Bld.Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poştal 010336, Bucureşti ; Tel: +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

CONTROL DEPARTMENT
No. _____/_____

Decision

Following the investigation performed at Bergenbier SA

The National Supervisory Authority for Personal Data Protection, with the headquarters in 28-30 G-ral Gheorghe Magheru Bld. District 1, post code 010336, Bucharest, legally represented by [redacted], president, **issues this decision against BERGENBIER SA,** with the headquarters in 9-9A Dimitrie Pompei Street, Building 20, 1st Floor, District 1, Bucharest, Romania, registered with the Trade Registry under no. J40/209/1999, sole registration code 6608725, legally represented by Mr./Mrs. [redacted], as director

Considering the following:

I. Personal data security breach notifications received based on Article 33

Molson Coors Global Business Services SRL notified a personal data security breach, by filling in the form regarding the breach of the personal data security provided under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), registered at the National Supervisory Authority for Personal Data Processing under no. 4618/12.03.2021**.**

Bergenbier SA notified a personal data security breach, by filling in the form regarding the breach of the personal data security provided under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), registered at the National Supervisory Authority for Personal Data Processing under no. 9923/28.05.2021**.**

Considering the above, ANSPDCP started an investigation at Bergenbier SA considering the mentions from the notification form no. 9923/28.05.2021, according to which „In Romania, Molson Coors activates through 2 entities – Bergenbier SA and Molson Coors Global Business Services SRL. The internal investigation of the Molson Coors Group showed that the controller is Bergenbier SA (and not *Molson Coors Global Business Services S.R.L)*".

Through the address no. 10624/08.06.2021, ANSPDCP requested additional information from **Bergenbier SA**, in order to identify the lead supervisory authority competent to handle the security breach notified through the forms no. 4618/12.03.2021 and no. 9923/28.05.2021.

Bergenbier SA responded through the address no. 11360/22.06.2021, as it follows: *"… at the level of Molson Coors Beverage Company an official designation of a representative in the Union, based on Article 3 paragraph 2 and Article 27 of the GDPR, was not performed. In this case, our internal investigation*

showed that the personal data controller responsible to notify the incident in the European Union is Bergenbier SA – an entity from the European Union."

Following the response provided through address no. 11360 from 22.06.2021, the National Supervisory Authority for Personal Data Processing (hereinafter, referred to as "ANSPDCP") acted as lead supervisory authority (LSA) in this case, considering that this company has its main establishment in Romania, by introducing within the application "Internal Market Information System" a notification according to Article 56 in order to inform the supervisory authorities from the other European Union Member States, registered under no. 428112.

We hereby present a resume of the security incident and of the results of the investigation performed by ANSPDCP in this case.

II. Description of the case:

According to the mentions from the notification form no. 9923/28.05.2021, on 9th of March 2021, time 12:00, it was identified that the global network and systems of the Molson Coors Group were subject of a cyber-attack. The internal investigation showed that one or several cyber attackers has/have gained access to the Molson Coors Group systems and installed "malware" type computer programs through the network, existing clues that certain information were copied by the attacker(s). Also, the investigation showed that the cyber-attack affected a server located in Ploiesti, used by the controller in order to store information.

As part of the Molson Coors Group (as defined below) the controller benefits from a complete range of controls for detecting the cyber threats and of prevention measures. This range includes, but is not limited, to the following:

- a computer program "firewall" type (network perimeter firewall) against the unwanted traffic, dangerous codes and intrusion attempts;

- the use of the "proxy" type server that acts as a gate between the business activity and internet and that verifies, before transmission, the communications;

- the use of a detection "endpoint" and of an antivirus computer program in order to monitor the access points (such as the laptops of the users) and to mitigate the cyber threats;

- a security team allocated 24/7 that monitors the threats received via e-mail and the "phishing" attacks and that is responsible for monitoring the antivirus brackets and alerts and acts in case of incidents;

- a special antivirus protection plan;

- a computer program Advanced Threat Protection type used for the detection, investigation and counteraction of the cyber-attacks on the network;

- A computer program Endpoint Protection Client type for the Windows servers;

- a software application that detects and responds to threats, installed by a security services provider in order to detect, investigate and combat the threats on the access points and network;

- the handling, monitoring and reporting of the journal files;

- intrusions detection systems;

- segmentation within the network in order to separate the "legacy" type network from the virtual networks;

- outsourced security controls;

- vulnerabilities detection;

- active vulnerabilities scanning.

The type of the personal data security breach is: availability and confidentiality.

