Athens, 19-04-2018

AP: C/EX/2977/19-04-2018

PRINCIPLE FOR DATA PRIVACY

FOR OPIC CHARACTER

A P O F A S H 34/2018

(Department)

The Personal Data Protection Authority met in

composition of the Department at its headquarters on 22-11-2017 at 10:00 a.m. after

invitation of the President. The Deputy President, George, was present

Batzalexis, obstructing the President of the Authority, Constantinos Menoudakos,

and the alternate members Panagiotis Rontogiannis, Charalambos Tsiliotis and

Grigorios Tsolias, as rapporteur, replacing the regular members of Antonio

ymbon, pyridon of Vlachopoulos and Charalambou Anthopoulos, respectively, the

who, although legally summoned in writing, did not attend due to obstruction.

Present without the right to vote was Fereniki Panagopoulou, legal auditor

- lawyer, and Leonidas Roussos, IT auditor as assistants to the rapporteur

and Irini Papageorgopoulou, employee of the administrative affairs department,

as secretary.

The Authority took into account the following:

the Authority was forwarded the no. prot. G/EI /1872/21-03-2014

appeal document of A (hereinafter "the appellant") against the person in charge

processing company N. CRETE - G. DAIRTZE S.A. PAPER TRADE

(hereinafter "the company") which pertains to, without prior notification and art

in the absence of the applicant, conducting a check on the computer which

used in his professional field, as completed with the following

no. prot. G/EI /4985/14.8.2014, G/EI /5145/29-08-2014, G/EI /7850/12.12.2014,

G/EI /3102/02-06-2015, G/EI /6210/26-11-2015 and G/EI /882/06-02-2017 documents.

The Authority was also forwarded the no. prot. G/EI /7264/26-11-2014 and

G/EI /1467/07-03-2016 answering documents of the company

(note also

supplementary documents).

The appellant claims that he was employed as an assistant accountant in

company, which during his absence due to sick leave, since

he investigated the corporate computer that had been assigned to him

in order to provide his services, he then removed the hard drive

to further check it, to recover deleted files, without having

previously informed about it or without his consent having been obtained and

without being present during the hard disk removal process.

It was later reported that the hard drive was sent for inspection and recovery

of the data that had been deleted, according to the claims of the company and

immediately expressed objections to this action, pointing out that in

hard drive included his personal data, which he wanted

to have access, but the company refused to satisfy his request.

Following this refusal, the appellant sent her from ... "Court

"Protest-Invitation-Declaration" to the company in which on the one hand

complained about his lack of prior information and the lack of provision

consent to the removal of the hard disk as well as the processing of

of its contents, of its personal data, in which (processing)

resisted, requesting the interruption of the processing, on the other hand, requesting to

be informed of the full details of the persons who carry out processing

of those stored on the hard disk of the company computer,

of his personal data, the purpose of processing, their recipients

data and the time period during which the processing takes place

she. The appellant claims that, while he exercised in accordance with the above

rights arising from articles 11, 12 and 13 of Law 2472/1997, the company

refused to satisfy them.

on the contrary, the company maintains that the applicant was an employee

of until ... when he left voluntarily when he was discharged on the same date

of his duties, his father, B, as its President and Managing Director

company, following the resignation of D. . her, and denies his claim

2

applicant about his justified absence due to his sick leave.

Furthermore, the company maintains that the applicant together with his father

and other persons committed illegal and criminal acts against her

of her property, violating at the same time the duty of loyalty that is incumbent upon them

result, to unfairly benefit a competing company, in which they participated

already. For this reason, according to the company, it became necessary to check them

files of the computer in question and its hard drive was sent

to a specialized company in order to carry out search and recovery actions

any deleted files. In particular, as mentioned verbatim in the by...

