorded data. The concrete legal basis for the logging of the data generated by the respondent and the traffic light system is Art. 6 (1) (f) GDPR, according to which the opponent's legitimate interests outweigh, because of the billing of the internet connection between the opponent and the processor, which was dependent on the opponent's Internet usage. The traffic light system was used for easy self-regulation of the opponents employees. A data protection assessment had not been carried out because it had fallen

under the electronic communication tools under DSFA-A20 (WP29, guidelines on data protection impact assessment (DSFA) etc.). The opponent did not see the need for an assessment of data protection due to the lack of intervention-intensive design, the strict access rules and, because this did not involve systematic monitoring. With regard to the alleged monitoring of the e-mail communication by the opponent's staff, the opponent informed that such a communication had not taken place. The only access to user-related e-mail mailboxes was through a common support system in case of technical errors via a ticket system. The processor had confirmed that there were no requests for "opening" (inspection) in e-mail accounts by the opponent.

4.The respondent's comments were forwarded to the Slovenian supervisory authority on 17 July 2020.

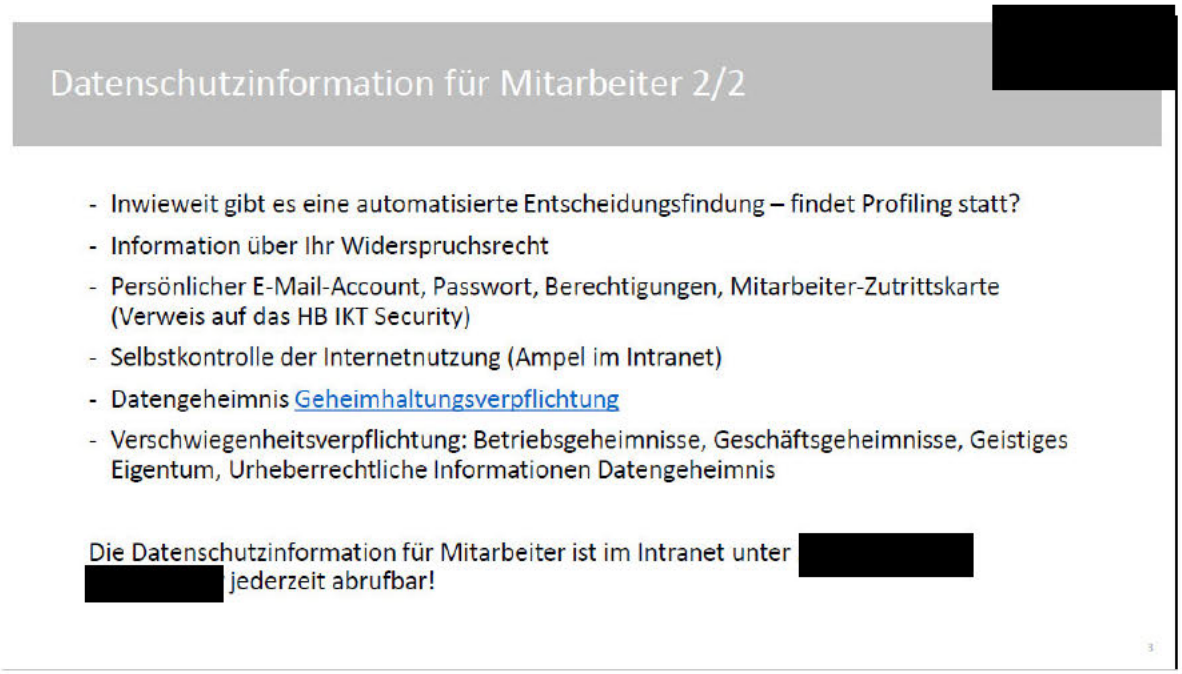
B. Subject of complaint

In the present case, the question arises as to whether the opponent's employees of the Slovenian branch have been infringed in their rights to information and whether the principles relating to processing of personal data and the lawfulness were infringed in accordance with Art. 6, Art. 12, Art. 13 and Art. 14 GDPR by monitoring the Internet use and the e-mail traffic oft he opponent's employees.

