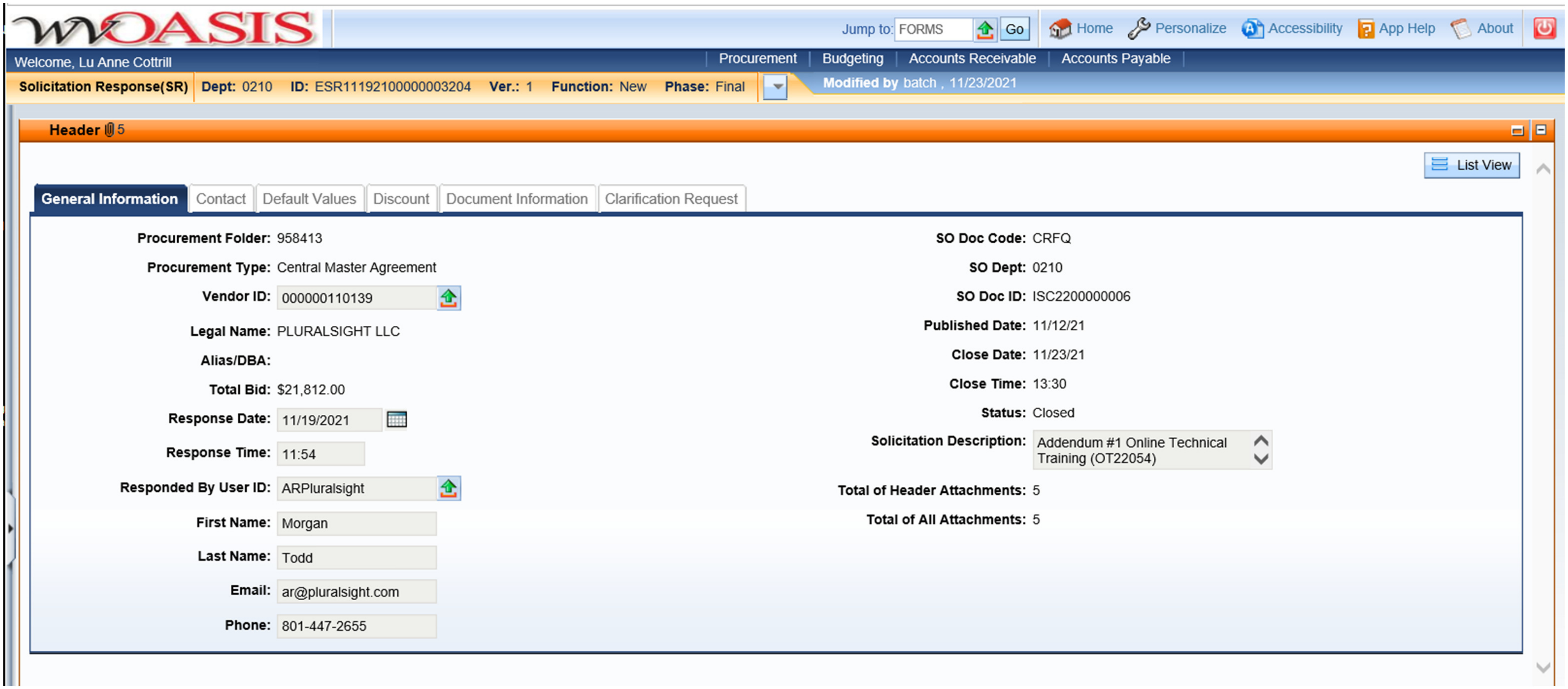
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at *wvOASIS.gov*. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at *WVPurchasing.gov* with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Solicitation Response(SR) **Dept:** 0210 **ID:** ESR11192100000003204 **Ver.:** 1 **Function:** New **Phase:** Final

Modified by batch , 11/23/2021

Procurement Folder: 958413

Procurement Type: Central Master Agreement

Vendor ID: 000000110139

Legal Name: PLURALSIGHT LLC

Alias/DBA:

Total Bid: $21,812.00

Response Date: 11/19/2021

Response Time: 11:54

Responded By User ID: ARPluralsight

First Name: Morgan

Last Name: Todd

Email: ar@pluralsight.com

Phone: 801-447-2655

SO Doc Code: CRFQ

SO Dept: 0210

SO Doc ID: ISC2200000006

Published Date: 11/12/21

Close Date: 11/23/21

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum #1 Online Technical Training (OT22054)

Total of Header Attachments: 5

Total of All Attachments: 5

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder:	958413
Solicitation Description:	Addendum #1 Online Technical Training (OT22054)
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2021-11-23 13:30	SR 0210 ESR11192100000003204	1

VENDOR

000000110139
PLURALSIGHT LLC

Solicitation Number: CRFQ 0210 ISC2200000006

Total Bid: 21812 **Response Date:** 2021-11-19 **Response Time:** 11:54:31

Comments: N/A

FOR INFORMATION CONTACT THE BUYER
Jessica L Hovanec
304-558-2314
jessica.l.hovanec@wv.gov

Vendor
Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Online Technical Training - User	28.00000	EA	779.000000	21812.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments: Please see the attached cost proposal. Pricing is $579 each for annual Professional License and $200 each for annual labs access.

Extended Description:

Online Technical Training - User

Item	Annual Price Per License	QTY	Total
Professional License	$579	28	$16,212
Labs	$200	28	$5,600

Combined total bid price: $21,812

Our pricing model is simple. We charge a per user per year license/subscription fee (USD). We do not charge per topic, for development, or updating of content. Pluralsight is a SaaS-based Platform (accessed via the web browser Web Browser) so all system, content and product updates are rolled out to all customers immediately without incurring deployment or implementation costs.

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Info Technology

Proc Folder:	958413		**Reason for Modification:**
Doc Description:	Addendum #1 Online Technical Training (OT22054)		Addendum #1
Proc Type:	Central Master Agreement		
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2021-11-12	2021-11-23 13:30	CRFQ 0210 ISC2200000006	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : Pluralsight, LLC

Address : 42 Future Way

Street :

City : Draper

State : UT **Country :** USA **Zip :** 84020

Principal Contact : Brandon Larsen

Vendor Contact Phone: (801) 867-6457 **Extension:**

FOR INFORMATION CONTACT THE BUYER
Jessica L Hovanec
304-558-2314
jessica.l.hovanec@wv.gov

Vendor Signature X Kylee Christensen **FEIN#** 20 - 1279619 **DATE** 11/18/2021

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

Addendum #1 is being issued to publish the Vendor Questions and Answers. Bid Opening Date & Time remain the same.

The West Virginia Purchasing Division is soliciting bids on behalf of the WV Office of Technology (WVOT) to establish an open-end contract for the purchase of online technical training, per the specifications and terms and conditions as attached hereto.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Online Technical Training - User	28.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Online Technical Training - User

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Technical Questions due by October 10, 2021 at 10:00 AM EST	2021-11-10

SOLICITATION NUMBER: CRFQ ISC2200000006
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as CRFQ ISC2200000006 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[ ] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[X] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

1) To attach the vendor questions and answers.

2) Bid opening date and time remain the same at November 23, 2021 at 1:30 PM EST

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ ISC2200000006

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[ ] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Pluralsight, LLC
Company

Kylee Christensen
Authorized Signature

111/18/2021
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

CRFQ ISC2200000006
Vendor Questions and Answers

Q1) Is the RFQ to renew an existing partnership? If so, who is the existing partner? How many licenses are being renewed? What was the cost for the previous year?
A1) Requesting copies of previously awarded contracts, other solicitations, or documents related to previous contracts through the question-and-answer process included in this solicitation is not appropriate. Requests for documentation of this nature can be obtained by interested parties through a Freedom of Information Act request.

Q2) Under general requirements section 3.1.1.3 - [redacted] offers hundreds of certification practice exams. Do they need to be created by the governing body or certifying vendor?
A2) They do not need to be created by governing body or certifying vendor.

Q3) 3.1.1.0 - "no longer than 30 questions". What is one of the assessments has 32 questions? Would that be a disqualification?
A3) The WVOT will accept up to 40 questions

Q4) 3.1.1.10 - This appears written specifically for Pluralsight. We can not meet this requirement - would this disqualify us from consideration?
A4) The WVOT is Vendor-agnostic, however, the visual dashboard is required.

Q5) Are you looking to have an online training program created and maintained, or to have someone source a system you already use?
A5) It will be the Vendor's solution, not housed in the State's system

Pluralsight Technical Response to Online Technical Training (OT22054) RFQ

Prepared for State of West Virginia
November 22, 2021
By Brandon Larsen

Table of Contents

Organization Details

Founded in 2004, Pluralsight is the leader in Saas-based technology skills development—helping enterprises grow and retain top talent, accelerate market leadership, and deliver on key business objectives. Our mission is to democratize technology skills and close the global technology skills gap.

Organizational highlights:

- 1,500+ expert authors
- 7,000+ courses and growing
- 1,700+ employees
- Trusted partner of more than 70% of Fortune 500 companies
- Headquarters in Utah, with office locations in Boston and Dublin and international affiliates in Australia, India, and Europe
- 17,700 business accounts with customers in 180 countries

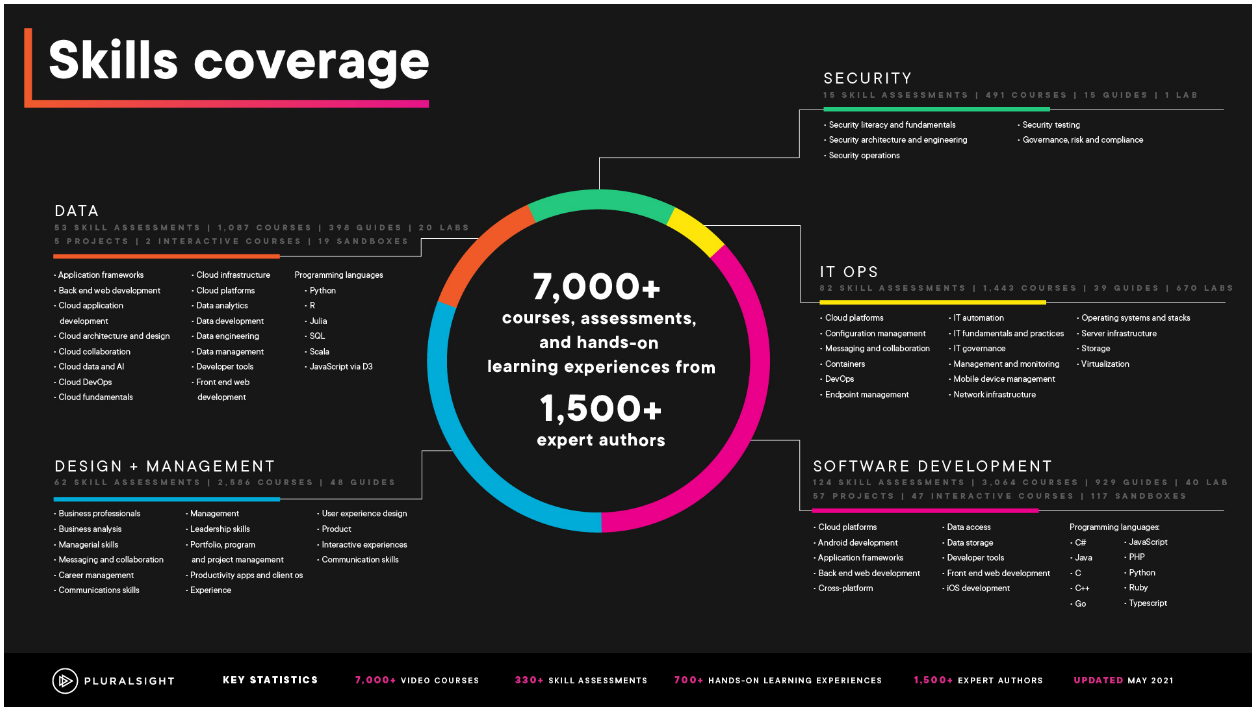
Below are the features included:

