Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	UiPath SRL (Organization)
Decision number (file number)	P2021-ND-218 (File #019482)
Date notice received by OIPC	December 25, 2020
Date Organization last provided information	December 25, 2020
Date of decision	November 8, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a provider of process automation software for enterprise customers. The Organization offers a training program – called UiPath Academy – for users of the software. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • country, • username associated with UiPath Academy, • UiPath Academy software certification level, if applicable, • the name of the company where the affected individuals are employed, and • an identifier by which UiPath in the past identified the user in the company's internal system (this identifier is obsolete and is no longer used by the Organization). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On approximately November 30, 2020, a third party notified the Organization that a file containing what appeared to be registration information of certain UiPath Academy participants was accessible on a publicly-available website. • The Organization investigated and determined that the content of the file identified by the third party matched the content of a file maintained by the Organization on a third-party cloud server. This file was last updated by the Organization on approximately March 17, 2020. • The Organization has not yet determined when the unauthorized user first accessed the file, but confirmed that the file was posted on the publicly-available website on or around November 30, 2020. • The Organization indicated that the incident resulted from human error, wherein an employee accidentally misconfigured the permissions for this file. • On December 2, 2020, the Organization correctly configured the file permission settings to prevent further unauthorized access.
Affected individuals	The incident affected 6,856 Canadians; however, the Organization is unable to determine how many are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Investigated to determine the cause and scope of the incident. • Eliminated the misconfiguration that led to the incident. • Expanded the use of technology that detects when file storage resources are at risk, including when permissions are set incorrectly. • Implemented a new training module on secure management of cloud resources. • Provided a pop-up notice and FAQs for affected individuals, via the UiPath Academy user portal.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 10, 2020.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization did not specifically identify any harms that might result from this incident, but its FAQs for affected individuals stated "This file did not contain any other personal or sensitive information such as passwords." In my view, a reasonable person would consider the contact, credential (username) and account information at issue, and particularly in conjunction with email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud, and to compromise other online accounts. These are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported, *Given the non-sensitive nature of the personal information impacted by this incident, [the Organization] does not believe that this incident gives rise to a real risk of significant harm to affected individuals.* In my view, a reasonable person would consider the likelihood of harm is decreased because the incident was caused by human error. However, the Organization was not able to determine when the unauthorized user first accessed the file, but confirmed that it was posted on a publicly available website. The Organization did not report how long the information was exposed before the breach was reported to it by a third party.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. A reasonable person would consider the contact, credential (username) and account information at issue, and particularly in conjunction with email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud, and to compromise other online accounts. These are significant harms. The likelihood of harm is decreased because the incident was caused by human error. However, the Organization was not able to determine when the unauthorized user first accessed the file, but confirmed that it was posted on a publicly available website. The Organization did not report how long the information was exposed before the breach was reported to it by a third party.	

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email on December 10, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner