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 la SC UiPath SRL

**The National Supervisory Authority for Personal Data Protection,** with the headquarters in 28-30 G-ral Gheorghe Magheru Blvd., District 1, post code 010336, Bucharest, legally represented by [redacted], President, issues this decision against SC UiPath SRL, with the headquarters in 4 and 11, Vasile Alecsandri and Constantin Daniel Street, Building A, 5th – 6th Floor, District 1, Bucharest, registered with the Trade Registry under no. J40/8216/2015, sole registration code 34737997, legally represented by [redacted], as director

## Considering the following:

## I. Personal data security breach notification received based on Article 33

SC UiPath 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), notification registered at the National Supervisory Authority for Personal Data Processing under no. 23973/07.12.2020 (by e-mail) and no. 2699/12.02.2021 (on-line).

Considering that the main establishment of the controller that performs activities in several Member States is the one from Romania, ANSPDCP is the supervisory authority of the main establishment of the controller, competent to act as lead supervisory authority for the cross-border processing performed by UiPath SRL according to the procedure provided under Article 60 of the GDPR, being at the same time the only supervisory authority from the EU to which the personal data security breach was notified.

Therefore, the National Supervisory Authority for Personal Data Processing (hereinafter referred to as „ANSPDCP") introduced within the application "Internal Market Information System" a notification according to Article 56 registered under no. 294927.1, in order to inform the supervisory authorities from the other European Union Member States.

Therefore, according to the mentions from the notification forms no. 23973/07.12.2020 (by e-mail) and no. 2699/12.02.2021 (on-line), on 1st of December 2020, 20:41 time, a breach of the personal data confidentiality estimated to have taken place on 30th of November 2020 was identified, consisting of the publishing of the personal data (user's first name and last name associated to the Academy Platform Account, user name, unique identifier of each user, e-mail address, name of the company where the user is employed, country and details on the level of knowledge level obtained within the UiPath Academy courses) of 600,000 users of the Academy

Platform on the website accessible at the URL address www.raidforums.com, information brought to the knowledge of the controller by a third party.

The „Academy Platform" was made available to the users in order to get familiar with the products marketed by UiPath, the latter being rewarded with a certification of the knowledge obtained. The access of the users to the Platform is performed through an account, all the data (above) being stored in a common database.

Based on the technical analysis performed by the controller, the latter found that the **technical settings of the storage space allowed the unauthorized access** to the personal data of the Academy Platform users. (At this moment the access is performed through a multi-factor authentication system single-on type, being limited to the persons entitled, based on some unique identification elements and on a password with complex elements).

The technical and organisational measures applied by the controller consisted of the prevention of the unauthorised and unauthenticated access, of the blocking of the unauthorised accessing source, a formal notification being submitted with the administrator of the third-party website with the request to eliminate that file.

The controller considered that the incident **is not likely to generate a high risk** for the data subjects (users of the Academy Platform), their information not being necessary, without excluding that, following the final analysis, the decision on their information to be taken, according to the notification submitted.

## II. Conclusions following the investigation performed at SC UiPath SRL:

From the investigation performed by ANSPDCP, the following resulted:

- the security incident consisted of the publishing of the personal data of the Academy Platform users on 30th of November 2020 at the URL address www.fileconvoy.com, where there have been redirected through a link accessible at the URL address www.raidforums.com; the data of the Academy Platform users were exposed during 30th of November 2020 – 9th of December 2020, persons from several EU Member States being affected;
- at this moment, "a very small part of the data continues to be found on www.raidforums.com, in the form of a preview";
- the personal data affected by the incident: user's first name and last name associated to the account from the Academy Platform, the e-mail address, unique identifier of each user, the name of the company where the user is employed, the country and details on the level of knowledge obtained within the UiPath Academy courses;
- from the investigation it resulted that no special categories of personal data were affected;
- SC UiPath SRL implemented, before the incident notified, a security management system (ISMS) according to the ISO/IEC 27001:2013 standard, which is annually audited; according to the conclusions of the audit report from 20th of March 2020, phase 2, it was found as early as 2019 in phase I that there is an improvement possibility in relation to the risks' evaluation; in phase 2, given that no activity in relation to this improvement possibility was performed, this remains open;
- before the incident took place, the controller implemented cybersecurity and confidentiality policies (on: the correct use of the technology, the access control, the work on own devices, cryptographic control, data retention, transfer and erasure, incidents' management, information classification, management of devices, network and

communications security, passwords, physical protection, security of the information disclosed by providers, teleworking, confidentiality, authorised external audit, as well as the plan for the continuance of the business (security), procedure on the storage of the documents and code of conduct);

- the annually reviewed policies are brought to the knowledge of the employees both at the hiring and periodically, during the employment;
- the employees receive warnings in relation to the need of performing the training, and each team leader receives reports in relation to the stage in which his team is in relation to the annual training; the policies are reviewed annually and are brought to the knowledge of the employees both annually and periodically;
- after the incident, the controller took the following measures:
  - established a plan for the reinforcement of the security of the storage accounts in cloud; the public storage accounts will be annually reviewed by the internal security team. Within the review procedures the details regarding the data stored in each such account will be recorded, as well as the reason for which that storage accounts are public;
  - added new policies within the storage platform of these accounts (Microsoft Azure) in order to ensure that all the storage accounts are implicitly created **privately**;
  - shall implement penetration tests in order to evaluate the security of the systems;
- SC UiPath SRL performed the information of the data subjects both by e-mail and through the UiPath Academy Platform;
- following the introduction of the case within the IMI application, the following Member States declared themselves as concerned supervisory authorities: Germany – Lower Saxony Land, Italy, Ireland, Slovenia, Belgium, Norway, Estonia, Austria, Netherlands, Finland, Sweden, Luxembourg, Spain, Bulgaria, Germany – Hessen Land, France and Denmark;
- following the investigation steps taken it was found that a number of 600,000 data subjects were affected, from 258 states, out of which 76,095 data subjects from the EU/EEA Member States;
- from the reviews performed until the date of conclusion of the report, it was found that no complaints were submitted by the persons concerned by the security incident notified by SC UiPath SRL.

## III. Information of the concerned supervisory authorities within IMI

On 17th of May 2021, the other supervisory authorities were informed through the IMI application, registered under no. 294927.1, within a LSA and CSA identification procedure (based on Article 56 of the GDPR), in relation to the security incident, as well as in relation to the intention of our authority to act as lead supervisory authority, with deadline until 07.08.2021.

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

- the Supervisory Authority from Germany – Lower Saxony Land (with the mention "the data subjects from Lower Saxony could be affected");

- the supervisory authorities from Italy, Ireland, Slovenia, Belgium, Norway, Estonia, Austria, Netherlands, Finland, Sweden, Luxembourg, Spain, Bulgaria, Germany – Hessen land, France, Denmark (with the mention "the processing is affecting or could substantially affect the data subjects from those states");
- the supervisory authority from Germany – Baden-Wurttemberg Land did not declare itself as concerned authority.

The concerned supervisory authorities did not submit relevant and reasoned objections, thus resulting this final decision.

## IV. The findings/sanctioning report

Following the investigation performed, the findings/sanctioning report no. 13172 through which the following aspects were found was concluded:

"*On the conclusion date of this report, 10.07.2023, it was found that* SC UiPath SRL, with the identification data and headquarters mentioned on the first page of this report, breached the provisions of Article 25 paragraph (2) and Article 32 paragraph (1) letters b) and d) and paragraph (2) of the GDPR, as it did not implement adequate technical and organisational measures in order to ensure that, implicitly, the personal data cannot be accessed, without a person's intervention, by an unlimited number of data subjects, including the capacity to ensure the continued confidentiality and resistance of the processing systems and services, as well as a process for the periodical testing, evaluation and of the efficiency of the technical and organisational measures in order to guarantee the security of the processing. This led to the **unauthorised disclosure and unauthorised access** to the personal data (first name and last name of the user associated to the Academy Platform account, user name, unique identifier of each user, the e-mail address, the name of the company where the user is employed, the country and details on the level of knowledge obtained within the UiPath Academy courses) of approximately 600,000 users of the Academy Platform belonging to the controller UiPath (out of which 76,095 data subjects from the EU/European Economic Area), during 30th of November 2020 – 9th of December 2020, at the URL address www.fileconvoy.com (where they have been redirected through a link accessible at the URL address www.raidforums.com), fact that can lead specifically to physical, material or moral damages for the natural persons affected, such as the loss of the control on their personal data or the loss of the personal data confidentiality through professional secret or another economic or social significant disadvantage for that natural person.

This deed represents a contravention according to Article 12 of Law no. 190/2018, by reference to the provisions mentioned under Article 83 paragraph (4) letter a) of Regulation (EU) 2016/679."

Considering the findings from the investigation performed at SC UiPath SRL, as well as from the analysis of the incident according to the criteria from Article 83 of the GDPR, the provisions of Article 60 of Regulation (EU) 679/2016, as well as those of Article 16 paragraphs (3) and (7) of Law no. 102/2005, republished, that provide for the application of sanctions/corrective measures through the decision of the President of ANSPDCP, based on the findings report and of the report of the control personnel, become applicable.

## V. Arguments and resolution:

Considering the conclusions resulting from the investigation performed at SC Uipath SRL,

Based on the deed found through the findings report no. 13172/10.07.2023, above mentioned,

Considering the provisions of Article 25 paragraph (1) and (2) of the GDPR, according to which: "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

Considering the provisions of Article 32 paragraph (1) letter b) and paragraph (2) of the GDPR, according to which "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"

Considering that the fine that can be applied for the breach of the controller's obligations mentioned above is of up to EUR 10,000,000 or, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, according to Article 83 paragraph (4) letter a) of the GDPR,

Considering the provisions of Article 83 paragraphs (1), (2) and (3) of the GDPR,

"(1) Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

(2) Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

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

b) the intentional or negligent character of the infringement

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

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;

e) any relevant previous infringements by the controller or processor;

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

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;

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;

j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

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.

(3) If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."

Considering the fine individualisation criteria established under Article 83 paragraphs (2) and (3) of the GDPR, depending on which the below fine was established based, mainly, on the following aspects:

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:
   - 600,000 data subjects affected (users of the Academy Platform);
   - the technical settings of the storage space that allowed the unauthorized access to the personal data of the Academy Platform users;
   - the incident that took place on 30th of November 2020 consisted of the publishing of the personal data on a third-party website, information brough to the knowledge of the user by a third party;
   - no complaints were submitted by the data subjects concerned by the security incident notified by SC Uipath SRL, therefore no damages suffered by them were able to be identified;
b) the intentional or negligent character of the infringement
   - out of negligence;
c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
   - the data subjects concerned by the incident were subsequently notified, by e-mail and through the Uipath Academy platform;
   - after the security incident took place 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 controller implemented cybersecurity and confidentiality policies;
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 deadline provided under GDPR and submitted 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 user associated to the Academy Platform Account, user name, unique identifier of each user, e-mail address, name of the company where the user is employed, country and details on the level of knowledge level obtained within the UiPath Academy courses. No special categories of personal data have been affected.

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 deadline provided under GDPR and submitted 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:
   - no measures were 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:
   - we considered that the security incident took place out of negligence, and not for avoiding some losses or obtaining some financial benefits directly or indirectly.