The nature and content of the personal data envisaged: personal data of the current and former employees, as well as of other data subjects (first name and last name, date of employment, PIN, series and number of the identity card, date of birth, bank account, ID/employee mark, number of the credit/debit card, the position held and others).

A number of 6334 natural data subjects was affected.

The controller benefited from a series of organisational and technical measures for the mitigation of the risks generated by this security breach, respectively:

From organisational perspective:

- The employment of external experts, in order to assist the controller with the implementation of the mitigation measures and within the investigation;
- the activation of a response plan to the incident;
- The forming of a working group composed of internal decision factors and external experts, to address both the organisational as well as technical aspects of the security incident, including the analysis of the high risk for the rights and freedoms of the affected data subjects.

From technical perspective:

- Immediately after the incident, they disconnected any external connexions including the VPN access type and Virtual Desktop access in order to allow the adequate cleaning of the systems and the remedy of any problems;
- They improved the authentication systems for the IT systems dedicated to the employees and providers;
- They added additional programs for the detection and prevention of any unauthorized access on the computers, laptops and mobile devices;
- They used extended software applications in order to detect and respond to the threats and programmes that continuously verify the systems in order to detect any suspicious activity and to stop the potential threats.
- They informed that natural data subjects affected by the incident by the e-mail addresses (for the former employees) and through the web page www.bergenbier.ro, section "GDPR Alert" (for former employees and third parties).

According to those declared through the security breach notification form submitted, it resulted that also natural data subjects from other member states of the European Union were affected such as: Hungary (427 persons), Czech Republic (677 persons), Slovakia (44 persons) and Croatia (658 persons).

In Romania an estimated number of 2636 natural data subjects were affected.

III. Handling steps taken by ANSPDCP

Through the address no. 10624/08.06.2021, ANSPDCP requested additional information from Bergenbier SA, that responded through letter no. 11360/22.06.2021 as it follows:

Q1: "considering that the company Bergenbier SA is part of the Molson Coors Beverage Company that has its headquarters in United States of America, those declared under points 16 and 17 from the notification form, as well as those mentioned above, please inform us if Molson Coors Beverage Company has designated a representative in the European Union and what this is, in order to identify the lead supervisory authority."

A1: *Molson Coors Beverage Company is a multinational beverages and beer company with two executive offices in Golden, Colorado and Montreal, Quebec, with activity in various states, including Romania.*

At the level of the Molson Coors Beverage Company an official designation of a representative in the Union, based on the Articles 3 paragraph (2) and 27, was not performed. In this case, our internal investigation showed that the personal data controller competent to notify the incident in the European Union (as defined below) is Bergenbier SA – an entity from the European Union.

Within Molson Coors a global Ethics and Compliance team, responsible with the support of the development and implementation of the practices that facilitates the compliance with the applicable legislation and policies of the Molson Coors Group, acts. For the successful fulfilment of the role held, the team is composed of members from the United States of America and Europe that are responsible, among others and each in relation to its own geographical jurisdiction, with the monitoring of the compliance with the applicable legislation in the field of the personal data protection within the Molson Coors Group.

We underline that the members of the global Ethics & Compliance team are closely handling the ensurance of the compliance with the provisions of the legislation applicable in the personal data field and are supported in this effort by the persons having competences from different levels within the organisation and in different territories around the world.

Q2: "please mention the residence states of the data subjects, as well as the number of data subjects affected detailed for each European Union member state /third party state, as well as if other supervisory authorities have been notified in relation to the security incident that took place at the level of Molson Coors Beverage Company";

R2: *Our client cannot perform an identification of the residence state of the data subjects due to the lack of the adequate technical and logistic means in order to perform this investigation. However, based on the information available at this moment, our client can provide a list with the estimated numbers of the data subjects broken down on each European Union member state/third party state. Therefore, please find attached to this answer a list containing the estimated number of the data subjects detailed on each of the European Union member state/third party states, in certified true copy (Annex 1).*

We underline that within 72 hours from the incident, as it was indicated within the notification registered within the General Registry of ANSPDCP under no. 4618/12.03.2021 and detailed within the completion of the notification registered within the General Registry of ANSPDCP under no. 9923/28.05.2021 ("the Incident"), the Molson Coors Group, through the affiliated entities, notified the relevant supervisory authorities.