C. Findings of the case:

1.Within its group and in its Slovenian branch [redacted], banking subsidiary, [redacted], [redacted], the opponent has installed a "traffic light system" which was made available by its processor, [redacted], from which the opponent receives its essential IT infrastructure services, at least until 24 October 2019.This processor records the total volume of Internet traffic caused by the opponent's employees, i.e. by the opponent's IT systems, for the purpose of billing, since the opponent's billing results in gigabytes of internet volume per month and quarter. In addition, there have been considerable problems in the past due to above-average Internet usage by individual employees. Therefore, the traffic light system was introduced, which only indicates the generated Internet traffic of the individual employee and serves them for self-control.

2.The respondent's employees were informed about the traffic light system, which displays their generated Internet traffic by means of data protection information via intranet and in the context of mandatory data protection training, as well as the data protection information for opponent's employees:(Excerpt, formatting not returned 1:1):



Datenschutzinformation für Mitarbeiter 2/2

- Inwieweit gibt es eine automatisierte Entscheidungsfindung – findet Profiling statt?
- Information über Ihr Widerspruchsrecht
- Persönlicher E-Mail-Account, Passwort, Berechtigungen, Mitarbeiter-Zutrittskarte (Verweis auf das HB IKT Security)
- Selbstkontrolle der Internetnutzung (Ampel im Intranet)
- Datengeheimnis Geheimhaltungsverpflichtung
- Verschwiegenheitsverpflichtung: Betriebsgeheimnisse, Geschäftsgeheimnisse, Geistiges Eigentum, Urheberrechtliche Informationen Datengeheimnis

Die Datenschutzinformation für Mitarbeiter ist im Intranet unter [redacted] jederzeit abrufbar!

Erhebung von Daten aus anderen Quellen (Art. 14 DSGVO)

Überdies erlangen wir Daten aus unseren technischen Systemen der IT-Infrastruktur. Wir verarbeiten in diesem Zusammenhang folgenden Kategorien von Daten: technische Logdaten und Protokolldaten, nämlich Datum, Uhrzeit, E-Mail-Adresse von Sender und Empfänger oder Username, Nachrichtengröße von E-Mails und im Logfile der Internetnutzung (Proyx-Log) werden IP-Adresse, von der aus die Internetnutzung erfolgt, IP-Adresse des aufgerufenen Servers, abgefragte Seiten, Datenvolumen, Datum und Uhrzeit und Benutzername des abfragenden Benutzers protokolliert. Die Verarbeitung dieser Daten erfolgt auf Basis berechtigter Interessen im Rahmen einer Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO), wobei unser berechtigtes Interesse sowie die verfolgten Zwecke in der Abrechnung der IT-Dienstleistungen mit unseren IT-Dienstleistern, insb. der [redacted] der Aufrechterhaltung der IT-Sicherheit sowie der Verhinderung und Aufklärung von Straftaten oder schwerwiegenden Pflichtverletzungen liegen.

3.The Slovenian supervisory authority received complaints that the internet use and e-mail traffic oft he opponent's employees had been monitored by the opponent, which prompted the Slovenian supervisory authority to initiate proceedings and they carried out an on-the-spot inspection procedure at the opponent's Slovenian branch on 24 October 2019.

4. As part of the on-the-spot inspection procedure, it was found that the employees on the intranet under the title "Internet use" ("traffic light system") had an indicator of their own Internet use (*emphasis by the data protection authority, formatting not returned 1:1*):

[redacted]

INFORMATIONSPORTAL für [redacted]

Donnerstag, 24. Oktober 2019

STÖRUNG: Systemprobleme Kondor
ZBE, Fr. [redacted] 79936:
Systemprobleme Kondor
An der Störungsbehebung wird bereits gearbeitet.
Beginn der Störung: 24.10.2019, 10:08 Uhr