- **COURSE LIBRARY.** Upskill employees with 7,000+ expert-led courses across hundreds of topics.
- **PATHS.** Empower employees to build the right skills in the right order with course lists curated by experts.
- **CERTIFICATION PREP PATHS.** Get step-by-step guidance on what skills to learn (and in what order) to ace industry-recognized certification exams.
- **GUIDES.** Find answers faster with searchable articles on technology topics written by industry experts.
- **CHANNELS.** Combine sections of different courses or paths to create a custom skill development plan for your team aligned to your business objectives.
- **SKILL IQ.** Measure and index technology proficiency with quick, adaptive skill assessments.
- **ROLE IQ.** See if your employees have the skills they need to succeed in their roles and give them guidance on what to work on to get to the next level.
- **BADGES.** Employees can earn badges as they learn and reach new milestones.
- **COURSE COMPLETION CERTIFICATES.** Get verification that a course has fully been completed.
- **COURSE LEARNING CHECKS.** Employees can test their retention of course material with short, self-paced quizzes.
- **COURSE DISCUSSIONS.** Employees can engage with peers and the expert author in a community dedicated to each course.
- **EXERCISE FILES.** Course slides, instructor notes, source code and more are available for download.
- **MOBILE, TV APPS & OFFLINE VIEWING.** Employees can learn anytime, anywhere with mobile and desktop apps that allow for offline viewing.
- **EMAIL AND PHONE SUPPORT.** Questions? We're here for you. Email: Support@pluralsight.com, available 24/7. Phone: (801) 784-9007, available M-F from 8 a.m. - 5 p.m. MT
- **LICENSE MANAGEMENT TOOLS.** View and assign available licenses to ensure you're getting the most out of your plan.
- **CENTRALIZED BILLING.** Bring your organization's Pluralsight subscriptions into one plan to simplify billing.

- **API ACCESS.** See skill and role proficiency, user data, course usage and course completions from Pluralsight Skills in your internal systems, and configure bulk actions like team and channel management.
- **CERTIFICATION PRACTICE EXAMS.** Prepare employees for professional certifications with industry-leading practice exams.
- **INTERACTIVE COURSES.** Employees can practice as they learn with hands-on coding challenges and guided feedback.
- **PROJECTS.** Employees can practice skills in real-world scenarios using their own developer workspace.
- **BASIC ROLES ANALYTICS.** Get an overview of your team's role proficiency.
- **BASIC SKILLS ANALYTICS.** Get an aggregate view of skill levels for your organization to identify where strengths and gaps exist.
- **BASIC CHANNELS ANALYTICS.** See high-level metrics around channel completion rates and engagement.
- **CONFERENCES.** Watch recordings of today's most in-demand tech conferences.

Capabilities and Experience

Platform Capabilities



Skills coverage

7,000+ courses, assessments, and hands-on learning experiences from 1,500+ expert authors

SECURITY

15 SKILL ASSESSMENTS | 491 COURSES | 15 GUIDES | 1 LAB

- Security literacy and fundamentals
- Security architecture and engineering
- Security operations
- Security testing
- Governance, risk and compliance

DATA

53 SKILL ASSESSMENTS | 1,087 COURSES | 398 GUIDES | 20 LABS
5 PROJECTS | 2 INTERACTIVE COURSES | 19 SANDBOXES

- Application frameworks
- Back end web development
- Cloud application development
- Cloud architecture and design
- Cloud collaboration
- Cloud data and AI
- Cloud DevOps
- Cloud fundamentals
- Cloud infrastructure
- Cloud platforms
- Data analytics
- Data development
- Data engineering
- Data management
- Developer tools
- Front end web development

Programming languages
- Python
- R
- Julia
- SQL
- Scala
- JavaScript via D3

IT OPS

82 SKILL ASSESSMENTS | 1,443 COURSES | 39 GUIDES | 670 LABS

- Cloud platforms
- Configuration management
- Messaging and collaboration
- Containers
- DevOps
- Endpoint management
- IT automation
- IT fundamentals and practices
- IT governance
- Management and monitoring
- Mobile device management
- Network infrastructure
- Operating systems and stacks
- Server infrastructure
- Storage
- Virtualization

DESIGN + MANAGEMENT

62 SKILL ASSESSMENTS | 2,586 COURSES | 48 GUIDES

- Business professionals
- Business analysis
- Managerial skills
- Messaging and collaboration
- Career management
- Communications skills
- Management
- Leadership skills
- Portfolio, program and project management
- Productivity apps and client os
- Experience
- User experience design
- Product
- Interactive experiences
- Communication skills

SOFTWARE DEVELOPMENT

124 SKILL ASSESSMENTS | 3,064 COURSES | 929 GUIDES | 40 LAB
57 PROJECTS | 47 INTERACTIVE COURSES | 117 SANDBOXES

- Cloud platforms
- Android development
- Application frameworks
- Back end web development
- Cross-platform
- Data access
- Data storage
- Developer tools
- Front end web development
- iOS development

Programming languages:
- C#
- Java
- C
- C++
- Go
- JavaScript
- PHP
- Python
- Ruby
- Typescript

PLURALSIGHT KEY STATISTICS 7,000+ VIDEO COURSES 330+ SKILL ASSESSMENTS 700+ HANDS-ON LEARNING EXPERIENCES 1,500+ EXPERT AUTHORS UPDATED MAY 2021

Our content

Skill up with thousands of on-demand video courses, teaching the most high-demand technologies, tools, processes and best practices across the IT industry. We add 100+ new courses each month. Inform your technology strategy with courses authored by trusted industry experts. Enable your teams to adapt quickly and create the future-focused technology needed by your company.

With interactive courses and projects, your team can practice and apply new skills in risk-free environments and get guided feedback along the way. They'll have confidence their skills are ready for critical projects. Here is a summary of some of the content we offer:

CLOUD COMPUTING - Create a successful cloud strategy and give your team the skills they need to tackle modern cloud roles, with broad and deep skills coverage in Microsoft Azure, AWS, Google Cloud and more.

MACHINE LEARNING / AI - Build AI and machine learning skills with courses and assessments on Python, TensorFlow, R, Neural Networks, Microsoft Cognitive Services and others to create more engaging experiences for your customers.

SOFTWARE DEVELOPMENT - Take your skills to the next level with courses on the most popular programming languages, developer tools, software practices and application development platforms. Gain a deep understanding of how to build, deploy, secure and scale everything from web apps to mobile apps using C#, Java, Angular, JavaScript and more. Learners can stay up to speed on the ever-changing landscape of emerging software development tools and techniques.

- Web Development
- Mobile Development
- JavaScript
- C#
- Python
- Node.js

IT OPERATIONS - Build your toolkit with the skills you need to excel in your job, including security best practices, server infrastructure and virtualization. Study for your next certification, whether it's the MCSA, CCNP, Network+ or dozens more, with courses designed by seasoned pros.

- IT Certifications
- Security
- Database Administration
- Virtualization
- IT Networking
- Servers

INFORMATION & CYBER SECURITY - Empower your entire organization to safeguard against rising security threats.

- IT Certifications
- Security
- Database Administration
- Virtualization
- IT Networking
- Servers

DATA PROFESSIONAL - Learn in-demand skills from experts with real-world experience in data analytics, engineering and science. Our training covers everything from big data, cloud, mobile and Internet of Things (IoT), and how to analyze and gain value from this data in tools like R, SQL Server, Tableau and more.

BUSINESS PROFESSIONAL - Become a well-rounded professional with courses that will help you navigate a successful career and become more productive. Improve your project management, leadership and communication skills, and get guidance on how to plan your career and land your next opportunity.

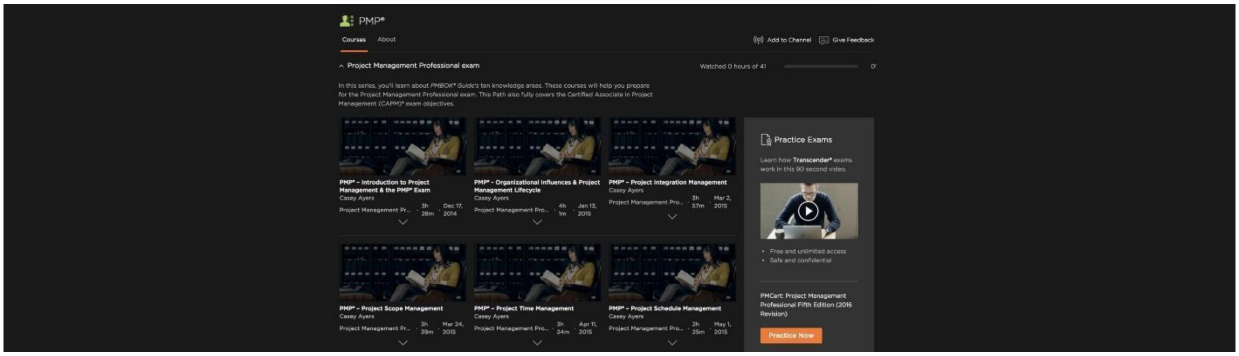
You can browse all paths and courses here: https://www.pluralsight.com/browse

Required skill areas in beginner, intermediate and advanced:

Skill Area	**Covered Y/N**
ASP.NET MVC 5	**Y**

ASP.NET Core	**Y**
API Development in ASP .NET Core	**Y**
C# Programming	**Y**
Entity Framework	**Y**
JavaScript	**Y**
AngularJS	**Y**
Visual Studio 2019	**Y (beginner, intermediate)**
Ethical Hacking	**Y**
DevSecOps	**Y**
DevOps	**Y**
Certified Business Analysis Professional (CBAP)	**Y**
Project Management Professional (PMP)	**Y**
Program Management Professional (PgMP)	**Y (beginner)**
PMI Agile Certified Practitioner (PMI-ACP)	**Y (intermediate)**
Scrum Framework	**Y (beginner, intermediate)**
Lean Six Sigma	**Y**
Citrix CCA-V and CCP-V: Citrix Virtual Apps and	**Y (intermediate)**
Desktop (CV AD) Administration	**Y (intermediate)**
AWS Certified Solution Architect	**Y**
AWS Certified DevOps Engineer	**Y (intermediate, advanced)**
AWS Automate Infrastructure with CloudFormation	**Y**
AWS Architecting	**Y**
G Suite Administration	**Y (Google Workspace Administration is the newer version, beginner)**
Getting Started with Google Workspace	**Y (beginner, intermediate)**
Window PowerShell	**Y**

Window PowerShell: Scripting and Toolmaking	**Y**
Designing and Implementing Microsoft DevOps Solutions	**Y**
Configuring Identity and Access in Microsoft Azure	**Y**
Building Data Storage Solutions with Microsoft Azure Services	**Y**
Building and Administering PowerApps	**Y**
Microsoft Azure AI Engineer	**Y**
Microsoft Azure App Service	**Y**
Microsoft Azure Architect Design	**Y (advanced)**
Microsoft Azure Architect Technologies	**Y (beginner, advanced)**
Microsoft Azure Data Engineer	**Y**
Microsoft Azure Data Solutions	**Y**
Microsoft Azure Infrastructure	**Y**
Microsoft Azure Solutions	**Y**
Microsoft Azure Storage	**Y**
Microsoft Azure Deployment & Integration	**Y**
Microsoft Azure Data Solutions	**Y (duplicate is above)**
Microsoft Azure Monitoring	**Y**
Microsoft Power Platform	**Y**
Microsoft Power BI for Analysts	**Y**



Project Management Professional exam

Watched 0 hours of 41

In this series, you'll learn about *PMBOK® Guide's* ten knowledge areas. These courses will help you prepare for the Project Management Professional exam. This Path also fully covers the Certified Associate in Project Management (CAPM)® exam objectives.

PMP® – Introduction to Project Management & the PMP® Exam
Casey Ayers
Project Management Pr... · 3h 28m · Dec 17, 2014

PMP® - Organizational Influences & Project Management Lifecycle
Casey Ayers
Project Management Pro... · 4h 1m · Jan 13, 2015

PMP® – Project Integration Management
Casey Ayers
Project Management Pro... · 3h 57m · Mar 2, 2015

PMP® – Project Scope Management
Casey Ayers
Project Management Pr... · 3h 39m · Mar 24, 2015

PMP® – Project Time Management
Casey Ayers
Project Management Pro... · 3h 24m · Apr 11, 2015

PMP® – Project Schedule Management
Casey Ayers
Project Management Pro... · 2h 25m · May 1, 2015

Learn how **Transcender®** exams work in this 90 second video.

- Free and unlimited access
- Safe and confidential

PMCert: Project Management Professional Fifth Edition (2016 Revision)

Certification Practice Exams

Whether you're looking to prepare for your own certifications or are encouraging employees to get certified, your road to exam-readiness starts with Pluralsight. You and your team can prepare for exams with unlimited access to Kaplan's practice tests to improve the likelihood of passing your certification exams—saving hundreds, if not thousands of dollars.

Once you're ready to take a practice exam, you can conveniently navigate to Kaplan right from the certification path. Learn from different test modes – including optimized tests, practice tests and flashcards – to assess your readiness. You can also view incorrect answers with detailed explanations to learn as you go. After completing practice exams, you can see your exam history and results right within Pluralsight.

Certifications

With 100+ paths aligned to leading certifications in cloud, IT, security and agile methodologies, you can upskill your teams to meet your most important initiatives.

Cloud Certifications include:

- AWS certified
- Microsoft Certified
- Google Cloud (Qwiklabs integration)
- Salesforce Certified
- CompTIA

IT & DevOps Certifications include:

- ITL®4 *
- Cisco
- CompTIA
- Kubernetes
- Microsoft 365
- Red hat
- Linux
- Citrix
- VMware
- Windows Server
- Terraform

Security Certifications include:

- CISSP®
- CEH Prep
- CISM®
- SSCP®
- CompTIA
- CSSLP®
- Azure
- AWS
- CRISC™
- CompTIA
- CCSP

Project Management and Business Analysis Certifications include:

- PMP®
- PgMP®
- PRINCE2® *
- Learn Six Sigma
- CompTIA
- ICAgile
- PMI-PBA®
- CCBA®

- IIBA®-AAC

Please note certifications for PRINCE2 and ITL are only provided with the purchase of an examination voucher at an additional cost. If these are required, please advise and pricing can be provided. We do not mark up these charges.

Labs
To build skills with confidence, your team needs a way to practice what they're learning. Pluralsight labs provide learners with a safe, provisioned environment so they can develop and test skills without the risk. By completing tasks similar to common ones tech teams tackle every day, your team can get comfortable applying their skills in real-world scenarios and get feedback to keep improving.

Have confidence your team can deliver
With guided, hands-on practice, your team can deepen their knowledge in key areas and build the skills they need to deliver on your big objectives.

Practice without risks
Safe, provisioned environments allow your team to bypass time-consuming setups and downloads and get straight to practicing—all without the fear of impacting your org's systems.

Streamline skill development
Forget managing multiple vendors. Pluralsight is the destination for every step in your team's journey from learning to practicing and applying new skills. With labs available across multiple key domains, you can upskill your teams for any initiative.

Labs are currently available in the following technologies:
Cloud

- Labs across AWS,GCP, and Azure
- Networking
- Virtual Private Cloud (VPC)
- Compute
- Monitoring and logging
- Cloud security
- Data and Databases
- Cloud Application Development
- Serverless
- Identity and Access Management
- CI/CD Pipelines
- Cloud Storage
- And more

Developer

- HTML and CSS
- JavaScript
- Python
- Flask
- Node.js
- R
- ASP.NET
- C#
- Spring Framework
- Django
- Go
- Java
- React
- Angular
- Vue.js

Data

- Python
- R

Sandboxes (Included with Labs)
Practice is an important part of building new skills. As a leader, you need to provide your team with a place to test out what they're learning without risk to your org's systems. Sandboxes provide your team with safe, provisioned environments where employees can

deepen their skills through more advanced, independent practice. And with no limitations to what they can explore, your team can practice completing tasks just like the ones they'll be tackling on the job.

Create project-ready teams
Sandboxes are unconstrained environments that allow your team to immediately apply their skills in real world scenarios and scenarios specific to your org's unique context.

Keep your systems secure
With risk-free, provisioned environments, your team can skip the time-consuming set up and get straight to practicing, all while keeping your organization's systems secure.

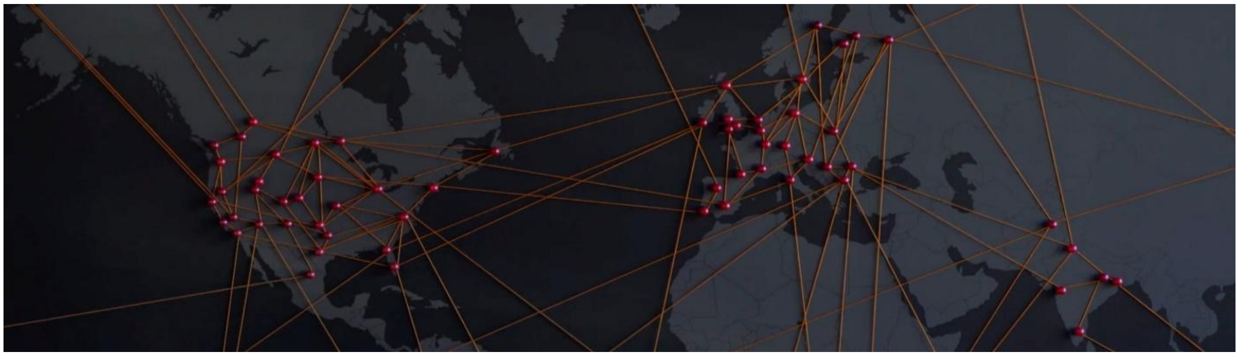
Streamline skill development
Forget managing multiple vendors. Pluralsight is the destination for every step in the skill development journey from learning to practicing and applying new skills. With sandboxes available across multiple key domains, you can upskill your teams for any initiative.

Sandboxes are available for the following technologies:
Developer

- ASP.NET
- C#
- Spring Framework
- HTML and CSS
- Javascript
- MySQL
- Git
- Java
- TypeScript
- PHP
- Vue.js
- SQL
- Kotlin
- Bootstrap
- LINQ
- React
- Angular
- Python
- Node.js
- C++

Data

- Python
- R
- SQL
- Apache Spark
- Machine Learning Literacy



Our authors

Our author ecosystem consists of hundreds of proven experts who not only have the passion, but have the teaching skills to spread their knowledge to the world. Whether you're a novice or an expert, our authors provide the content needed to take your skills to the next level.

On average, we only publish three out of every 1,000 content proposals we receive. Why? To ensure every course we publish meets the quality standards our customers demand.

To ensure your team members are learning from the highest quality content, Pluralsight does not simply aggregate content from across the web. Rather, the Pluralsight quality/review process is interwoven into our entire production system and starts before the course is recorded—with the Author audition process and quality standards.

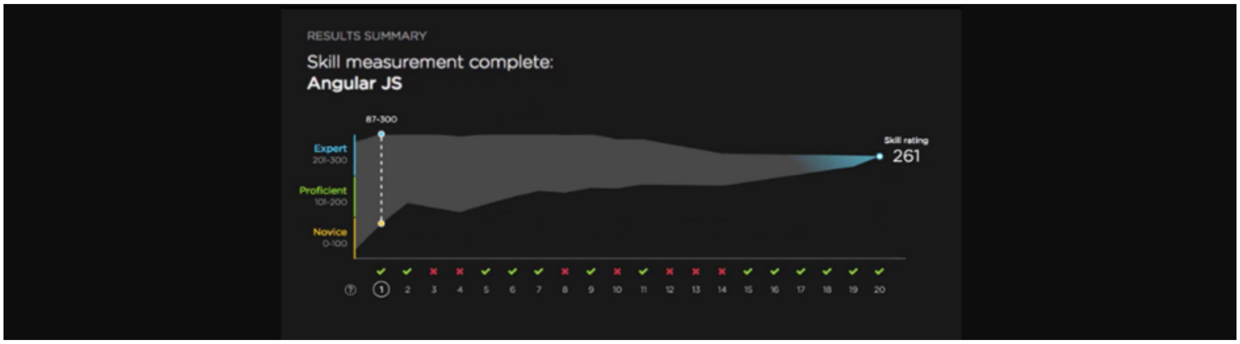
The initial vetting of prospective authors before interview(s) and discovery is done primarily through networking and research (their public body of work, their influence in the industry, etc.). All prospective Authors are asked to create an audition video that we coach them through. It is then reviewed by our acquisition and curriculum team across multiple criteria to determine if the necessary skills, information, delivery and other demonstrated criteria are acceptable. If they make it through this stage, the Author then goes through an in-depth on-boarding process which includes a number of trainings and access to our "Author Kit".

The global Pluralsight Author network now includes 1,500+ subject matter experts. Overall acceptance rate for new Authors is less than 10%, with an average 18 years of professional experience.

Iris

Iris is a new way to measure and evolve technology skills. This artificial intelligence powers our assessment algorithm and guides learners to the skills your business needs now. The more they learn about technology, the more Iris learns about their skills. Iris uses data to create a smarter, personalized skill development journey. It is the science behind our platform.

Iris is disrupting skill development for individuals, businesses and the world. With Iris, learners can validate their current proficiency and feel confident they know where to focus on improving their skills. Pluralsight is at the center of the tech skills ecosystem and the future of a new world for technology certifications. And it starts with the ability to measure an individual's skills.



RESULTS SUMMARY

Skill measurement complete:
Angular JS

Skill IQ

With Skill IQ, you can see the strengths, weaknesses and progress of your team members, so you can measure growth and put the right people on the right projects.

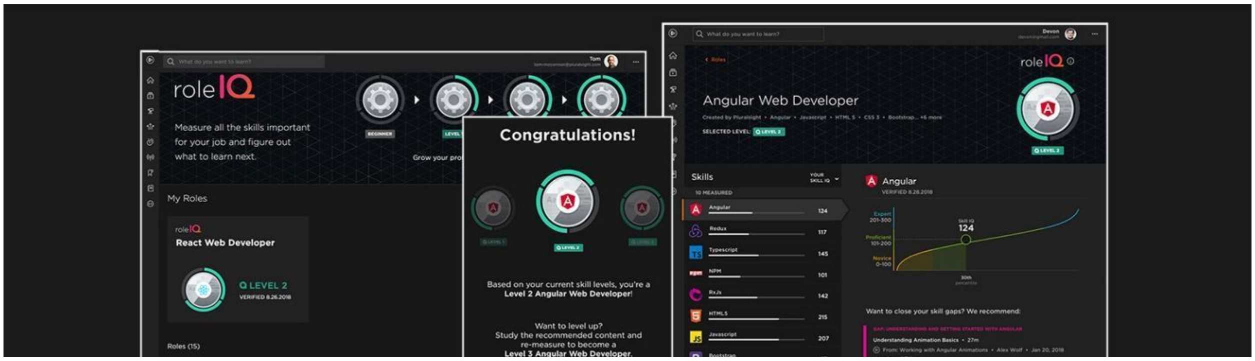
For Leaders:
Skill IQ is the most accurate and current measurement of technology skills today. As a leader, Skill IQ allows you to index your team's proficiency, identify gaps against your priorities and accelerate skill development in the topics impacting your tech strategy.
HOW IT WORKS:
1. Employees take an adaptive skill assessment, which measures proficiency in a topic in as little as 20 questions.
2. Once they complete the assessment, they'll receive their Skill IQ, a ranking from 0-300 indicating if they are Novice, Proficient or Expert.
3. Based on their Skill IQ, employees will receive personalized recommendations in courses and clips to help them fill gaps in knowledge and skip over content they already know.
4. After they've spent time working on their skills, employees should retake the skill assessment to see how they've grown.

For Learners:
Skill IQ is the fastest and most accurate way to see where your skills are at, discover gaps in knowledge and get personalized recommendations on how to improve.

Skill IQ empowers you to understand your own proficiency and streamlines your path to expertise. You can also share your results on Stack Overflow, LinkedIn and Twitter to showcase your expertise within your network.
HERE'S HOW IT WORKS:
1. Take a skill assessment: Our skill assessments are adaptive, meaning we can reliably identify your proficiency in as little as 20 questions.
2.Get your Skill IQ: After you've completed an assessment, we'll benchmark your proficiency against other professionals around the world to give you your Skill IQ.
3.Understand your results: Your Skill IQ will tell you where your skill ranks using the following scale:

NOVICE: 1-100 (or 1-20 percentile)
PROFICIENT: 101-200 (or 21-80 percentile)
EXPERT: 201-300 (or 81-100 percentile)

4.Grow your skills: Based on your Skill IQ, we'll recommend courses and short video clips to fill knowledge gaps. 5.Reassess: After working on your skills, retake the assessment to see how you've improved.



Measure all the skills important for your job and figure out what to learn next.

Congratulations!

Based on your current skill levels, you're a **Level 2 Angular Web Developer!**

Want to level up?
Study the recommended content and re-measure to become a **Level 3 Angular Web Developer.**

Angular Web Developer
Created by Pluralsight • Angular • Javascript • HTML 5 • CSS 3 • Bootstrap... +6 more
SELECTED LEVEL: LEVEL 2

Angular	124
Redux	117
Typescript	145
NPM	101
RxJs	142
HTML5	215
Javascript	207
Bootstrap	

Want to close your skill gaps? We recommend:
GAP: UNDERSTANDING AND GETTING STARTED WITH ANGULAR
Understanding Animation Basics • 27m
From: Working with Angular Animations • Alex Wolf • Jan 20, 2018

Role IQ

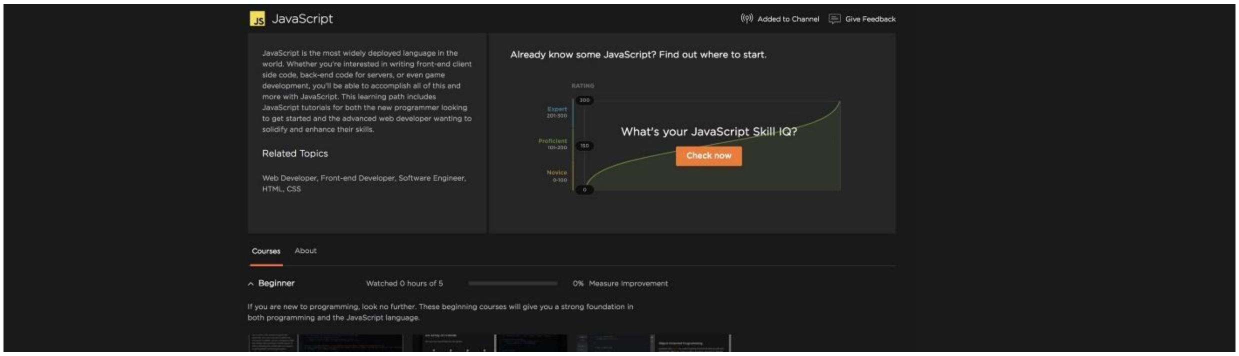
We also offer Role IQ, which shows you and your team members the skills you need to succeed, where skills gaps exist and what you need to work on to reach role mastery. Leaders can customize roles to fit specific business needs and help everyone build the right skills.

For Leaders:

While Skill IQ measures proficiency in a specific skill, Role IQ measures proficiency in a role by assessing the collective skills that make up that role. As a leader, Role IQ enables you to upskill employees into modern tech roles and onboard new hires faster.
HOW IT WORKS
1. Employees complete all skill assessments for a given role.
2. Based on their assessment results, they'll receive their Role IQ, indicating their level of technical proficiency in their role.
3. Role IQ will serve content recommendations to help employees fill gaps and get to the next level.

For Learners
While Skill IQ shows you your proficiency in a specific skill, Role IQ shows you your proficiency in a role by assessing you on the collective skills that make up that role.

As technology evolves, the responsibilities in your role will change too. You may even need to take on roles that don't exist yet today. Role IQ ensures you have the right skills to succeed.
HERE'S HOW IT WORKS:
1. Move from chaos to clarity: Role IQ shows you which skills you need to succeed, where skills gaps exist and what you need to work on to reach role mastery.
2.Speed up success: Discover the skills gaps holding you back in your role and fill them fast. Role IQ recommends learning opportunities to help you reach the next level and prepare for projects without slowing down progress.
3.Grow your skills: By working on the skills related to your role, you can move to the next level. Retake the skill assessments related to your role to see if you're keeping up with important changes.



JavaScript

JavaScript is the most widely deployed language in the world. Whether you're interested in writing front-end client side code, back-end code for servers, or even game development, you'll be able to accomplish all of this and more with JavaScript. This learning path includes JavaScript tutorials for both the new programmer looking to get started and the advanced web developer wanting to solidify and enhance their skills.

Related Topics

Web Developer, Front-end Developer, Software Engineer, HTML, CSS

Already know some JavaScript? Find out where to start.

What's your JavaScript Skill IQ?

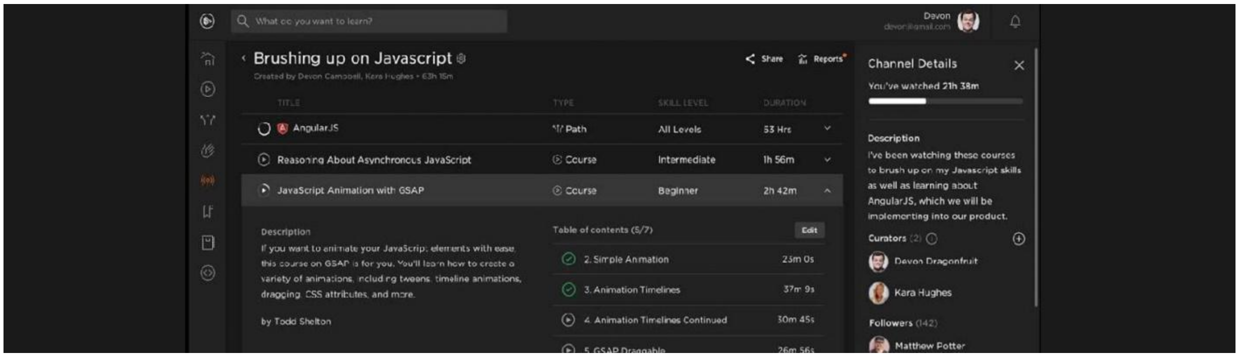
Beginner — Watched 0 hours of 5 — 0% — Measure Improvement

If you are new to programming, look no further. These beginning courses will give you a strong foundation in both programming and the JavaScript language.

Paths

It can be tough to know where to start learning. Paths combine specific courses and tools into one experience to teach you any given skill from start to finish. Paths are aligned to an individual's knowledge level, to help you and your team develop the right skills in the right order.

Our paths combine courses and tools into one experience so you can effectively learn a new skill in the right order. Individuals can measure knowledge and skill development over time by completing associated learning checks, skill assessments and certification practice exams.



What do you want to learn?

Devon

Brushing up on Javascript

Created by Devon Campbell, Kara Hughes • 63h 15m

Share | Reports

TITLE	TYPE	SKILL LEVEL	DURATION
AngularJS	Path	All Levels	53 Hrs
Reasoning About Asynchronous JavaScript	Course	Intermediate	1h 56m
JavaScript Animation with GSAP	Course	Beginner	2h 42m

Description

If you want to animate your JavaScript elements with ease, this course on GSAP is for you. You'll learn how to create a variety of animations, including tweens, timeline animations, dragging, CSS attributes, and more.

by Todd Shelton

Table of contents (5/7) Edit

2. Simple Animation	23m 0s
3. Animation Timelines	37m 9s
4. Animation Timelines Continued	30m 45s
5. GSAP Draggable	26m 56s

Channel Details

You've watched 21h 38m

Description

I've been watching these courses to brush up on my Javascript skills as well as learning about AngularJS, which we will be implementing into our product.