More precise, in Romania, Molson Coors Global Business Services SRL notified ANSPDCP as lead supervisory authority in relation to the processing within the European Union. This notification was registered within the General Registry of ANSPDCP under no. 4618/12.03.2021. In Great Britain, Molson Coors Brewing Company (UK) Limited notified Information Commissioner's Office ("ICO"), and in Canada, Molson Canada 2005 notified the Privacy Commissioner of Canada.

Following the internal investigation, the support of the external experts contracting for assisting the remedy and investigation process and of the correspondence with different supervisory authorities, the need to submit additional notifications or to provide clarifications resulted.

Therefore, in Romania, Bergenbier SA submitted a completion to the notification registered within the General Registry of ANSPDCP under no. 4618/12.03.2021, considering the fact that the internal investigation revealed that Bergenbier SA is, actually, the controller of the personal data competent to notify the Incident within the European Union. This completion of the notification was registered within the General Registry of ANSPDCP under no. 9923/28.05.2021.

In Great Britain, ICO requested additional information regarding the incident and the progress of the internal investigation, an update of the notification being correspondingly submitted. ICO closed the investigation and confirmed that no other measures will be taken.

In Canada, an additional notification and a model of individual information notice were submitted to Privacy Commissioner of Canada.

Country	Estimated number of data subjects
Romania	2636
Serbia	770
Hungary	427
Bosnia and Herzegovina	84
Bulgaria	748
Montenegro	242
Czech Republic	677
Slovakia	44
Croatia	658
Great Britain	2
Not determined	46

Subsequently, through address no. 14822/02.09.2022 ANSPDCP requested additional information to Bergenbier SA, that responded through address no. 15392/13.09.2022 as it follows:

Q1: The investigation report of the incident performed with the support of the experts

A2: *The incident investigation report performed with the support of the experts, we attach to this answer the incident investigation report performed by Securityworks Inc. in the English version (certified true copy – Annex I.A) and translated into Romanian (Annex I.B.) to the extent you consider appropriate, at your request, we can also make available a legalized translation in Romanian of the incident investigation report.*

Q2: Considering the provisions of Article 24 and Recitals 75 and 76 from the Regulation (EU) 2016/679, by reference to point 11 from the notification "possible consequences and adverse effects (risks) for the natural data subjects", we hereby request you to provide the **evaluation procedure/methodology regarding the risk for the persons' rights and freedoms;**

A2: Considering the provisions of Article 24 and Recitals 75 and 76 of Regulation (EU) 2016/679, by reference to point 11 from the notification "possible consequences and adverse effects (risks) for the natural data subjects", we hereby request you to provide the evaluation procedure/methodology

regarding the risk for the persons' rights and freedoms, we mention that the methodology used by our Client involved the following steps:

Step 1: The identification of the existence or not of the personal data within the incident

Step 2: Establishing the categories of personal data affected

Among the personal data affected are:

- *First name and last name, PIN, number and series of the identification card, number of the banking account, number of the credit/debit card and/or*
- *Address and/or date of birth and/or the position held at the previous work place and/or date of employment*
- *Among the personal data affected there are no data from the category of special data (as provided under Article 9 from the General Data Protection Regulation)*

Step 3: The identification (as much as possible) of the third persons that could have access to the personal data affected by the incident;

- *The investigation showed that the cyber attacker/attackers had unauthorized access to the personal data identified at Step 2 above;*

Step 4: the evaluation of the general context of the incident

- *The identification of other details related to the incident, the type of unauthorized access, the working method of the cyber attacker/attackers, and others*

Step 5: the evaluation of the risks and the review and update of the corresponding measures

- *The analysis of the categories of personal data and of the context of the unauthorized processing, as well as of the probability of any risk on the data subjects' rights and freedoms and the adopting of additional measures in order to increase the protection of the data subjects (please see the measures of the Human Resources Operations Department detailed below).*

Q3: Considering the provisions of Article 24 and Recitals 75 and 76 from the Regulation (EU) 2016/679, by reference to point 11 from the notification "possible consequences and adverse effects (risks) for the natural data subjects", we hereby request you to provide us an evaluation regarding the risks for the persons' rights and freedoms that contain inclusively the framing within a risk degree (low, medium. high)

A3: Considering the provisions of Article 24 and Recitals 75 and 76 from the Regulation (EU) 2016/679, by reference to point 11 from the notification "possible consequences and adverse effects (risks) for the natural data subjects", we hereby request you to provide us an evaluation regarding the risks for the persons' rights and freedoms that contain inclusively the framing within a risk degree (low, medium. high), our Client performed an evaluation based on the following criteria:

The potential impact that the incident could have had, generally, on the life of the data subjects and if the incident could have affected them in any manner:

• The following questions were of interest for our Client:

Can the incident create an unsecure situation in which the affected data subject would be?