Considering, in conclusion, the breaches found, the elements for the individualization of the sanctions, identified based on Article 83 paragraph (2) and paragraph (3) from the GDPR, based on which ANSPDCP proceeded to the analysis of the effectiveness, proportionality and dissuasive effect of the fines applied,

Based on Articles 14, 15 and 16 of Law no. 102/2005, republished, of Article 12 of Law no. 190/2018, by reference to Article 83 paragraph (2) and to the provisions detailed under Article 83 paragraph (4) letter a) of Regulation (EU) 2016/679, corroborated with the provisions of Article 58 paragraph (2) letter i), as well as those of Article 60 from Regulation (EU) 2016/679, by reference to the provisions of Article 24 and 26 of the Procedure for conducting investigations, approved by Decision of the President of ANSPDCP no. 161/2018, with the subsequent amendments and completions, we propose the following:

**The National Supervisory Authority for Personal Data Processing**

**DECIDES**

**The following measures against SC UiPath SRL:**

- to impose a fine in amount of Lei 346,598, the equivalent of EUR 70,000, for the deed found based on the findings report no. 13172 from 10.07.2023 based on Article 58 paragraph (2) letter i) and Article 83 paragraph (4) letter a) of Regulation (EU) 679/2016, for the breach of Article 25 paragraphs (1) and (2) and Article 32 paragraph (1) letter b) and paragraph (2) of the GDPR;
- to apply the corrective measures provided under Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 consisting of the implementation of a procedural mechanism and applied at regular time intervals, regarding the testing, evaluation and periodical evaluation of the efficiency of the measures taken, considering the risk

represented by the processing, in order to ensure a corresponding level of security and to avoid in the future similar security incidents – deadline: 30 days as of the communication of this decision.

This decision is subject to the procedure provided under Chapter VII of Regulation (EU) 2016/679, being provided to the concerned supervisory authorities.

According to Article 15 paragraph (6) of Law no. 102/2005, republished, when applying the fine, the official exchange rate of the National Bank of Romania of the 10th of July 2023, hour 15 was taken into consideration (EUR 1= Lei 4.9514).

According to the provisions of Article 17 paragraph (3) of Law no. 102/2005, republished, **SC UiPath SRL** has the obligation that within 15 days as of the communication of the report of findings (attached in copy) and of this decision to pay the fine, contrary following to be proceeded to enforcement.

The fine will be paid in the account of the State Treasury where **SC UiPath SRL** has his fiscal headquarters, account code 20A350102, within 15 days from communication, following for a copy of the receipt or payment order to be sent to the National Supervisory Authority for Personal Data Processing within the same deadline.

Article 83 from Regulation (EU) 679/2016 only provides for the maximum threshold of the fines that can be applied, not for their minimum limit, so that Article 28 paragraph (1) from GO no. 2/2001, with its subsequent amendments and completion, regarding the possibility to pay half of the minimum of the fine provided under the normative act, does not apply in this case.

This decision, together with the report of findings no. 13172 of 10.07.2023 (attached in copy), is communicated to **SC UiPath SRL** that has the right to challenge them, according to Article 17 from Law no. 102/2005:

”Article 17
(1) The data controller or processor may file an appeal against the report of the finding/sanctioning and/or the decision to apply the corrective measures, as the case may be, with the administrative contentious section of the competent court, within 15 days from handing, respectively from communication. The decision resolving the appeal can be appealed only by appeal. The appeal is judged by the competent court of appeal. In all cases, the competent courts are those in Romania.
(2) The report of finding/sanctioning or the decision of the president of the National Supervisory Authority unchallenged within 15 days from the date of handing, respectively the communication, constitutes an enforceable title without any other formality. Introducing the appeal provided in paragraph (1) suspends only the payment of the fine, until a final court decision is issued.
(3)The deadline of payment of the fine is 15 days from the date of handing, respectively from the date of communication of the minutes of finding/sanctioning or of the decision of the president of the National Supervisory Authority.

**President,**

[redacted]