Curators (2)

Devon Dragonfruit

Kara Hughes

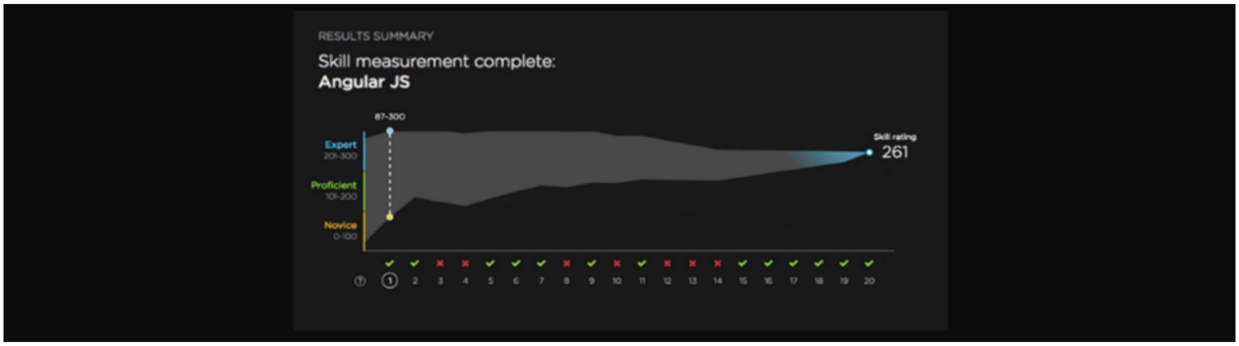
Followers (142)

Matthew Potter

Channels

Channels are an intuitive way to organize and share Pluralsight content so you can reach your learning goals and business objectives more effectively. Create channels to curate content for your own learning, for team development or to share learning journeys with the world.

Channels empower operational leaders to curate custom learning plans to address desired outcomes. With channels, you can align learning to your key business objectives and guide teams towards skills that will make them successful.

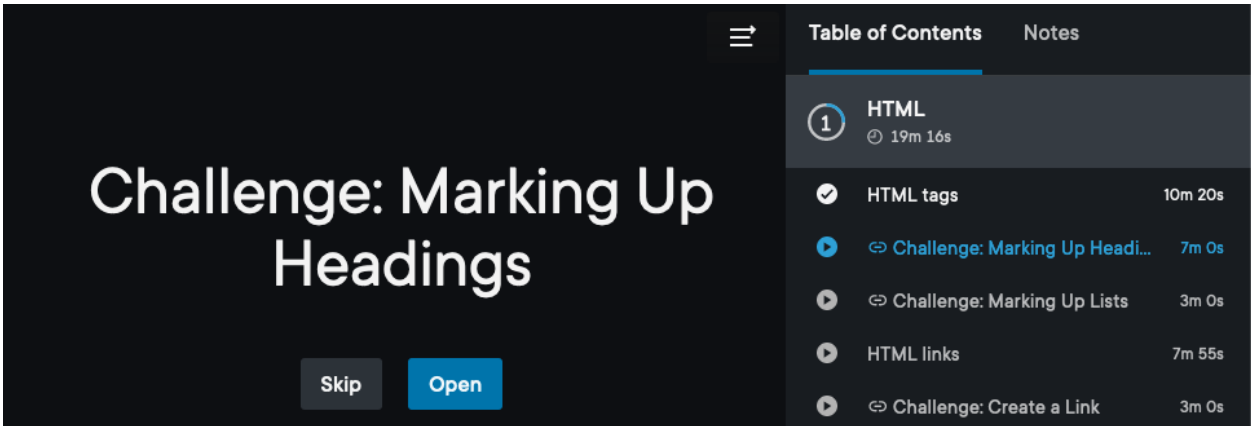


RESULTS SUMMARY

Skill measurement complete:
Angular JS

Skill Assessments

Get an accurate read on your skills. In as little as five minutes, you and your team members can see exactly where your skills stand on dozens of technologies, allowing you to pinpoint areas of expertise and improvement. Skill assessments measure your knowledge of a particular skill and gives you an objective rating of where you stand in relation to other technologists around the world with your Skill IQ.



Challenge: Marking Up Headings

Skip Open

Table of Contents Notes

1 HTML 19m 16s

HTML tags 10m 20s

Challenge: Marking Up Headi... 7m 0s

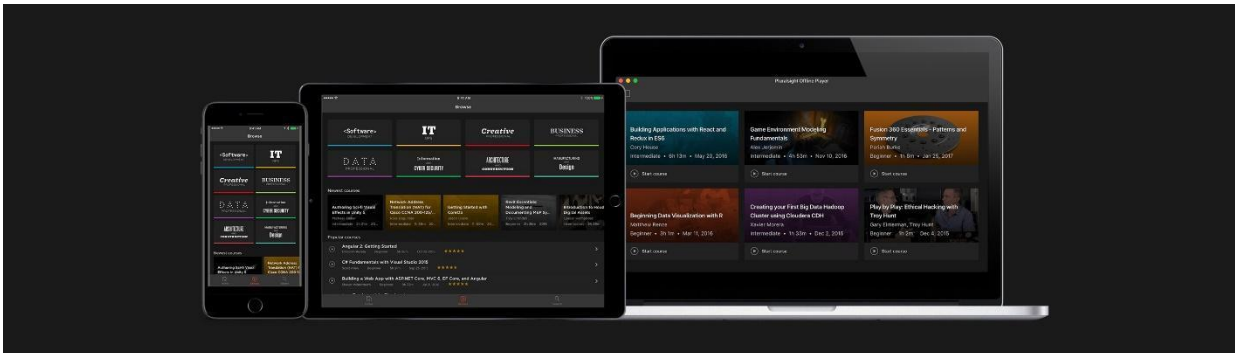
Challenge: Marking Up Lists 3m 0s

HTML links 7m 55s

Challenge: Create a Link 3m 0s

Interactive Courses

With interactive courses, your team can practice as they learn with hands-on coding challenges and guided feedback in the form of hints error messages and answers. Empower learners to take skill development into their own hands with experiences that include hands-on coding challenges and guided feedback. Learners start by watching a video to learn a concept, then test their knowledge through a series of challenges in a browser environment.



Mobile, Desktop, and Streaming Apps

Make your learning fit your schedule with an on-demand platform that's ready whenever and wherever you are. Whether you're taking a break at work, in the comfort of your home or on your commute, you can pick up exactly where you left off and keep learning with Pluralsight.

Easily stream or download training on your iPhone, iPad, Android phone or tablet. No internet? No problem. Download courses and learn with offline player apps for Windows (requires Windows 7 and up) and Mac (requires OS X 10.11 and up). You can extend your learning to the big screen with apps for Apple TV, Amazon Fire TV and Roku.

Contractual Terms

Pluralsight has responded in good faith to the terms of this RFP. However, Pluralsight rejects the idea that the terms found in this RFP will constitute a final and binding agreement. If Pluralsight is awarded the bid under this RFP, Pluralsight prefers to negotiate from Pluralsight's form of MSA which has been attached hereto. Pluralsight's form of MSA best outlines the SaaS services provided by Pluralsight. Pluralsight will be happy to entertain any edits required by the State of West Virginia to Pluralsight's form of agreement and, if awarded would enter into such negotiations in good faith. We have redlined the contract document that was provided below.

Customer DPA (Controller:Processor)

I. Introduction

The undersigned, Pluralsight, LLC for and on behalf of itself and its Affiliates, (collectively, "Pluralsight") and for and on behalf of itself and its Affiliates (collectively, "Customer") agree to the terms of this Data Protection Addendum ("DPA") which sets forth their obligations with respect to the processing and security of Customer Data in connection with the Products provided by Pluralsight to Customer, (collectively, the "Parties") in conjunction with the terms and conditions entered into between the Parties for the Products. Such terms and conditions and any other terms set out by Pluralsight in conjunction with the Products, including without limitation Pluralsight's Terms of Use, Sales Orders and terms for professional services, shall be collectively referred to as the "Agreements." The DPA is deemed incorporated by reference into the Agreements. The provision of third-party products and services made available to Customer via the Platform are governed by separate terms provided to Customer, including different privacy and security terms as provided by such third party.

For the purpose of this DPA and compliance with the GDPR, the Parties agree to enter into the Standard Contractual Clauses issued by the EU Commission on June 4, 2021. Where applicable, and as set out in Annex 1, for transfers of Personal Data from a Customer established in the EEA, as a data controller, to a Pluralsight entity established in a country outside the EEA, as a data processor, the Parties agree to enter into the Controller to Processor SCCs. The Controller to Processor SCCs will only apply to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in Customer's Agreements, the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Pluralsight Privacy Policy that otherwise may apply to processing of Customer Data as defined herein. Where the SCCs apply and as required by Clause 5 of the Controller to Processor SCCs, the Controller to Processor SCCs prevail over any other term of the DPA Terms and terms of the Agreements.

II. Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the Agreements. The following defined terms are used in this DPA:

"Affiliate" means, (i) in the case of Pluralsight, any entity controlled by Pluralsight, LLC, and (ii) in the case of Customer, any entity controlled by Customer. For purposes of the preceding sentence, "control" means the direct or indirect ownership of more than 50% of the voting interests of an entity.

"Controller to Processor SCCs" or ("SCCs") means the set of Standard Contractual Clauses set out in Module II of the European Commission decision 2021/914, dated 4 June 2021 and set out in Annex 1 of this DPA.

"Customer Data" means all data, including all text, sound, video, or image files related to Customer that are provided to Pluralsight by Customer through use of the Platform. Customer Data also includes Customer's Personal Data that is Customer Data.

"Data Protection Requirements" means the GDPR, Local EU/EEA/Switzerland Data Protection Laws, the UK Data Protection Act 2018, the UK GDPR and any other applicable laws, regulations, and other legal requirements relating to privacy and data security, including any future legislation on data protection and security in the United Kingdom.

"DPA Terms" means the terms in this DPA.

"EEA" means the European Economic Area.

"EU" means the European Union.

"GDPR" means 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).

"Local EU/EEA/Switzerland Data Protection Laws" means any legislation and regulation implementing the GDPR.

"Non-Pluralsight Products" shall bear the meaning set forth in the Agreements and where not defined therein shall mean any third-party products or services made available ancillary to the Products whether via the Platform or otherwise and are subject to the third-party's terms of use, DPA and privacy policy.

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Platform" shall bear the meaning set forth in the Agreements and where not defined therein shall mean Pluralsight's training platform with applications and features as more fully described in one or more Sales Orders.

"Product(s)"means the SaaS services and associated professional services provided in conjunction with the Platform excluding Non-Pluralsight Products and all on-prem applications.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data. Security Incident also includes any personal data breach as defined by the GDPR. A Security Incident does not include any activity which does not result in unauthorized access to Customer Data including without limitation, denial of service and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful login attempts, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

"Standard Contractual Clauses" means the standard data protection clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and implemented by the European Commission decision 2021/914, dated 4 June 2021.

"Sub-processor" means other processors used by Pluralsight to process Customer Data, as described in Article 28 of the GDPR.

"UK GDPR" means the General Data Protection Regulation as incorporated into UK law by the UK Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, (each as amended, replaced, or superseded).

The terms "data importer" and "data exporter" have the meanings assigned in the Standard Contractual Clauses.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether the GDPR applies.

III. DPA Terms

A. Compliance with Laws

Pluralsight will comply with all laws and regulations applicable to its provision of the Products including security breach notification law, Data Protection Requirements and the SCCs. However, Pluralsight is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not applicable to SaaS providers. Pluralsight does not determine whether Customer's Data includes information subject to any such specific law or regulation.

