OFFICE FOR PERSONAL DATA PROTECTION

Lt. Col. Sochora 27, 170 00 Prague 7

tel .: 234 665 111, fax: 234 665 444

posta@uoou.cz, www.uoou.cz

* UOOUX00CQJ22 *

Ref. UOOU-04073 / 18-11

DECISION

Chairwoman of the Office for Personal Data Protection as an appellate body competent pursuant to § 2, § 29 and Section 32 of Act No. 101/2000 Coll., on the Protection of Personal Data and on the Amendment of Certain Acts and pursuant to § 10 and § 152 para. 2 of Act No. 500/2004 Coll., the Administrative Procedure Code decided on 21 September 2018

according to the provisions of § 152 par. 6 let. b) of Act No. 500/2004 Coll., Administrative Procedure Code, as follows:

Disintegration of the accused, the company

based

against the decision of the Office for Personal Data Protection ref. UOOU-04073 / 18-5

of 23 May 2018, is rejected and the contested decision is upheld.

Justification

The basis for initiating administrative proceedings on suspicion of committing a misdemeanor conducted

The Office for Personal Data Protection (hereinafter referred to as the “Office”) with the accused company

based

(hereinafter referred to as the "accused"),

the file material was collected as part of an inspection carried out on the accused by the inspector

Office of MVDr. František Bartoš and concluded with a protocol on the control of Ref. UOOU-08428 / 17-31 of 21 March 2018.

The file shows that the accused runs an e-shop as part of her business

and manages its customers' user accounts. Accused in this regard on August 27, 2017

informed the Office that on 25 August 2017 it had detected a breach of security in the management of personal data

data. These were to be user accounts that contained simple passwords. In systems

The accused was so-called "hashing of passwords", when passwords are stored in encrypted

form. However, the database in question was encoded by an older one, no longer in use today

way, the so-called

. According to the accused, steps were taken

to minimize the consequences of security breaches. Specifically, all passwords were reset

potentially compromised user accounts set up a year ago

, they were

the data subjects are informed in writing and the customer care center has also been strengthened.

1/5

, of which

records from

From the record of the security incident and the results of the internal investigation conducted by the accused

it appears that the security incident occurred on

when an unknown person stole

accused database of customer records. To then upload the file containing

database of customers charged to the server

  which contained personal data to the extent

name, surname, e-mail address, user account password and in some cases also

unlogged user. From the internal report below

phone number occurred on

it turned out that the incident involved

  contained

unique customer email address.

On the basis of the situation thus established, the administrative authority of the first instance considered that

the accused has not taken or implemented measures to ensure security of processing
personal data of their customers before unauthorized access in the period
at least from 31 December 2014 to August 2017 and as a result from 27 July
From 2017 to 25 August 2017, the above personal data was made available on the server
. The accused thereby violated the obligation stipulated in § 13 par. 1 of the Act
No. 101/2000 Coll., on the protection of personal data and on the amendment of certain acts, ie the obligation
take measures to prevent unauthorized or accidental access
to personal data, to their change, destruction or loss, unauthorized transfers, to their
other unauthorized processing as well as other misuse of personal data. From these
reasons was the decision of Ref. UOOU-04073 / 18-5 of 23 May 2018 (hereinafter referred to as
"Decision") found guilty of committing an offense under § 45 para. h) of the Act
No. 101/2000 Coll. and was fined CZK 1,500,000.
However, the accused challenged the decision in a timely manner. In it the decision, taking into account
allegedly almost absent justification, she described as completely unreviewable. Next, how
the accused considers that the fulfillment of the liberation conditions according to § 21 par. 1 should have been proved
Act No. 250/2016 Coll., on liability for misdemeanors and proceedings on them. That's why she suggested
annul the decision and stay the proceedings.
In this context, the accused mainly disputed the conclusion of the administrative body of the first
degree that if the consequence provided for in Section 13 (1) of Act No. 101/2000 Coll.
it means that the personal data controller has committed an offense. In fact
offense according to § 45 par. 1 let. h) of Act No. 101/2000 Coll., as the accused stated, there is no
nothing is stated about the consequence and it is therefore not clear how the administrative body of first instance
the conclusion has come. On the contrary, it is clear from the very wording of that provision that the obligation to
applies to the adoption of appropriate measures, and does not arise for the occurrence of liability
consequence significant. Liability for failure to take appropriate action shall also arise if
there will be no consequence and the very occurrence of the consequence says nothing about whether or not