"Extrajudicial Response Protest Statement Invitation with reservation of rights"

of the company against legal entities and natural persons, among which the

of the applicant (p. 9): "We found that his final job position from you A

and the computer located in this position had undergone an intervention

and all correspondence etc. records had been deleted from him. Transport him

computer to specialist typists but it has not been possible until today to

recover the deleted correspondence of the company for special orders

agreements etc.'

The company denies that it carried out illegal data processing

personal nature of the applicant arguing that from the control that

performed on the hard drive, no file found, either containing personal

data of the applicant, or containing data of any person,

personally or not. He claims that the appellant together with his father rushed

to remotely destroy email that was

stored on the hard drive in question so that they are not found

evidence of their illegal and criminal acts, since

saved correspondence related to customers, billing, balances, nuisances,

offers, moreover, all the traces of the passage from him would not appear

every one electronic mail computer and from electronic

address given to him by the company. Finally, the company claims that the

computer and any contained documents and files belong to

her property, that other employees also had access to it and that in

case in which the applicant had stored personal data

of him, such an action took place illegally, without his knowledge and approval

her.

3

The appellant refutes the above claims of the company and

denies that he remotely interfered with the computer at issue and

deleted files stored on it.

The company in turn claims that the disputed hard disk

sent to a specialized company for digital recovery of the deleted from

this data, he also attaches relevant data from 19-11-2014

electronic letter according to which “[…] after checking that

it happened on the two discs you sent us...we couldn't do it

data recovery because we found no data resulting in the disks not being

recoverable".

Finally, between the applicant, his father and the company there is

intense legal dispute on both sides, as can be seen from the documents which

were presented (lawsuits, insurance measures, lawsuits, etc.), for the purpose of each

part to support his claims.

With the nos. prot.

documents, the APDPH invited the company and the appellant to a hearing

Wednesday 13.9.2017 at 9.00 a.m., at the Authority's headquarters, Kifisias 1-3,

Ampelokipi, Athens,

floor, during which the

5th

under no. prot. C/EI /1872/21.3.2014 appeal of A against the company. The company

came through the representative of C and the attorney-at-law of Vasiliou

Urla and Eleftheriou Petritsopoulos. A came in person after her

power of attorney of Tylianis Tsakonas.

The applicant during the hearing and subsequently with the

under no. prot.

the other memos and documents he had sent to the Authority, he argued

that in principle he acknowledges that he is not the owner of the disputed electronic

computer, which belongs to the company and was allocated to him for the fulfillment of

of his work obligations, without ever being informed, either verbally or

in writing that it is prohibited to store his personal data on him

as the company does not have a relevant internal Regulation, nor was it included

relevant provision in the employment contract he signed, while he was never informed

about the possibility and possibility of the company's access to the electronic

computer he was using. Moreover, the appellant argued that he had

stored exclusively on the company computer simply and

sensitive personal data, as he lacked his own computer

in his home, nor had he kept a copy of the above files in

portable digital data storage devices or in storage

cloud computing. In addition, the appellant argued during the course

of the hearing and then with his reminder that he had created a separate one

electronic folder ("folder") with his name on the disputed electronic one

computer, where his personal data was stored, in order to

distinguished from the rest of the records relating to his work.

The applicant accepts that from time to time access to the disputed

his colleagues had a computer when he was absent, for that matter

to look for a file necessary for the company, without raising it himself

objections. During the hearing and subsequently in his memorandum the appellant

argued that the disputed computer was protected by a code, the

which he disclosed to his colleagues by phone, in case of his absence

from work, when there was a need for access for company needs.

The appellant accepts that he had no objection to any processing

of the files that related to his work and were stored in the litigant

computer and further stated that “Files or e-mails concerning

in my work they were not the subject of my current appeal, as

I know that on these professional files, the company is entitled to have

full access, which doesn't bother me at all."

The appellant accepts that he cannot prove it on his part

storage of personal data on the computer in question, nor

provides any evidence in support of the relevant

claim.

Finally, to refute the company's claim that his father

applicant, as president of the company, had granted, on his behalf

applicant, his consent regarding the control of the electronic

computer, the appellant replies that the consent of a third party is not understood,

nor supposed such.

The company during the hearing and subsequently with the no.

5

prot.

memos and documents he had sent to the Authority, he denied having done so

in illegal processing of the applicant's personal data and

admitted that he initially checked the computer in question

to find evidence of any illegal and criminal activity

acts against her. the context of the control of the disputed electronic

computer, the company claims that it has been found that its entirety has been deleted

saved file of the electronic mail and indeed ex

distance. Subsequently, his hard drive was removed from the company

computer and sent to a specialized company in order to recover them

deleted files, but without success, as can be seen from the content

relevant letter provided.

The company maintains that it was never informed by the applicant

for any storage of his personal data on his part

computer owned by her, nor was such storage found

data and that in any case he had the right of access to corporate

data that was stored on a company computer, as well as on

e-mail from and to a corporate e-mail address. Yes, yes

and, the company maintains that it had obtained the consent of his father

of the applicant, then president of the company, to check the disputed electronic

computer.

The Authority, after examining the aforementioned data, heard him

rapporteur and the assistant rapporteurs, who subsequently left, and

after thorough discussion,

The Authority taking into account in particular:

1. The provisions of the decree, and in particular those of articles 2 par. 1, 5 par.

1, 9A, 17, 28, and 25.

2. The provisions of article 4 par. 1 of Law 2472/1997, according to which

"[…] the personal data to be subject to legal processing

must: a) Be collected in a legitimate and legal way for specified,

clear and legitimate purposes and to be fair and lawful processing

in view of these goals b) To be relevant, appropriate, and no more

from what each time is required in view of the purposes of the processing. [...]".

3. The provisions of par. 1 of art. 5 of Law 2472/97, according to which the

processing of personal data is permitted in principle only

when the data subject has given his consent. However,

exceptionally, processing is permitted without his consent

subject, as long as one of the conditions provided for in par. 2 is met

cases of the same article.

4. The provisions of article 10 of law 2472/97 and in particular those of paragraph 3,

according to which the controller must receive the

appropriate organizational and technical measures for data security

and their protection against accidental or wrongful destruction, accidental loss,

alteration, prohibited distribution or access and any other form

unfair processing.

5. The provisions of par. 1 of art. 11 of Law 2472/97, according to which,

controller must, during the data collection stage

of a personal nature, to inform in an appropriate and clear manner

subject at least for the purpose of the processing and the recipients

of his data and in accordance with paragraph 2 of the same article to

requests the consent of the subject in writing.

6. The provisions of article 12 of Law 2472/97, according to which each

has the right to know whether personal data that

concern are or were the subject of processing. To this end, Mr

controller, has an obligation to respond to him in writing.

7. The provisions of article 13 of Law 2472/97, according to which the

data subject has the right to object to the

processing of data concerning it.

8. The provisions of Directive no. 115/2001 of the Protection Authority

Personal Data with regard to employee files.

9. The under no. 2/2017 Opinion of the Article 29 Working Group, on

processing of personal data at work (WP 249)

10. The Working Document of the Article 29 Working Group dated 5-29-2002

for the surveillance of electronic communications in the workplace

(WP55)

11. Under no. 8/2001 Opinion of the Article 29 Working Group on

processing of personal data in the context of work

relations (WP 48)

12. The Code of Ethics of the International Labor Organization for

protection of the personal data of its employees

1997.

13. , The under no. 2015/5 request of the Council of Ministers of 04-01-2015

for the processing of personal data in the context of

labor relations.

14. The under no. R (89)2 request of the Council of Ministers of 01-18-1989

for the protection of personal data received

processing in labor relations.