Customer must comply with all laws and regulations applicable to its use of Products including laws related to biometric data, confidentiality of communications, Data Protection Requirements and the SCCs. Customer is responsible for determining whether the Products are appropriate for storage and processing of information subject to any specific law or regulation and for using the Products in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of Products.

B. Scope

The DPA Terms apply to all Products except as described in this section.

The DPA Terms will not apply to any Non-Pluralsight Product which is governed by the privacy and security terms in the applicable Non-Pluralsight Product-specific terms.

For clarity, the DPA Terms apply only to the processing of Personal Data in environments controlled by Pluralsight and Pluralsight's Sub-processors. This includes Personal Data processed by Pluralsight when providing the Products but does not include Personal Data that remains on Customer's premises or in any Customer selected third-party operating environments.

C. Limits on Updates

When Customer renews or purchases a new subscription to a Product, the then-current DPA Terms will apply and will not change during Customer's subscription for that Product.

D. New Features, Supplements, or Related Software

Notwithstanding the foregoing limits on updates, when Pluralsight introduces features, offerings, supplements or related Products that are new (i.e., that were not previously included with the Products), Pluralsight may provide terms or make updates to this DPA that apply to Customer's use of those new features, offerings, supplements or related Products. If those terms include any material adverse changes to the DPA Terms, Pluralsight may provide Customer a choice to use the new features, offerings, supplements, or related Products, without loss of existing functionality of a generally available Product. If Customer does not install or use the new features, offerings, supplements, or related Products, the corresponding new terms will not apply.

E. Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, Pluralsight may modify or terminate a Product in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects Pluralsight to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for Pluralsight to continue offering the Product without modification, and/or (3) causes Pluralsight to believe the DPA Terms or the Product may conflict with any such requirement or obligation.

Pluralsight may amend the terms of this DPA where required to comply with Data Protection Requirements and to reflect any changes in the applicable Data Protection Requirements, so long as any such revisions continue to ensure the protection of Personal Data processed by Pluralsight in the course of providing the Products to Customer.

F. Electronic Notices

Pluralsight may provide Customer with information and notices about Products electronically, including via email, an RSS Feed, or through a web site that Pluralsight identifies. Notice is given as of the date it is made available by Pluralsight.

G. Nature of Data Processing; Ownership

Pluralsight will use and otherwise process Customer Data only as described and subject to the limitations provided below (a) to provide Customer the Products in accordance with Customer's documented instructions, and (b) for business operations incident to providing the Products to Customer.

1. Processing to Provide Customer the Products and Services

For purposes of this DPA, "to provide" a Product consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, and repairing problems including Security Incidents);
- Ongoing improvement (installing the latest updates if and when available and making improvements to user productivity, reliability, efficacy, quality, and security); and
- Providing services ancillary to the Products.

2. Processing for Business Operations

For purposes of this DPA, "business operations" consist of the following, each as incident to delivery of the Products to Customer: (1) billing and account management; (2) compensation (e.g., calculating Pluralsight employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud and cybercrime; (5) improving functionality of the Products and the Customer experience; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Processed Data outlined below). Pluralsight will comply with its obligations, as an independent data controller, under the GDPR for such use.

H. Disclosure of Processed Data

Pluralsight will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law and in any event in accordance with clause 14 and 15 of the Controller to Processor SCCs. For purposes of this section, "Processed Data" means: Customer Data and any other data processed by Pluralsight in connection with the Products that is Customer's confidential information under the Agreements. All processing of Processed Data is subject to Pluralsight's obligation of confidentiality under the Agreements.

Pluralsight will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Pluralsight with a demand for Processed Data, Pluralsight will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Pluralsight will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Pluralsight will promptly notify Customer unless prohibited by law. Pluralsight will reject the request unless required by law to comply. If the request is valid, Pluralsight will attempt to redirect the third party to request the data directly from Customer.

Pluralsight will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Pluralsight is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Pluralsight may provide Customer's basic contact information to the third party.

With respect to clause 15. 1 (c) of the Controller to Processor SCCs, if permitted by the laws of the country of destination, Pluralsight will provide to Customer, upon Customer's written request, at regular intervals and in no event more than once in a twelve months' period starting from the term of the applicable Agreement for its duration, as much relevant information as possible on the requests for disclosure received.

I. Processing of Personal Data; GDPR

All Personal Data processed by Pluralsight in connection with providing the Products is obtained as part of either Customer Data or data generated, derived or collected by Pluralsight or its Sub-processors, including data sent to Pluralsight as a result of a Customer's use of service-based capabilities. Pseudonymized identifiers may be included in data processed by Pluralsight in connection with providing the Products and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

1. Processor and Controller Roles and Responsibilities

Customer and Pluralsight agree that Customer is the controller of Personal Data and Pluralsight is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Pluralsight is a Sub-processor. When Pluralsight acts as the processor or Sub-processor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its Agreements (including the DPA Terms and any applicable updates), are Customer's complete documented instructions to Pluralsight for the processing of Personal Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Agreements. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Pluralsight that Customer's instructions, including appointment of Pluralsight as a processor or Sub-processor, have been authorized by the relevant controller.

2. Data Subject Rights; Assistance with Requests

Pluralsight will make available to Customer, in a manner consistent with the functionality of the Products and Pluralsight's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Pluralsight receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with the Products for which Pluralsight is a data processor or Sub-processor, Pluralsight will promptly notify the Customer and redirect the data subject to make its request directly to Customer. Pluralsight will assist Customer in fulfilling its obligations to respond to data subjects' requests by implementing technical and organizational measures set out in Annex II of Addendum I. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Products. Pluralsight shall comply with requests by Customer to assist with Customer's response to such a data subject request where Customer is otherwise unable to leverage the functionality of the Products as a result of Pluralsight's failure to make such functionality available.

3. Records of Processing Activities

To the extent the GDPR or any other Data Protection Regulation requires Pluralsight to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Pluralsight and keep it accurate and up-to-date. Pluralsight may make any such information available to any supervisory or regulatory authority if required by the Data Protection Requirements.

J. Data Security

1. Security Practices and Policies

Pluralsight will implement and maintain appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise processed. Those measures shall be set forth in a Pluralsight Security Policy. Pluralsight will make available to Customer information reasonably requested by Customer regarding Pluralsight security practices and policies.

In addition, those measures, Pluralsight shall comply with the requirements set forth in ISO 27001. A description of the security controls for these requirements is available to Customers.

2. Data Encryption

Customer Data in transit over public networks between Customer and Pluralsight, or between Pluralsight entities, is encrypted by default.

Pluralsight also encrypts Customer Data stored at rest.

3. Data Access

Pluralsight employs least privilege access mechanisms to control access to Customer Data. Role-based access controls are employed to ensure that access to Customer Data is for an appropriate purpose and approved with management oversight. Pluralsight maintains Access Control mechanisms described in the table entitled “Security Measures” in Appendix A.

4. Customer Responsibilities

Customer is responsible for making an independent determination as to whether the technical and organizational measures for Products meet Customer’s requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Pluralsight provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls.

K. Auditing Compliance

Pluralsight will conduct audits of the security of the computers, computing environment, and physical data centers that it uses in processing Customer Data as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third-party security auditors at Pluralsight’s selection and expense.

Each audit will result in the generation of an audit report (“Pluralsight Audit Report”), which Pluralsight will make available upon written request. The Pluralsight Audit Report will be Pluralsight’s Confidential Information and will clearly disclose any material findings by the auditor. Pluralsight will promptly remediate issues raised in any Pluralsight Audit Report to the satisfaction of the auditor. If Customer requests, Pluralsight will provide Customer with each Pluralsight Audit Report. The Pluralsight Audit Report will be subject to non-disclosure and distribution limitations of Pluralsight and the auditor.

To the extent Customer’s audit requirements under the SCCs or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Pluralsight makes generally available to its customers, Pluralsight will promptly respond to Customer’s additional audit instructions. Before the commencement of an audit, Customer and Pluralsight will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Pluralsight to unreasonably delay performance of the audit. To the extent needed to perform the audit, Pluralsight will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data by Pluralsight, its Affiliates, and its Sub-processors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Pluralsight, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Pluralsight’s other customers or to Pluralsight systems or facilities not involved in providing the applicable Products. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Pluralsight expends for any such audit, in addition to the rates for services performed by Pluralsight. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Pluralsight and Pluralsight shall promptly cure any material non-compliance.

L. Security Incident Notification

If Pluralsight becomes aware of a Security Incident regarding Customer Data while processed by Pluralsight in the context of providing the Products, Pluralsight will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident; and (4) comply with the requirements of clause 8.6 of the SCCs where applicable.

Notification(s) of security Incidents will be delivered to Customer by any means Pluralsight selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information with Pluralsight for each applicable Product. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Pluralsight shall reasonably assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Pluralsight's notification of or response to a Security Incident under this section is not an acknowledgement by Pluralsight of any fault or liability with respect to the Security Incident.

Customer must notify Pluralsight promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Products at security@pluralsight.com.

M. Data Transfers

Customer Data that Pluralsight processes on Customer's behalf may not be transferred to or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section. Taking into account such safeguards, Customer appoints Pluralsight to transfer Customer Data to the United States or any other country in which Pluralsight or its Sub-processors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms.

Transfers from the United Kingdom and Switzerland shall be governed by the 2010 Standard Contractual Clauses pending any revision or replacement of the 2010 Standard Contractual Clauses by the ICO. In the event of such revision or replacement, Pluralsight shall amend this DPA to reflect the updates as required to continue the transfers.

All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

N. Data Retention and Deletion

At all times during the term of Customer's Agreements, Customer will have the ability to access, extract and delete Customer Data stored in the Platform, subject to availability as set forth in the Agreements.

Pluralsight will return or destroy Customer Data upon the expiration or termination of any Agreement or at Customer's instructions at any time, where such Customer Data is no longer required to be processed, in accordance with Data Protection Requirements.

The Platform may not support retention or extraction of data by third-party software provided by Customer and Pluralsight has no liability for the deletion of Customer Data or Personal Data in this manner.

O. Notice and Controls on use of Sub-processors

Pluralsight may hire Sub-processors, including Pluralsight Affiliates, to provide certain limited or ancillary services on its behalf. Customer authorizes Pluralsight's engagement of Sub-processors.

Where the Controller to Processor SCCs apply, the Parties agree to use "Option 2" in clause 9 of the Controller to Processor SCCs (i.e., Customer's general written authorization for the engagement of Pluralsight's Sub-processors). Pluralsight is responsible for its Sub-processors' compliance with Pluralsight's obligations in this DPA. Pluralsight makes available information about Sub-processors on Pluralsight's website https://www.pluralsight.com/terms/sub-processors. When engaging any Sub-processor, Pluralsight will ensure via a written contract that the Sub-processor may access and use Customer Data only to deliver the services Pluralsight has retained them to provide and is prohibited from using Customer Data for any other purpose. Pluralsight will ensure that Sub-processors are bound by written agreements that provides for, in substance, the same data protection obligations as those binding Pluralsight under the SCCs where applicable. Pluralsight agrees to oversee the Sub-processors to ensure that these contractual obligations are met.

From time to time, Pluralsight may engage new Sub-processors. Pluralsight will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least thirty (30) days in advance of engaging that new Sub-processor. If Pluralsight engages a new Sub-processor for a new Product that processes Customer Data Pluralsight will give Customer notice prior to availability of that Product.