Can the affected data subjects lose money or the workplace following this incident?

Can the incident affect the health or the good living of the affected data subjects?

The attempt to identify the impact helped our Client to identify the measures necessary to be taken in order to limit the negative effects of it and to protect the data subjects from subsequent injuries.

The categories of personal data affected

• These were identified according to Step 2 detailed within the methodology from above.

The manner in which the unauthorized access could affect the data subjects; in other words, how could the data be used?

Considering the methodology applied and the criteria above, our Client paid more attention to the following aspects:

- *No special categories of personal data were accessed;*
- *Although there have been accessed some financial personal data or data from the identity card, the probability for this access to lead to a financial loss and/or fraud of the identity was classified as medium to low, considering that the financial institutions frequently have advanced security measures, such as multiple authentications, in order to verify and, thus, to prevent the identity frauds or other similar incidents.*

However, our Client decided, out of prudence, to qualify this incident as having a high risk for the affected data subjects and, therefore, to notify the data subjects, as we also showed within the completion to the notification registered within the General Registry of ANSPDCP under no. 9923/28.05.2021, and to adopt the indicated additional technical and organisational measures.

Q4: possible additional technical and organisational measures adopted, by reference to Article 32 GDPR, following the investigation performed

A4: the possible additional technical and organisational measures adopted, by reference to Article 32 GDPR, following the investigation performed, we mention the following aspects:

- At technical level, the IT security of the Molson Coors Group (that our Client is part of) is centrally governed and is part of the global network. As a response to this incident, based on the cyber security plan, several amendments were implemented both at technical and processes level. A company specialised in response to information security related incidents services was contracted (Securityworks Inc, as we showed in point 1 above) for the assistance related to the response and recovery process. Therefore, several remediation actions needed to be adopted following the activity of the cyber attacker/attackers, as is mentioned in the report attached to this response. Therefore, the additional measures include:

Multi-factor authentication system for all the remote access methods

The limitation of the number of users that have management rights within the Microsoft Active Directory system and the implementation of a management system for the privileged access (IBM Secret Server) in order to monitor the access data corresponding to the special critic accounts. Our Client included a control for review of the rights and access data within the list of the compliance controls in order to ensure that these rights and access data are periodically, quarterly revised;

The implementation of a computer program for the detection and counter-attack of the information attacks, program acquired from the Security Services Provider (MSSP) (Secureworks), on all the working stations of the users and on the Windows and Linux servers from the data centres and the beer factories connected in the same network; the update of the type of services offered to MSSP in order to move from outsourced personnel services to services for the management of the detection and counter-attack of the

information attacks. Also, the number of employees from the Security Operations Centre was increased. These actions were finalized in July 2021, considering the time necessary to make the transition to this new type of services and to employ additional human resources

Performing an action to renew all passwords, including the Kerberos tickets;

The update of the passwords' policies by amending the length requirement to a minimum of 12 characters and at the same time the increase of the size of the validity period of the password from 90 days to 365 days

Adding a computer program for the detection of the phishing attempts and their automatic rejection, in addition to the computer program

Microsoft Advanced Threat Protection, for a better detection of the phishing e-mails

The blocking of the access to certain websites that allow the sharing of data as well as of the data sharing applications, by using different computer programs, such as Zscaler Internet Access (Internet firewall);

The update of all the working stations from Windows 7 to Windows 10

The installation of the computer programs Microsoft Azure Information Protection and Microsoft Identity Protection, as well as the enhancement of the data loss detection and prevention mechanism made available by the computer program Microsoft Office 365;

The replacement of the existing solution for VPN with a new one, „reverse proxy security type, named Zscaler Private Access, that allows a „zero-trust" type approach for network access. This new solution continues to use the authentication with multiple factors for remote access

The launch of a global training program for the awareness of the security risks, program named CyberSIP.

The implementation of additional options for archiving and recovery of the data and the inclusion of a data copy option that does not involve the connection to the network.