SEVEN E ACCORDING TO THE LAW

Access by the employer to personal data stored in

employee's computer constitutes processing of personnel data

character within the meaning of article 2 paragraph d of Law 2472/1997 (see

61/2004). In order for the above data processing to be legal

of a personal nature by the employer the conditions must be met

implementation of the provisions of articles 4, 5 and 11 of Law 2472/1997 as well as of

of the provisions of the Directive 115/2001 of the Labor Code on employee records

(regarding, see also Article 29 Working Group, Opinion 2/2017 on the processing

of data at work, WP 249, pp. 7 ff. and L. Mitrou, The protection

employee data in Leonidas Kotsali (ed.), Personal Data,

Analysis-holia-Application, Law Library, Athens 2016 p. 185 ff., especially

197 ff.)

In particular, the employer is entitled to inspect the stored

of data located on the employee's computer, among others

cases, and in that of subsection e' of paragraph 2 of article 5 of Law.
2472/1997, i.e. in the event that said access (processing) is
absolutely necessary for the satisfaction of the legitimate interest it seeks as
data controller and provided that this clearly outweighs the
rights and interests of the employee, without prejudice to the fundamental
liberties thereof (see APDPH 37/2007). The same legal basis is adopted by
recent ECtHR jurisprudence (see Barbulescu v. Romania decision of 09-05-2017

in broad composition, para. 127).
The satisfaction of the legal interest (for the relevant concept see Team
Work Article 29 Opinion 6/2014) that the employer seeks may
it consists, among other things, in the exercise of the directorship on his part
of right, from which derive the subsequent obligations of loyalty to him
him1 and from them the obligation to provide information to him is deduced
as well as the control of leakage of know-how, confidential information or
commercial/business secrets (see L. Mitrou, Labor Inspection
of Law, 76th volume, 2017, pp. 137 ff., especially 146-147). In particular, such a law
it may be in the interest of the employer to ensure the location
operation of the business with the establishment of control mechanisms
workers (see ECHR Barbulescu v. Romania, ibid., para. 127) as well as the
his need to protect the business and its property2 from significant
threats, such as preventing the transmission of confidential information to one
competitor or to secure the confirmation or proof of criminal activities
of the employee (regarding, see Article 29 Working Group Working Document for
the surveillance of electronic communications at the workplace of 5-29-2002
WP55, p. 18), to the extent of course that the employer, in the latter case, does not

enters into the exercise of investigative actions reserved by law

exclusively to the competent judicial-prosecution authorities and services that

act under their direct supervision.

Employees have a legitimate expectation of privacy

at the place of work, which is not detracted from the fact that they use

equipment, communication devices or any other professional

facilities and infrastructure (e.g. electronic communications network, wifi, etc.) of

employer (see APDPX 61/2004, Working Group of article 29 WP55, ibid. p. 9, L.

1 literally see AP (All) 1/2017 "From the provisions of articles 652 and 288 of the Civil Code and 16 of Law 146/1914

it follows that the employee, who has a duty of loyalty to his employer, is obliged not to

engages in competitive actions that harm the interests of the employer. Such acts, except

others, is the exercise for one's own account, without the knowledge of the employer, of commercial work, of similar

towards the actions of the latter, as well as the customer service of the employer directly by him

employee (AP 1285/1984)".

2 The managerial right of the employer is guaranteed by article 17. in combination with

provisions of articles 5 par. 1, 9, 9A, 22 par. 1, but also 106 par. 2 (see Fereniki Panagopoulou-

Koutnatzi, New technologies and the protection of the private sphere in the workplace,

European States 2/2011, pp. 325 ff., 331 ff.), through which the principle of

objective interest of the company that allows the judge to weigh them

conflicting interests when reviewing a decision of the employer.