If Customer does not reasonably approve of a new Sub-processor, then Customer may terminate any subscription for the affected Product without penalty or termination fee by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Pluralsight to re-evaluate any such new Sub-processor based on the applicable concerns. After termination, Pluralsight will remove payment obligations for any subscriptions or other applicable unpaid services for the terminated Products or Services from subsequent invoices to Customer or its reseller.

P. Limitation of liability

Except as regards towards data subjects and as otherwise provided by the Data Protection Requirements, either Party’s liability to the other shall be as set forth in the applicable Agreements.

Q. M. California Consumer Privacy Act (CCPA)

If Pluralsight is processing Personal Data within the scope of the CCPA, Pluralsight makes the following additional commitments to Customer. Pluralsight will process Customer Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any “sale” exemption. In no event will Pluralsight sell any such data. These CCPA terms do not limit or reduce any data protection commitments Pluralsight makes to Customer in the DPA Terms or other Agreements between Pluralsight and Customer.

R. How to Contact Pluralsight

If Customer has any questions, please contact Pluralsight at the following mailing address:

Pluralsight, LLC

42 Future Way

Draper, UT 84020

Attn. Legal

Email: contract-notices@pluralsight.com

Whereas the Parties’ authorized signatories have duly executed this DPA:

<<Customer Name>>	Pluralsight, LLC
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

Appendix A – Security Measures

Pluralsight has implemented and will maintain for Customer Data the following security measures, which in conjunction with the security commitments in this DPA, are Pluralsight's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership**. Pluralsight has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. Pluralsight personnel with access to Customer Data are subject to confidentiality obligations. Least privilege access is used. **Risk Management Program**. Pluralsight performed a risk assessment before processing the Customer Data.
Asset Management	**Asset Inventory**. Pluralsight maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Pluralsight personnel authorized in writing to have such access. **Asset Handling** - Pluralsight classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Pluralsight imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain such data. - Pluralsight personnel must obtain Pluralsight authorization prior to storing Customer Data on portable devices, remotely accessing such data, or processing such data outside Pluralsight's facilities.
Security Training	**Security Training**. Pluralsight informs its personnel about relevant security procedures and their respective roles. Pluralsight also informs its personnel of possible consequences of breaching the security rules and procedures. Pluralsight will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. Pluralsight limits access to facilities where information systems that process Customer Data are located to identified authorized individuals. **Physical Access to Components**. Pluralsight maintains records of the incoming and outgoing media containing Customer Data including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain. **Protection from Disruptions**. Pluralsight uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Pluralsight uses industry standard processes to delete and/or return Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Pluralsight maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Pluralsight maintains multiple copies of Customer Data from which such data can be recovered.

Domain	Practices
	- Pluralsight stores copies of Customer Data and data recovery procedures in a different geographic location from where the primary computer equipment processing the Customer Data are located. - Pluralsight has specific procedures in place governing access to copies of Customer Data. - Pluralsight reviews data recovery procedures at least every twelve months. - Pluralsight logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Pluralsight has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data including malicious software originating from public networks. **Data Beyond Boundaries** - Pluralsight encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - Pluralsight restricts access to Customer Data in media leaving its facilities. **Event Logging**. Pluralsight logs, or enables Customer to log, access and use of information systems containing Customer Data registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Pluralsight maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** - Pluralsight maintains and updates a record of personnel authorized to access Pluralsight systems that contain Customer Data. - Pluralsight deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Pluralsight identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Pluralsight ensures that where more than one individual has access to systems containing Customer Data the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - Pluralsight restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Pluralsight instructs Pluralsight personnel to disable administrative sessions when leaving premises Pluralsight controls or when computers are otherwise left unattended. - Pluralsight stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Pluralsight uses industry standard practices to identify and authenticate users who attempt to access information systems.

Domain	Practices
	- Where authentication mechanisms are based on passwords, Pluralsight requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Pluralsight requires the password to be at least eight characters long. - Pluralsight ensures that de-activated or expired identifiers are not granted to other individuals. - Pluralsight monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Pluralsight maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Pluralsight uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Pluralsight has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - Pluralsight maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each Security Incident, notification by Pluralsight (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Pluralsight tracks, or enables Customer to track, disclosures of Customer Data including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Pluralsight security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Pluralsight maintains emergency and contingency plans for the facilities in which Pluralsight information systems that process Customer Data are located. - Pluralsight's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

Appendix B – Data Subjects and Categories of Personal Data

Data subjects: Data subjects include the Customer's representatives and end-users including employees, contractors, and collaborators of the Customer. Pluralsight acknowledges that, depending on Customer's use of the Products, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter; or
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former).

Categories of data: The personal data that is uploaded to the Platform and included in email, documents and other data in an electronic form in the context of the Products. Pluralsight acknowledges that, depending on Customer's use of the Products , Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, screen name/handle, email address);
- Authentication data (for example user name/handle, password, security question, audit trail);
- Contact information (for example physical addresses, email, phone numbers, social media identifiers);
- Unique identification numbers such as IP addresses, employee number, student number, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial information (for example bank account name and number, credit card name and number, and invoice number;
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Internet activity (for example browsing and search history while on the Platform);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- Employment data derived from a data subject's association with a commercial customer (for example job and position data);
- Education data (for example degree and certification history)
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority; or
- Any other personal data identified in Article 4 of the GDPR.

Addendum I – Standard Contractual Clauses (Controller to Processor) Module 2

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) [1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/91.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b)

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Intentionally Left Blank

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union [2](in the same country as the data

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. [3] The

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7 .

Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it.

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller].

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of **The Republic of Ireland** (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of The Republic of Ireland (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Activities relevant to the data transferred under these Clauses: …

   Signature and date: …

   Role (controller/processor): …Controller

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: …Pluralsight, LLC

   Address: …42 Future Way, Draper, UT 84020

   Contact person's name, position and contact details: …

   Activities relevant to the data transferred under these Clauses: …For the provision of SaaS Products.

   Signature and date: …

   Role (controller/processor): …Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

… ***Data subjects: Data subjects include the Customer's representatives and end-users including employees, contractors, and collaborators. Pluralsight acknowledges that, depending on Customer's use of the Products, Customer may elect to include personal data from any of the following types of data subjects in the personal data:***

- ***Employees, contractors and temporary workers (current, former, prospective) of data exporter; and***
- ***Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former).***

Categories of personal data transferred

… ***Categories of data: The personal data that is uploaded to the Platform and included in email, documents and other data in an electronic form in the context of the Products. Pluralsight acknowledges that, depending on Customer's use of the Products , Customer may elect to include personal data from any of the following categories in the personal data:***

- ***Basic personal data (for example street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, screen name/handle, email address);***
- ***Authentication data (for example user name/handle, password, security question, audit trail);***
- ***Contact information (for example physical addresses, email, phone numbers, social media identifiers);***
- ***Unique identification numbers such as IP addresses, employee number, student number, unique identifier in tracking cookies or similar technology);***
- ***Pseudonymous identifiers;***
- ***Financial information (for example bank account name and number, credit card name and number, and invoice number;***
- ***Commercial Information (for example history of purchases, special offers, subscription information, payment history);***
- ***Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);***
- ***Photos, video and audio;***
- ***Internet activity (for example browsing and search history while on the Platform);***
- ***Device identification (for example IMEI-number, SIM card number, MAC address);***
- ***Profiling (for example based on pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);***
- ***Employment data derived from a data subject's association with a commercial customer (for example job and position data);***
- ***Education data (for example degree and certification history);***
- ***Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority; or***
- ***Any other personal data identified in Article 4 of the GDPR.***

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

… Not applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

… ***On a continuous basis as necessary for the data importer to meet its obligations in conjunction with the provision of the SaaS services for the term of the agreements with the data exporter.***

Nature of the processing

…***The nature and purpose of the processing shall include the collection, organisation, storage, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the personal data as necessary to provide the products or services pursuant to the agreements with data exporter.***

Purpose(s) of the data transfer and further processing

…***Personal data will be processed in conjunction with data exporter's Agreements to allow the data importer to fulfill its obligations thereunder.***

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

…***Personal data will be retained for so long as the user(s) continue to maintain and use their accounts. Dormant accounts are checked intermittently and where contact cannot be made with the user to confirm their intent to maintain the account, the account is canceled. Upon such cancelation all date associated with that account will no longer be identifiable to a natural person***.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

…Only sub-processors are retained in support of the SaaS products/services provided to data exporters and are contractually bound as to subject matter, nature and duration of the processing similarly in kind as the data importer taking into account the sub-processors specific role.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

□ ***OPTION 1 - The data exporter is established in an EU Member State:*** *the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer will act as competent supervisory authority. In the context of this DPA, the competent supervisory authority is*

□ ***OPTION 2 - The data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR):*** *the supervisory authority of the Member State in which the is established will act as competent supervisory authority. In the context of this DPA, the competent supervisory authority is*

□ ***OPTION 3 - The data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU:*** *the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the Standard Contractual Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, will act as competent supervisory authority. In the context of this DPA, the competent supervisory authority is* ***.***

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

- *All sensitive data transferred to destinations outside of Pluralsight environments must be encrypted with at least 256-bit keys.*
- *The IT and Operations teams ensure that sensitive data in transit within the Pluralsight environment is also encrypted with TLS and strong ciphers. Additionally, remote access to Pluralsight systems and applications must be encrypted.*
- *Team members ensure that emails (including attachments) are encrypted whenever sensitive data is contained or attached. The IT team ensures there are email encryption capabilities available to team members.*
- *The IT team is responsible for implementing Wi-Fi Protected Access (i.e. WPA2 - Enterprise) encryption which is mandatory for all Pluralsight business wireless networks.*
- *All corporate endpoint devices/laptops are encrypted using NIST standard encryption algorithms at the disk or volume level leveraging technologies incorporated in the operating system.*
- *Application credentials and service accounts are encrypted and stored in centrally managed solutions.*
- *Amazon RDS Databases are encrypted at the database level using NIST AES standard of 128 bit encryption or higher.*
- *Pluralsight does not ever store credit card information in our data stores; rather, Pluralsight utilizes third-party services, which are PCI-certified and implement industry data security standards appropriate for that data classification, to manage all confidential subscription and billing information.*
- *The Pluralsight platform leverages the bcrypt hashing algorithm for all individual customer passwords and only ever stores the hashed output of that computation.*