the administrator has or has not breached an obligation. The result is, in the opinion of the accused,
in this case, the adoption or non-adoption of appropriate measures to protect personal data.
The accused further argued that the measures taken pursuant to Section 13 (1) of the Act
No. 101/2000 Coll. it must be appropriate to the nature and extent of the processing, the type and quantity
processed data and the purpose of the processing. It is therefore not an objective aspect, but
it is assessed for a specific case. Examining whether the liberation provision has been complied with is so
should be carried out in relation to conduct which preceded the defendant from failing to take action
according to § 13 of Act No. 101/2000 Coll. Liberation reasons, ie making every effort, would
then examined in relation to what conduct the accused had taken to fulfill the obligation.
The eligibility criterion for liberalization should therefore apply only to activities aimed at

to avoid the foreseeable consequence. Demand the accused to make every effort
according to her lawyer, it is in conflict with the text of the law, as it does not follow from any
legislation. In this context, the accused referred to a commentary on the law
No. 101/2000 Coll., according to which “measures are to ensure, taking into account the state of the art and the cost of
their implementation, an adequate level of security commensurate with the risks arising from
data processing and the nature of the data to be protected. "
Subsequently, the accused described all the organizational and technical measures she had taken
which has been implemented and their implementation monitored. Individual technologies
at the same time they should be updated or completely changed with respect to
technological progress. In this context, the accused objected that the decision had not been settled
with the existence of the measures taken and their critical evaluation and comparison has not been carried out. He has
therefore considered that the inadequacy of the measures taken had not been demonstrated. He considers you
appropriate to the purpose, nature and extent of the processing, the type and amount of data processed.
At the same time, however, the accused does not deny that a security incident occurred, but nevertheless
did not occur as a result of a breach of duty by the accused, but as a result of the actions of an unknown person.

This action could have been an unauthorized intrusion into the system from outside or an employee's excess
or the system vendor, which in the opinion of the lawyer cannot be attributed
accused.
The nature of the conduct which was described by the administrative authority at first instance as ongoing
tort, the accused stated that it was not clear when the measures taken would have ceased to comply with her
criteria presumed by law and when the illegal situation arose and then
end. With regard to technological development and implementation of new technologies occurs
the level of security of individual systems is constantly being strengthened and is also happening
to modify processes when working with personal data. If the duration of the infringement relates to part
the database that was the subject of the incident cannot be a permanent offense, as this database
it is no longer in the possession of the accused and the offense was completed at the time of the separation. In this
In this case, the liability for the offense would cease to exist due to his time
assessed the commission according to the previous valid regulation (Section 46, Paragraph 3 of Act No. 101/2000 Coll.).
The appellate body reviewed the decision in its entirety, including the previous process
its release and first dealt with the arguments of the accused.
In this context, however, considers it necessary, above all, to point out that the personal administrator
data which, as the statement of reasons for the decision has already stated, he has just accused
pursuant to the provisions of Section 13, Paragraph 1 of Act No. 101/2000 Coll., the application of which in this case
the obligation to take such measures as to prevent the unauthorized or
accidental access to, modification, destruction or loss of personal data, unauthorized
transfers, their other unauthorized processing, as well as other misuse of personal data
data. As part of this, he is also obliged to assess certain risks and fulfill other obligations
defined in Section 13, Paragraphs 3 and 4 of Act No. 101/2000 Coll., to which, for example, assessment also belongs
risks in relation to preventing unauthorized persons from accessing personal data, etc.
Therefore, a mere grammatical interpretation can clearly conclude that the original intention
that provision is to lay down the obligation to take certain measures. This, of course, must have