Verpflichtende PIN-Eingabe im SB-Bereich (Betrifft: Vertrieb)
ZBE, Hr. [redacted] 79467:
Seit 24.10.2019 ist es bei allen SB-Geräten (außer Münzeinzahlern) notwendig, dass der Karteninhaber sich mit der PIN identifiziert. Einzige Ausnahme: bei Einzahlungen - hier ist die PIN-Eingabe nicht notwendig.
Grund für die Änderung: Wahrung von Datenschutz und Bankgeheimnis; Schutz vor Missbrauch der Kundendaten

Checkliste Sicherheiten
ZKM, Fr. [redacted] 79129:
Die Checkliste Sicherheiten wurde im Punkt „Grundbücherliche Sicherheiten" ergänzt:
Bei der Erstfreigabe der Sicherheit ist nur das Feld "Datum GB-Prüfung" zu befüllen (die Felder „Prüfintervall" und „letzte Prüfung am" sind auf Grund der autom. Compasseinspielungen nicht zu befüllen).
Bei hypothekarischen Sicherheiten ob ETW ist zwingend auch das TOP im SICH aufzugeben. Bei noch nicht parifizierten Wohneinheiten, z.B. Bauträgerprojekten, können sich so die LBW-Schätzung und die entsprechende Sicherheit finden, wenn zwar die B-LNr. fehlt, aber das TOP in beiden Systemen aufgegeben ist.

Mittwoch, 23. Oktober 2019

Segmentierung FK & GK (KSM-Kampagne)

5. Statistics on the specific amount of data used by the respective employee and the average monthly use of the data at the level of the banking group are available under http://statistica/proxystats.There is also a link "Request Top Sites Report" (*formatting not returned 1:1, highlights by the data protection authority*):

[redacted]

Statistica

Ihre Internet-Nutzung

Internet-Datenvolumen Ihres Benutzers im aktuellen Monat

Benutzername	Datenvolumen in MB	Richtwert in MB (Median vom Vormonat)
yl95jer	1138	438

Detailreports ihres Benutzers anfordern

- Top Sites Report anfordern
- Private Top Sites Report anfordern

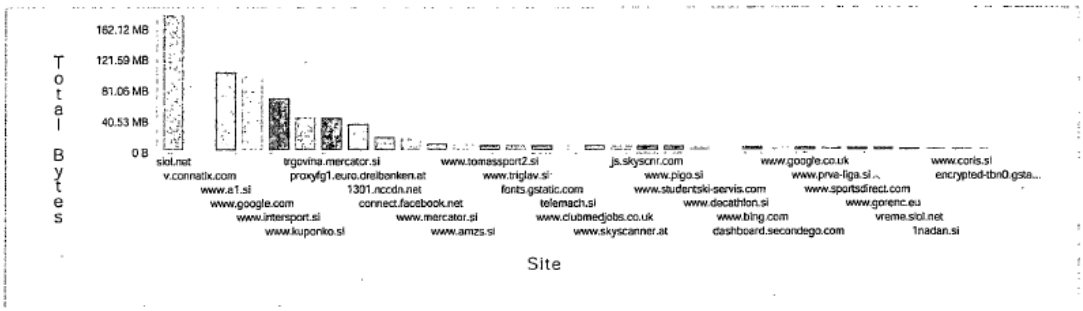
zurück zu Internet-Nutzungsstatistiken
Daten zuletzt aktualisiert am 24.10.2019 um 10:01:25 Uhr.
angemeldet als [redacted]
Statistica Version 1.0 - © 2011 3BEG, Ing. [redacted]

6.By clicking on the link ("Statista" link), an employee of the opponent was able to receive an e-mail with a PDF report on the websites he visited by himself. It was not possible to access reports from other

employees. The report only shows the main domain of the websites visited and not the specific websites. This link was not designed for the opponent's employees and was not commissioned by the opponent, but had been created by the processor for internal security reasons. In order to ensure traceability in the event of a security incident, which connections are made from which systems to the Internet, user name, IP address, searched pages, data volume, date and time have been stored in a "proxy log". The opponent was not aware of the "Statista" link. How the link reached an employee of the opponent can no longer be determined.

Top Sites Report - yl95jer: Calculated by Total Bytes

Symantec.