Mitrou, op. op. in a collective volume Kotsali, ibid., p. 204). The distinction of boundaries

between private and public in the workplace has become indistinguishable

in view of the possibility of providing the work remotely (e.g. from home or

during business trips) or using owned devices

to the employee (Bring Your Own Device- BYOD3) [see Article Working Group

29 Opinion 2/17, WP 249 especially pp. 4, 15, 16 and 22]. So, on his part
employee use of a computer belonging to and for the employer
which has previously been expressly informed that its use is prohibited for non
professional reasons does not in itself constitute a legal reason for surveillance or
control of the personal data processed by the employee,
but more specific information is required (regarding see ECHR, Barbulescu v Romania,
ibid., para. 77).
In particular, from the provisions of articles 4 par. 1 sec. a' and 11 par. 1 N.
2472/1997 results in the obligation of the employer (data controller) to
informs the employee in advance in an appropriate and clear manner
(data subject) for the introduction and use of control methods and
monitoring during the personnel data collection stage
its character (see also APDPH Directive 115/2001 ch. C' para. 3 and E' para. 8).
according to the Working Group of article 29 the workers must
they are informed in advance about the surveillance of their work, the purpose
processing their data and other information necessary for the
ensuring legitimate and legal processing (see Opinion 8/2001, p. 25 and Opinion
2/2017, p. 8).
Moreover, when the employer monitors his electronic communications
employee, in addition to complying with all data protection principles
of a personal nature in order for it to be legal and justified, shall
must not only inform the employee beforehand, but
brings to his attention a legible, clear and precise statement of the Policy and of
Surveillance procedures (see Opinion 2/2017, in particular pp. 8, 10, 14, 23, WP document
55, ibid. pp. 16-17, APDPH 61/2004, 37/2007).
in this context the European Court of Human Rights

3 literally see the Guide of the competent supervisory authority of the United Kingdom – Information

https://ico.org.uk/media/for-

Commissioner

organizations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

(ICO)

in

10

by decision of 05-9-2017 in the case of Barbulescu v. Romania (op. op.) ruled in

broad synthesis that the employee's right to protection is being violated

of private life under no. 8 E DA in a case in which it takes place

surveillance of his electronic communications by the employer, without having

previously informed about both this eventuality and the circumstances

of carrying out such monitoring (purpose, nature, extent, degree

restriction of the individual right), which indeed should constitute the

last means of achieving the intended purpose (see paras. 133-140).

Unbeknownst to and in the absence of the employee, surveillance and control by him

employer of personnel data stored on the computer

character and communications cannot be excluded a priori, but is reserved

in exceptional cases, provided that such action either

is provided for, or does not contradict the national legislation and if the

necessary measures and due procedures have been provided for access to

professional electronic communication (see document WP 55, ibid. in particular pp. 5, 15,

16, Code of Ethics of the International Labor Organization for the protection of

of personal data of employees 1997, in particular articles 6.14 and

11.8, resolution 2015/5 of the Council of Ministers of 04-01-2015 for the

processing of personal data in the context of work

relations, especially articles 14.1-14.5 and 15.6).

and in accordance with article 11.8 of the International Code of Ethics

Organization of Work for the protection of their personal data

employees of 1997, the employer is entitled in the event of an audit which

is carried out on personal data for security reasons to refuse

temporarily the employee's access to them until the end of the audit

in order not to jeopardize the conduct of the investigation.

In addition, any control of the employee's computer without

prior notification of him and without his presence could be judged as

legal, necessary and appropriate for the achievement of the intended purpose if

there was a compelling reason for force majeure (see APDPH 37/2007) and since

the principle of proportionality was met.

In this case, from the data in the case file,

the hearing, the submissions and the whole process

it emerged that the company proceeded with computer control in principle

used by the applicant, from whom he found the deletion

saved files and for this reason proceeded to remove the hard drive

disk and sending it to a specialized company for their recovery

in order to establish the possible performance of illegal acts aimed at

weight of her property. Both this control and the removal of the hard

disk from the computer took place without his presence

applicant, without having previously been informed about the control and

removing the hard drive and without any care being taken for it

ensuring the legality and objectivity of the audit process.

The claim of the company, according to which it had

inform and obtain the consent of the applicant's father for him

control of his computer, as consent is provided by no.