to the extent necessary to prevent the misuse of personal data, as set out in the provision
§ 13 of Act No. 101/2000 Coll. Therefore, if the incident in question occurs, this is necessary a priori
understood as a breach of the obligation in question.
3/5
The definition of the factual nature of the offense according to § 45 par. 1 let. h) of the Act
No. 101/2000 Coll. a trustee who fails to take or implement precautionary measures
security of personal data processing. It is also possible to refer to the argumentation
Of the Supreme Administrative Court on the issue of strict liability for administrative offenses
in the judgment no. 9 As 36 / 2007-59 of 24 January 2008, albeit in a different area of public law. From her
however, it can generally be concluded that the concept of security must be interpreted as a guarantee and not
only as the creation of certain conditions to ensure the desired state.
In other words, the controller, who did not prevent the leakage of personal data, did not secure
security of personal data processing so that the conditions set out in § 13 are met
Act No. 101/2000 Coll. and therefore committed an offense under § 45 para. h) of the Act
No. 101/2000 Coll. This is also necessary to understand the accused references to professional
literature. Accepting the accused's arguments would then lead to a complete denial of meaning, resp.
formalization of the security responsibilities of the administrator in relation to him
processed personal data.
As regards the specific circumstances of the case, the Appellate Body found that it was entirely
undoubtedly proven the theft of part of the database of customer records accused. How
When this occurred, the accused did not find out either over time or on the basis declared by her
updating the measures taken. It is therefore clear that the measures taken to safeguard
processed data did not meet the conditions set by Act No. 101/2000 Coll. Plus
given these circumstances, the measures existing at the time of the incident cannot be reliably
to evaluate, and therefore it is already conceptually excluded from the accused to admit liberation reasons according to § 21
par. 1

Act No. 250/2016 Coll., when it is required to prove all, ie the maximum effort that is

may be required.

However, the administrative authority of the first instance correctly assessed, in favor of the accused,

the moment the data leak was detected and the password reset proceeded, which eliminated the obvious, however

not in this context, a clear security vulnerability, such as

the time of termination of the illegal situation. It was only on this day that, in accordance with § 30 letter b)

and § 31 par. 2 let. c) of Act No. 250/2016 Coll. and also in accordance with the former § 46 para. 3 of the Act

No. 101/2000 Coll., to run a three-year limitation period. If, for example, an interpretation were accepted

accused, according to which the duration of the infringement must be applied to part of the database,

incident, it should be noted that the act has not yet been completed,

as this database is no longer in the possession of the accused, with all the consequences. From the other side

however, the mere fact that personal data has come into the possession of another person does not relieve the accused

her duties resp. responsibilities in relation to the data subject to processing,

which she performs, because she was their administrator and had just such an act or. condition

prevent. As the beginning of the illegal situation, it was, again in favor of the accused,

determined by the accused itself a defined date of theft of the database, as this theoretically

could be moved resp. extended to the date from which the measures constituting the

relevant security vulnerability.

For the sake of completeness, it can be added that the accused in question would be accused, resp. any administrator

or the processor committed even in a situation of complete absence of the measures in question or in a situation

taking manifestly insufficient measures without any security

incident, which is not the case.

The decision is then, albeit in a somewhat concise form, duly reasoned and with administrative conclusions

body of first instance, the appellate body shall identify itself. That with this justification accused

disagrees, cannot be understood as its absence, moreover, establishing the unreviewability of the decision.

At the same time, the new legislation contained in the European Parliament's regulation was assessed

and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to

processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC

(General Data Protection Regulation), however, as the Appellate Body found it does not

there is no effect on the assessment of the case.

The appellate body therefore rejected the defendant's arguments. After an overall review, then the appellate

the authority notes that it did not find any errors in the procedure of the administrative body of the first instance.

On the basis of all the above facts, he therefore decided as stated in the statement

of this Decision.

Lessons learned:

Pursuant to the provisions of Section 91 (1) of the Act, this decision shall be challenged

No. 500/2004 Coll., Administrative Procedure Code, cannot be revoked.

Prague, September 21, 2018

For correctness of execution:

official stamp imprint

JUDr. Ivana Janů, v. R.

chairwoman