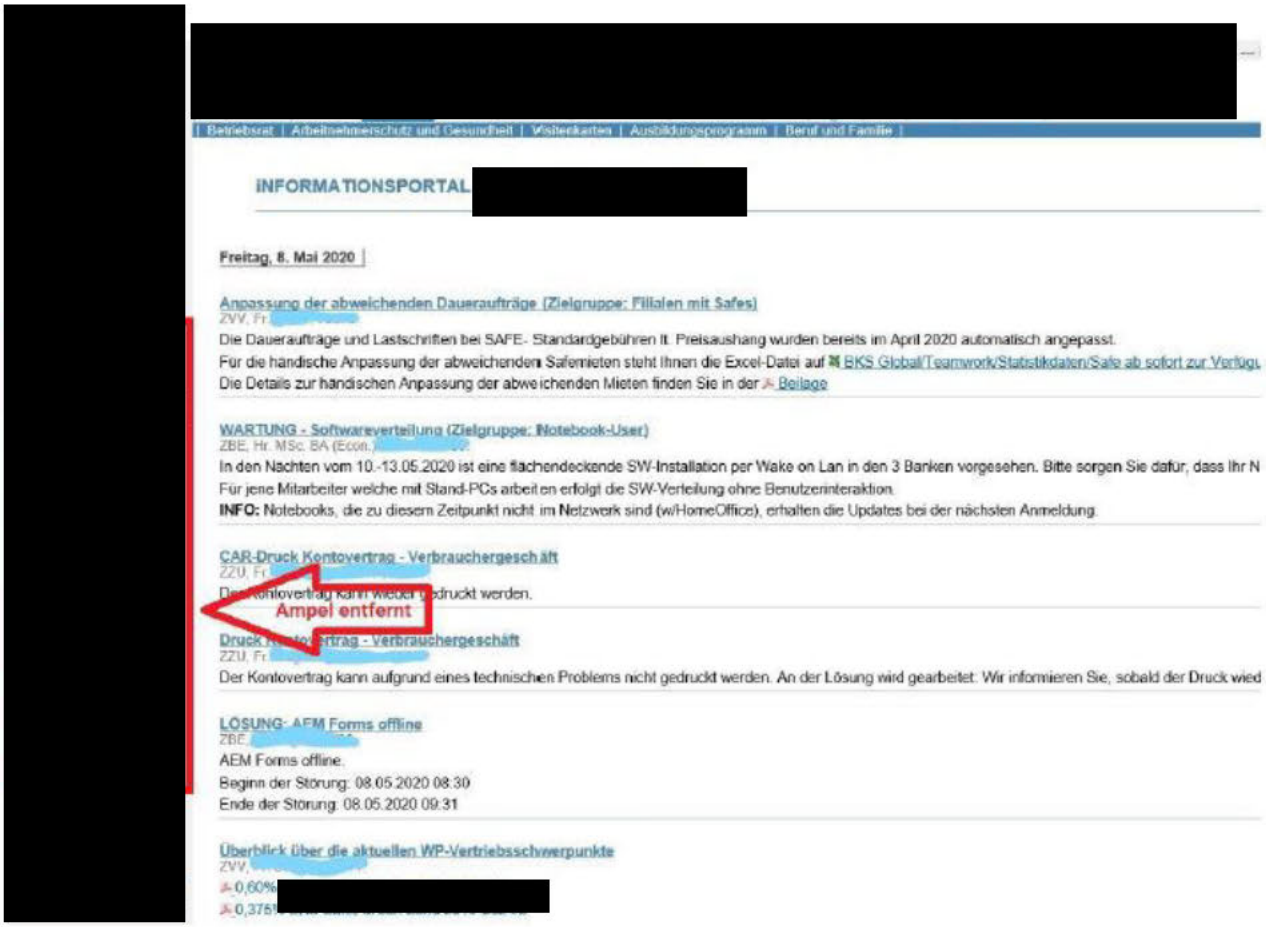
Report Filter: Date is Current and Previous 0 months (2019-10-01 - 2019-10-24) where Verdict is "allowed" and User is "yl95jer"