2 pcs. ia' N . 2472/1997 only by the data subject himself, who

is informed beforehand.

less so, that the direct and imperative did not arise from any evidence

need to check the computer and remove it

hard disk without the presence of the employee, nor was it justified by the

company because a less onerous measure was not chosen, such as e.g. the temporary

turning off and locking the computer until the call and

presence of the applicant.

In addition, it emerged that the company did not have an internal Regulation for it

proper use and operation of the IT equipment and network and

communications from employees, from the content of which it would arise

on the one hand, that the use of personal computers was prohibited

purposes, on the other hand, the possibility and possibility of control would be expressly provided for

of these, the conditions, terms, procedure, scope and guarantees of its implementation

control.

on the other hand, the applicant admits that access to

other colleagues also had his computer from time to time,

on the other hand, it claims to have stored personal data (just

sensitive) on the computer in question, without however proving it

his claim (see APDPH 56/2013). And his claim that it was lacking

personal computer in his home and that all kinds of personal

data (e.g. photos from leisure trips, university papers,

his electronic communications data, etc.) stored exclusively in

disputed computer of his work, in addition to being inconsistent with the

lessons of common experience and logic, is not strengthened by any other

evidence e.g. by providing a portable digital storage

media (usb stick) where he kept backup copies of things so important to him

same files, from the examination of which he could (under conditions) to

check the validity of his claim. Additionally it should be noted that

if he kept personal data on his company computer and

namely sensitive, of the kind invoked, according to common experience and logic it will not

allowed colleagues to access his computer

and indeed in his absence.

In addition, from the documents presented by the company it emerged that Mr

hard drive of the disputed computer was empty at the time

of carrying out the control and files that may have been stored previously, had

already deleted beforehand by the audit, without making it possible to

their recovery and the determination of their content.

Given therefore that the existence of the stored was not proven

file of personal data of the applicant in the disputed electronic

computer, both during the initial control carried out by the company, and by

specialized control that took place after the removal of the hard disk, h

The Authority considers that the said appeal should be rejected in this part.

On the contrary, regarding the obligation of the controller to

gives the data subject a satisfactory answer during its exercise

right of access, it is established that, in this case, the company did not respond

satisfactory to the applicant's request to receive clear information about it

with the data concerning him, as well as with regard to any other element

which concerns the further processing of his data, such as e.g. her goals

processing, the recipients or categories of recipients, the evolution of the processing for

the time period since its previous update etc. (see in particular article 12

par. 2 of Law 2472/1997), nor did it notify the Authority of its response,

informing the interested party that he can appeal to it (see article 12

par. 4 Law 2472/1997).

In particular, the company, instead of providing answers to the applicant, even

and negative of any processing of his data, identifying him

13

at the same time, the persons to whom he sent the electronic hard disk

computer, he was effectively denied the satisfaction of his right

supporting the by ... "Extrajudicial Response Complaint Statement Invitation

With Reservation of Rights" that the appellant did not tell her "specifically who

is your personal data detailed and specified exactly and which

documents contain your personal data. If this includes correspondence

with the company, your father's orders as chairman of the board, the movement of

account from you as well as browsing the company's funds

us from your father's account, these documents are not your personal

data but data useful for our company... After your use

what you write in your ex parte declaration for personal data processing

they are not stable in character...".

The above response does not constitute satisfaction of the access request

of the applicant under no. 12 Law 2472/1997 in accordance with the above,

moreover, the appellant had no obligation to report to the company

"specifically what are his personal data", nor to specify them

"detailed and accurate", nor to indicate "which documents contain personal

given", at the very moment when the company claims the opposite

that no personal data file was found on his hard drive

computer.

Finally, it should be noted that the company as data controller

is burdened with the obligation to receive the appropriate organizational and technical

measures for the security of the data and their protection from accidental or

wrongful destruction, accidental loss, alteration, prohibited dissemination or

access and any other form of unfair processing under no. 10 par. 3 n.