-At organizational level, at the beginning of January 2022, the Human Resources Operations Department implemented additional measures to ensure a high level of employees' data protection, in this respect the Human Resources Operations Department was notified in relation to the need to comply with the following additional rules:

The protection with password of the documents: any personnel file containing personal data will be protected with password, The provision of the documents protected by password will be performed via a different e-mail from the e-mail through which the password will be communicated;

The control of the provision: any personnel file that contains personal data will be transferred solely to the department employees responsible with/with attributions (access based on the position);

The access to internal platforms: the access on the Sal wages platform and on the platform named People Central will be performed solely using user name and password (in addition, for the access on the SAL wages platform, a special license is necessary), and the level of access is granted depending on the position held and the responsibilities/job description (access based on positions)

The verification of the access: the Operations Manager verifies the audit report issued by the SAL wages platform in order to ensure that the access of the employees is according to those describe above.

Q5: the last audit report regarding the certification according to the standard *ISO/IEC 27001:2013,* in case that at the company level a certified management level for the security of information is implemented

A5: the last audit report regarding the certification according to the standard *ISO/IEC 27001:2013, in case that at the company level a certified management level for the security of information is implemented, our Client does not have the ISO/IEC 27001:2013 standard implemented, but it has to be mentioned that its informatic security program is based on the Cyber Security NIST Framework.*

IV. The information of the concerned supervisory authorities within IMI

On 12.08.2022, the other supervisory authorities were informed, through the IMI application, within a procedure for identification of LSA and CSA (based on Article 56 GDPR), about the security incident, as well as regarding the intention of our institution to act as lead supervisory authority, registered under no. 428112, the deadline being 13.11.2022.

Until the date of this report, the following supervisory authorities declared as CSA:

- The Supervisory Authority from Netherlands (with the mention that "based on the information we cannot decide if the data subjects from Netherlands were affected by this incident. However, we will consider ourselves CSA in order to be sure")
- The Supervisory Authority from Poland (with the mention "In case the data subjects that live in Poland are affected, we want to be considered CSA")
- The Authority from Bulgaria;
- The Authority from Hungary;
- The Authority from Berlin, Germany (with the mention "In case the data subjects residing in Berlin are affected, we want to be considered CSA")

On 20.03.2023, through the IMI application, ANSPDCP informed the supervisory authorities from the EU states, which declared themselves "concerned supervisory authority", within the consultation procedures (based on art. 60 para. (7) of the RGPD), regarding the draft decision to be adopted following the investigation carried out.

The response deadline was set in IMI until 11.04.2023.

As a result of the verification carried out in the IMI application, on 12.04.2023, it was found that no comments/objections were made regarding the draft Decision.

V. <u>Conclusions:</u>

From the investigation performed by ANSPDCP through the address no. 10624/08.06.2021 and nr.14822/02.09.2022, and from the Bergenbier SA answers no. 11360/22.06.2021 and no. 15392/13.09.2022, the following resulted:

- The security incident consisted of the unauthorized access of the personal data of the employees/former employees/other data subjects from the Molson Coors Group entities, data subjects from several Member States being affected;
- The personal data affected:

    - first name and last name, PIN, number and series of identity card, number of bank account, number of the credit/debit card and/or
    - address and/or date of birth and/or the position held at the previous work place and/or the date of employment

- The investigation showed that no special categories of personal data were unauthorized accessed.

- As a response to this incident, based on the cyber security plan, the controller implemented several amendments both at technical and processes level. A company specialized in informational security response services was contracted (Securityworks Inc) for the assistance related to the response and recovery process.
- Subsequently to the security incident, additional technical and organizational measures were adopted, finalized in July 2021. These include:
    - Multi-factor authentication system for all the remote access methods
    - The limitation of the number of users that have management rights within the Microsoft Active Directory system and the implementation of a management system for the privileged access (IBM Secret Server) in order to monitor the access data corresponding to the special critic accounts
    - A control for review of the access rights and date within the list of the conformity controls in order to ensure that these rights and access data are periodically, quarterly re-certified
    - The implementation of a computer program for the detection and counter-attack of the information attacks on the working stations of the users and on all the Windows and Linux servers from the data centres and beer factories connected in the same network; the update of the type of services offered by MSSP to pass from the external personnel services to services for management of the detection and counter-attack of the information attacks
    - The increase of the number of employees from the Security Operations Centre.
- Performing an action to renew all passwords, including the Kerberos tickets;
- The update of the passwords' policies by amending the length requirement to a minimum of 12 characters
- Adding a computer program for the detection of the phishing attempts and their automatic rejection, in addition to the computer program Microsoft Advanced Threat Protection, for a better detection of the phishing type e-mails;
- The blocking of the access to certain websites that allow the sharing of data as well as of the data sharing applications, by using different computer programs, such as Zscaler Internet Access (Internet firewall);
- The update of all the working stations from Windows 7 to Windows 10;
- The installation of the computer programs Microsoft Azure Information Protection and Microsoft Identity Protection, as well as the enhancement of the data loss detection and prevention mechanism made available by the computer program Microsoft Office 365;