Site	Requests	Page Views	Total Bytes
siol.net	624	0	176.61 MB
v.connatix.com	4	0	131.01 MB
www.a1.si	4,016	27	103.67 MB
www.google.com	764	12	97.81 MB
www.intersport.si	3,224	154	70.02 MB
www.kuponko.si	1,223	25	45.67 MB
trgovina.mercator.si	9,840	58	45.50 MB
proxyfg1.euro.dreibanken.at	173	0	37.19 MB
1301.nccdn.net	608	0	20.57 MB
connect.facebook.net	366	0	18.78 MB
www.mercator.si	826	23	12.36 MB
www.amzs.si	293	9	11.26 MB
www.tomassport2.si	560	107	10.44 MB
www.triglav.si	501	3	10.05 MB
fonts.gstatic.com	454	0	9.83 MB
telemach.si	145	8	9.74 MB
www.clubmedjobs.co.uk	165	8	9.66 MB
www.skyscanner.at	898	25	9.13 MB
js.skyscnr.com	458	0	8.92 MB
www.pigo.si	2,259	87	8.89 MB
www.studentski-servis.com	70	0	8.25 MB
www.decathlon.si	265	23	8.10 MB
www.bing.com	51	0	7.79 MB
dashboard.secondego.com	351	81	7.53 MB
www.google.co.uk	22	0	7.37 MB
www.prva-liga.si	1,044	13	6.93 MB
www.sportsdirect.com	50	0	6.92 MB
www.gorenc.eu	500	13	6.84 MB
vreme.siol.net	2,322	0	6.50 MB
1nadan.si	372	2	6.33 MB

Top Sites Report - yl95jer, Page: 1
Generated by queryuser via Symantec Reporter on 24/Oct/2019

7.As of May 19, 2020, the "Statista" link was deactivated and the resulting evaluations were deleted.

8.As of 8 May 2020, the “traffic light syste,” on the opponent’s staff’s intranet was removed (*formatting not 1:1; highlights by the opponent*:



9.The only access to user-related e-mail mailboxes by others is within the framework of a usual support system, where employees can report technical errors via a ticket system. The access to the e-mail mailboxes of the opponent’s employees is only possible via the processor, which needs this access option in order to eliminate any IT malfunctions. For 2019, the processor has not received requests for “opening” (inspection) in e-mail accounts by the opponent, neither from the main establishment nor from the opponent’s branches abroad.

Appraisal of evidence: The evidence of the uncontested facts were taken from the submissions of the Slovenian supervisory authority and the respondent. The findings on points 6, 7 and 8 are based on the credible written statements of the processor.

D. Legal conclusions:

A. General information:

1.On accountability iSd.Art. 4 subpara 7 GDPR

This is a cross-border procedure, which must be handled in accordance with the provisions of the GDPR. The opponent's main office is [redacted], company book number[redacted], address [redacted]r [redacted] Austria so that the Austrian data protection authority is the leading supervisory authority in accordance with Article 56(1) of the GDPR. The Austrian opponent is the head office of the group, which makes the main management decisions for the purposes and means of processing the personal data of its employees in the branches in Austria, Slovenia, Slovakia, Hungary and Croatia. The opponent is, therefore, the responsible party according to Article 4 (7) GDPR.

2.On the existence of personal data:

Personal data according to Art. 4 (1) GDPR is all information relating to an identified or identifiable natural person. Identifiable shall be considered to be a natural person who is directly or indirectly expressing the physical or social identity of that natural person, in particular by assigning it to an identifier such as a name [...] or to one or more specific characteristics, which are an expression of the physical [...] or social identity of that natural person.

In the case of e-mails as well as the present „traffic light system" and the data of the "statista" link, through which the internet use of the respective employees is processed, it is undisputed personal data according to Art. 4 (1) GDPR, since the individual employees, or their Internet usage, are identifiable.

B. On the alleged breach of the duty of information pursuant to Art. 13 and Art. 14 GDPR:

In the present case it was claimed that the employees were not informed about the processing of their Internet usage data.