2472/1997. A breach of personal data means

breach of security leading to accidental or unlawful destruction, loss,

alteration, unauthorized disclosure or access of personal data

transmitted, stored or otherwise processed

(see Opinion OE29 under no. 03/2014 on Personal Data Breach Notification WP 213),

i.e. the property of the existence of personal data is assumed.

In view of the above, although the existence of data was not proven

of a personal nature in order to check any security breach

them, however, it emerged that the company as controller has not received,

as he owes, the under no. 10 par. 3 of Law 2472/1997 necessary technically and organizationally

security measures of its information system, through which they are trafficked

and receive personal data processing as well as the same

alleges (although not proven) remote illegal access to

company computer in question and the deletion of stored files

(cf. APDPH 136/2015) which generally creates a risk of prohibited

access and destruction of stored data (cf. Guidelines

Lines of OE 29 WP 250 on Personal data breach notification of 03-10-2017 for

the distinction between a security incident and a privacy breach

of data, p. 7 and footnote 13).

Therefore, the Authority considers that the company violated the provisions of the article

12 L. 2472/1997 and after taking into account the seriousness of the violation, judges that

must be imposed on the company N. KRITIKO - G. DAIRTZE SA. TRADE

CHARTER the provision in article 21 par. 1 sec. b' of Law 2472/1997 sanction which

referred to in the ordinance and which is proportionate to its gravity

violation and the insult of the applicant as well as to address her

additionally according to article 19 par. 1 item c' of Law 2472/1997 the recommendations

mentioned in the ordinance.

FOR THOSE REASONS

1. It imposes on the company N. KRITIKO - G. DAIRTZE S.A. TRADE

PAPER fine of three thousand (3,000.00) Euros for non-fulfillment of

of its obligation to respond satisfactorily to the appellant in breach of it

according to article 12 of Law 2472/1997 his right of access.

2. Addresses to the company N. KRITIKO - G. DAIRTZE S.A. TRADE

CHARTER recommendation to take care of the preparation and implementation of internal

Regulation for the correct use and operation of the equipment and the network

IT and communications by employees

(subjects of

data), in the content of which should, among others,

included:

I.

Acceptable Use Policy for corporate computers (or

other related equipment), the corporate communications network (or other related

infrastructure) and corporate e-mail accounts as well

the relevant terms, conditions and procedures. in case of prohibition

use of the company computer for personal use by them

employees, to examine the possibility of granting the use of digital

storage space for personal use, in which it will not be allowed

employer access.

II.

Company computer access and control policy

(or other related equipment) used by employees in which to

described as a minimum:

the relevant purposes (justifications) of access and control,

respecting the principle of proportionality,

the nature and extent of the audit;

the procedure, manner and terms of access and control both in case

presence, as well as any absence of the employee,

the procedural safeguards concerning access and control, in particular

regarding the assurance and proof of correctness and

its objectivity as well as the presence or absence of the employee,

the way of informing the employee about the audit findings,

the procedure followed after the completion of the control with the

on which personal data may be processed

of findings to achieve the purposes of the audit as well as the relevant

informing the employee,

procedure and conditions, according to which the possibility is provided

avoiding access and control of all stored

files, data and information by adopting another, less

burdensome, method,

the previous information of the employees about the possibility of access

and control over corporate computers (or other related equipment) that

use as well as the cases of exemption from the obligation

information, respecting the principle of proportionality,

the possibility of appeal provided by the current legislation

workers in legal protection,

16

i.

ii.

iii.

iv.

v.

vi.

vii.

viii.

ix.

3.

Addresses to the company N. KRITIKO - G. DAIRTZE S.A. TRADE

PAPER recommendation to take care of receiving the appropriate organizational and

of technical security measures of its information system no. 10 par. 3

Law 2472/1997. the registration that exists is relevant to this issue

to

online

place

her

Principle

at

position

http://www.dpa.gr/pls/portal/url/ITEM/B6F5DCC88FD8EC4AE040A8C07C24572A.

The Deputy President

The Secretary

George Batzalexis

Irini Papageorgopoulou

17