- The replacement of the existing solution for VPN with a new one, „reverse proxy security type, named Zscaler Private Access, that allows a „zero-trust" type approach for network access.
- The implementation of additional options for archiving and recovery of the data and the inclusion of a data copy option that does not involve the connection to the network.
- The protection through password of the documents; provisions control; access to internal platforms by using user name and password
- Bergenbier SA informed the data subjects affected by the incident were informed as it follows: the current employees were informed by e-mail and the information of the former employees and/or third parties was performed on the website www.bergenbiersa.ro, section GDPR Alert;
- following the introduction of the case within the IMI application the following member states declared as being concerned supervisory authorities: Netherlands, Poland, Bulgaria, Hungary and Germany
- Following the investigation procedures performed it was found that a number of 6334 data subjects were affected from the following states: Romania, Serbia, Hungary, Bosnia și Herzegovina, Bulgaria, Montenegro, Czech Republic, Slovakia, Croatia, Great Britain;
- From the verifications performed until the conclusion of this report, ……., it was found that no complaints were submitted by the security incident notified by Bergenbier SA.

VI. Analysis according to the Article 83 GDPR criteria

The conclusions resulting following the analysis of the security incident according to the Article 83 GDPR criteria:

a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
   - 6334 data subjects affected (employees/former employees/third parties)
   - The systems and global network of the Molson Coors Group were subject to a cyber-attack following which one or several cyber attackers has/have gained access to the Molson Coors Group systems and installed malware type computer programs through the network
   - The incident took place in March 2021, the additional technical and organizational measures, implemented by the controller for the remedy of the incident being finalized in July 2021
   - No complaints were submitted by the persons envisaged by the security incident notified by Bergenbier SA, therefore no damages incurred by them were able to be identified

b) the intentional or negligent character of the infringement;
   - malware type cyber-attack

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
   - the data subjects affected by the incident were informed as it follows: the current employees were informed by e-mail and the information of the former employees and/or third parties was performed on the website www.bergenbiersa.ro, section GDPR Alert;
   - an evaluation regarding the risk for the data subjects' rights and freedoms was performed
   - subsequent to the security incident additional technical and organisational measures were adopted

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
   - the informational security program of the controller is based on the Cyber Security NIST Framework

- a firewall type computer program (network perimeter firewall) against the unwanted traffic, dangerous codes and intrusion attempts
- the use of a proxy type server that acts like a gate between the business activity and Internet and that verifies, before provisions, the communications;
- the use of a detection endpoint of an antivirus type computer program in order to monitor the access points (such as laptops of the users) and to mitigate the cyber threats
- a security team allocated 24/7 that monitors the threats received via e-mail and the phishing type attacks and that is responsible to monitor the antivirus consoles and that alerts and acts in case of incidents
- a special antivirus protection plan
- an Advanced Threat Protection type computer program used for the detection, investigation and counter-attack of the cyber-attacks on the network
- an Endpoint Protection Client type computer program for the Windows servers
- a software application that detects and answers to the threats, installed by a security services provider for the detection, investigation and combatting the threats on the access points and on the network
- the handling, monitoring and reporting of the journal files
- the intrusion detection systems
- segmentation within the network in order to separate the legacy type network from the virtual networks
- outsourced security controls
- vulnerabilities detection
- scanning of active vulnerabilities

e) any relevant previous infringements by the controller or processor;
   - no previous breaches were identified

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
   - the controller notified the security incident within the term provided by GDPR and communicated to ANSPDCP all the information requested within the investigation performed

g) the categories of personal data affected by the infringement;
   - first name and last name, PIN, number and series of identity card, number of bank account, number of the credit/debit card and/or
   - address and/or date of birth and/or the position held at the previous work place and/or the date of employment
   - The investigation showed that **no special categories of personal data were accessed unauthorized**

h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
   - the controller **notified the security incident within the term provided by GDPR and communicated to ANSPDCP all the information requested within the investigation performed**

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
   - measures have not been applied previously

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

- The security incident took place following a malware type security incident and not to avoid some losses of to obtain some financial benefits directly or indirectly

Considering the findings resulted from the investigation performed at the Bergenbier SA, as well as from the analysis of the incident according to the criteria from Article 83 GDPR, we consider that in this case the application of a sanction is not required.

President,

[redacted]