Art. 13 and 14 GDPR are to be understood as the basis for the data subject's rights in accordance with Chapter III (rights of the data subject) GDPR, since the data subject first learns that data is processed by a particular controller about him/her. Also the Recital 60 GDPR refers to the principle of fair and transparent processing, which enables the data subject to be informed of the existence and purposes of the processing process. The importance of informing the parties concerned is also emphasised by the ECJ in its case law (cf. on the legal situation under Directive 95/46/EC the judgment of 1 October 2015, C-201/14).

The date to inform the data subject is according to Art 13 (1) GDPR the time when the personal data is obtained. The date of the collection may also be when the person concerned knowingly gives data to

the person responsible (Knyrim *in Ehmann/Selmayr (ed.)*, General Data Protection Regulation, Art. 13, Rz. 11).

While Art. 13 GDPR regulates the case that the data is collected directly from the data subject, Art. 14 GDPR regulates cases in which the data is not collected from the data subject (Knyrim *in Ehmann/Selmayr (ed.),* General Data Protection Regulation*,* Art. 14, Rz 2).

The opponent was able to provide credibly and substantiate evidence that the employees have become aware of the “traffic light system” or the collection of their internet usage via intranet, as well as by the group data protection officer, in the context of an obligatory data protection training, as well as the general data protection information for employees of the processing of their data in a transparent and understandable manner pursuant toArt. 12 (1) GDPR. Thus, there is no violation of the right to information relating to the processing of employee data about their Internet use in accordance with Articles 13 and 14.GDPR.

C. On the legality of processing:

1.On the alleged monitoring of the Internet usage:

In accordance with Art. 6 (1) (f) GDPR, processing is lawful if the processing is necessary to safeguard the legitimate interests of the controller or a third party, unless the interests or fundamental rights and freedoms of the data subject which require the protection of personal data prevail.

As a result, a balance of interests must be carried out in accordance with Art. 6 (1) (f) GDPR. If the processing of the data in question was necessary to safeguard the legitimate interests of the controller or a third party, this may be justified unless the interests of the complainant outweigh. Consideration must be given to the content and significance of the data concerned as well as to the purpose of processing (*Buchner/Petri* in *Kühling/Buchner,* General Data Protection Regulation, Rz 149). Additionally the expectations of the data subject must be considered according to Rec. 47 of the GDPR, in particular whether the data subject reasonably had to expect further processing at the time of the collection of the data.

As stated, the basis for the billing between the opponent and its processor is the volume of Internet data consumed in the group. Therefore, there have been problems in the past due to above-average data use by individual employees.

The opponent’s legitimate interest in installing a system that warns employees at high data consumption through a traffic light system is to achieve the fairest possible balance of data consumption between employees and to introduce a cost-limiting measure by simple self-regulation. Especially since the opponent has provided Internet access for service purposes and the processor has credibly submitted that the evaluations of the website visits (“statista” link) of the individual employees were not

commissioned by the opponent, who had not even been aware of it. The statista link was only used for internal IT security purposes by the processor.

On the other hand, the employee's legitimate interests lie in the protection of their personal data in accordance with Art. 8 EU-CFR, whereby the employees could expect the processing in question for security purposes and cost limitations.

In the present case, the Austrian data protection authority considers the interests of the employees to be safeguarded and considers that the secrecy interest of the employees in their use of the Internet for work-related reasons should not be given more importance than the opponent's interest in limiting costs and fair balance between employees and the need of the processor to store the requested pages of the employees ("proxy log") for the purpose of IT security.

2.On the alleged monitoring of e-mail correspondence:

As stated, there are no concrete indications that in 2019 the opponent made use of its access to the e-mails of its employees via the processor who supervised the entire IT infrastructure. Thus, the data protection authority could not find evidence of the monitoring of the e-mail correspondence through the opponent.

Pursuant to Art. 60.8 GDPR, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof. As stated, the complaint was anonymous, therefore the Slovenian supervisory authority is not obliged to notify the unknown complainant.

30. Juni 2021

Für die Leiterin der Datenschutzbehörde:

[redacted]