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- *Pluralsight's production environment is housed in the AWS US-West-2 Region. High Availability (HA) is turned on for critical services. The AWS infrastructure provides redundancy for Pluralsight platform availability.*
- *The App.Pluralsight.com Disaster Recovery Plan is activated when an event is determined to significantly affect or threaten to significantly affect The Pluralsight Skills product. The degree and*

extent of activation depends upon the impact and timing of the event, but for the purposes of this plan, a disaster will be declared when the primary Amazon region hosting app.pluralsight.com is unavailable and the Estimated Time to Resolution(ETR) for that region is less than our projected ETR for recovering to a different Amazon region. Specific actions to be undertaken upon disaster declaration and plan activation are detailed hereafter. Both our RTO and RPO are 24 hrs. Those objectives are what we will compare with AWS's ETR.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- *Disaster Recovery Testing is conducted quarterly*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*
- *Measures for user identification and authorization.*
- *Centralized directory (Okta) integration with ticketing system and HRIS systems auto provisions access for the team member with appropriate access for their role.*
- *Any additional requests for access to IT systems not managed by the IT team are requested by the team member and/or manager to the application owner.*
- *Team members shall be positively identified, authorized, and authenticated before they are granted access to company information resources.*
- *Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).*
- *Access to information resources shall be controlled through a defined and managed process which addresses authorizing, modifying, and revoking access, and which includes a periodic review of information system privileges.*
- *A user enrollment process shall be created, documented, implemented, and maintained on a regular basis.*
- *Each user shall be uniquely identified.*
- *Each user requiring access to Pluralsight's information assets above the standard access for their job function shall submit a request*
- *User access requests shall be retained as required by business and regulatory needs.*
- *Information resources and network services shall not be accessible to users unless the user has been explicitly authorized and granted permission to access the resource or service.*
- *The allocation and use of privileges shall be restricted and managed.*
- *User privileges shall be tracked at the application level and each user's profile (identity, access, privileges, and authorization) recorded and managed to prevent misuse of resources.*
- *Authentication tokens (i.e., passwords) and keys for privileged users must be rotated upon termination.*
- *User access and privileges shall be reviewed through a defined process.*
- *Reviews of non-administrative and administrative user access rights shall be performed at least annually.*

Measures for user identification and authorisation

- *All sensitive data transferred to destinations outside of Pluralsight environments must be encrypted with at least 256-bit keys.*
- *The IT and Operations teams ensure that sensitive data in transit within the Pluralsight environment is also encrypted with TLS and strong ciphers. Additionally, remote access to Pluralsight systems and applications must be encrypted.*
- *Team members ensure that emails (including attachments) are encrypted whenever sensitive data is contained or attached. The IT team ensures there are email encryption capabilities available to team members.*
- *The IT team is responsible for implementing Wi-Fi Protected Access (i.e. WPA2 - Enterprise) encryption which is mandatory for all Pluralsight business wireless networks.*

Measures for the protection of data during transmission

- *All sensitive data transferred to destinations outside of Pluralsight environments must be encrypted with at least 256-bit keys.*
- *The IT and Operations teams ensure that sensitive data in transit within the Pluralsight environment is also encrypted with TLS and strong ciphers. Additionally, remote access to Pluralsight systems and applications must be encrypted.*
- *Team members ensure that emails (including attachments) are encrypted whenever sensitive data is contained or attached. The IT team ensures there are email encryption capabilities available to team members.*
- *The IT team is responsible for implementing Wi-Fi Protected Access (i.e. WPA2 - Enterprise) encryption which is mandatory for all Pluralsight business wireless networks.*

Measures for the protection of data during storage

- *All corporate endpoint devices/laptops are encrypted using NIST standard encryption algorithms at the disk or volume level leveraging technologies incorporated in the operating system (e.g. Bitlocker and Filevault using AES-128 bit encryption or higher);*
- *Application credentials and service accounts are encrypted and stored in centrally managed solutions. (e.g. Hashicorp Vault, LastPass, etc.)*
- *Amazon RDS Databases are encrypted at the database level using NIST AES standard of 128 bit encryption or higher.*
- *Pluralsight plans to enhance encryption at rest strategies in AWS by the end of 2021 by further encrypting all Amazon EBS volumes and all customer data stored in Amazon S3 buckets.*
- *Pluralsight does not ever store credit card information in our data stores; rather, Pluralsight utilizes third-party services, which are PCI-certified and implement industry data security standards appropriate for that data classification, to manage all confidential subscription and billing information.*
- *The Pluralsight platform leverages the bcrypt hashing algorithm for all individual customer passwords and only ever stores the hashed output of that computation.*

Measures for ensuring physical security of locations at which personal data are processed

- *Customer data is housed in AWS where their physical security controls are leveraged (www.aws.amazon.com/security & www.aws.amazon.com/compliance)*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required that Pluralsight reviews Amazon Web Services (AWS) SOC II which provides appropriate assurance of AWS' physical security practices.*

Measures for ensuring events logging

- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required that Pluralsight has appropriate event logging practices in place.*
- *All critical devices, systems, datastores, and applications have event logging enabled. Logging events must contain what occurred, who or what caused the event, when the event occurred (i.e. timestamp), and the associated system applications or data affected by the events.*
- *Where possible, the following system, datastore, and application types of events should be logged:*
  - *All authentication events (success and fail)*
  - *Account or role creation, modification, or deletion*
  - *Changes to system or application configuration*
  - *All alerts raised by the access control system*
  - *Administrator or operator activities*
- *Centrally collected event logs from systems, datastores, and applications. Access to centrally collected event logs is controlled by these teams and limited to "need to know" scenarios. Centrally collected event logs are retained for a period of no less than 12 months.*

Measures for ensuring system configuration, including default configuration

- *Configuration Standards such as an Implementation Checklist and Operating Procedures are in place for system components. This also includes a description of any manual or automated tasks for installation and maintenance, backup, error handling, system restart and recovery procedures, logging and monitoring methods.*
- *Default vendor passwords must be changed after the installation of systems or software and before system or software is used in production.*

Measures for internal IT and IT security governance and management

- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*
- *Personal data is protected with least privilege access and handled with appropriate operational procedures.*
- *Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).*
- *Laptops are necessary to conduct business tasks and are provided and centrally managed by IT. Other personally-owned mobile devices, such as smartphones, that are not owned by Pluralsight must adhere to our Mobile Device Policy & Standard (MDM). To protect mobile devices and business related data, the IT team is responsible for the implementation of technical security measures. Additionally, every team member is responsible to ensure that mobile devices accessing Pluralsight data comply with the following requirements:*
    - *Access to devices must be authenticated (including a PIN on mobile devices).*
    - *The device is encrypted.*
    - *Anti-malware software and definitions are updated automatically.*

  The IT team and Information Security team have the right to control information on mobile devices and forensically examine the device believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.

- *Team members are permitted to carry personal smartphones or tablets with them to corporate offices. The accessing, processing, copying, or taking pictures of business related data and documents is strictly prohibited.*
- *Team members shall be positively identified, authorized, and authenticated before they are granted access to company information resources.*
- *Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).*
- *Access to information resources shall be controlled through a defined and managed process which addresses authorizing, modifying, and revoking access, and which includes a periodic review of information system privileges.*
- *A user enrollment process shall be created, documented, implemented, and maintained on a regular basis.*
- *Each user shall be uniquely identified.*
- *Each user requiring access to Pluralsight's information assets above the standard access for their job function shall submit a request*
- *User access requests shall be retained as required by business and regulatory needs.*
- *Information resources and network services shall not be accessible to users unless the user has been explicitly authorized and granted permission to access the resource or service.*
- *The allocation and use of privileges shall be restricted and managed.*
- *User privileges shall be tracked at the application level and each user's profile (identity, access, privileges, and authorization) recorded and managed to prevent misuse of resources.*
- *Authentication tokens (i.e., passwords) and keys for privileged users must be rotated upon termination.*

- *User access and privileges shall be reviewed through a defined process.*
- *Reviews of non-administrative and administrative user access rights shall be performed at least annually.*
- *Change requests serve as a "notice" to others within Pluralsight regarding proposed alterations to the IT environment. Change requests may come from a variety of individuals within the company and are necessary for effective tracking and information management. Requests are initiated by logging a request for change on the IT change request system.*
- *Change authorization is performed by the Pluralsight IT and Security teams.*
- *A Change review will occur following the implementation of the change into the production environment. This function may be performed by a variety of personnel, but traditionally the function is best performed by those performing the actual distribution functions, or others who may be most familiar with the performance of the production environment.*
- *All Pluralsight team members are trained and educated on internet browsing and email best practices to help protect against malware, phishing, and ransomware. Team members must be attentive to indications of a compromise and must contact the IT team immediately if a compromise is suspected.*
- *The IT and Operations teams are responsible for implementing anti-malware capabilities. They establish a patch management process for systems they support and a procedure to remain aware of new vulnerabilities. These teams are also responsible for ensuring the following take place:*
- *All Windows and MacOS systems, as well as Linux systems have approved anti-malware software installed and operating.*
- *Anti-malware is centrally administered by the IT and Operations teams.*
- *Anti-malware is centrally monitored by the Information Security team.*
- *Anti-malware definition files and/or updates are downloaded and installed automatically.*
- *Anti-malware software is configured to scan all files before being accessed and/or written to disk.*
- *Anti-malware is configured to clean, quarantine, or delete any infected file.*
- *Anti-malware software is enabled at system startup and configured to only be disabled by system administrators.*
- *Anti-malware software is capable of generating audit logs and is enabled at all times.*
- *Operational software is only installed, deployed, maintained, and tested by the IT or Operations teams and a configuration control system is deployed to manage and document authorized software, applications, or libraries.*
- *The IT and Operations teams are responsible for the management of the Pluralsight business and product networks, respectively. This includes the administration and monitoring of those networks for the purposes of security and availability. All remote network level access and administration is restricted by firewall authentication. Complete network level access is only granted to the IT and Operations teams. All requests for access and network changes follow the change management process .*
- *Networks, including the components which comprise them, shall be managed and controlled to limit threats and vulnerabilities.*
- *Network controls shall ensure the protection and security of the information processing services and applications dependent on the network infrastructure.*
- *Network services agreements, whether in-house or outsourced, shall include the following provisions:*
- *Security features and requirements.*
- *Service level agreements.*
- *Specified responsibility for managing security requirements on both sides of the service delivery process.*
- *Groups of information services, users, and information systems shall be segregated on the network.*
- *Grouping shall be determined by business function, information classification, the Access Control Policy, and user access requirements.*
- *The IT and Operations teams ensure that Pluralsight networks are segregated (using authentication, physical and logical access restrictions) from each other using network ACLS, firewalls, VPNs, security groups, etc. They establish specific segments for each office location, guest wireless, team member wireless, development/test, stage, and production environments. Team member wireless access is, at a minimum, WPA2 Enterprise and requires unique credentials for each user.*
- *The Information Security team assesses each environment at least annually for risks.*

Measures for certification/assurance of processes and products

- *Disaster Recovery Testing is conducted quarterly*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*

Measures for ensuring data minimisation

- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*
- *Personal data is protected with least privilege access and handled with appropriate operational procedures.*
- *Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).*

Measures for ensuring data quality

- *Disaster Recovery Testing is conducted quarterly.*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted. Data validation inputs are also reviewed as part of the ISO 27001 certification.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*

Measures for ensuring limited data retention

- *Data protection laws require that personal data not be retained for longer than is necessary for the purpose for which it is processed.*
- *Records must not be retained beyond the period indicated in the Records Retention Schedule unless the record is identified as information subject to a litigation hold or other valid business reason. If you are uncertain as to when a record can be destroyed, you can reach out to the Legal Department for guidance.*
- *Erasure Requests: Pluralsight has added a "delete my account" feature, thus facilitating learner requests to be forgotten. When a learner deletes their account, all data associated with that account in the product will no longer be identifiable to a natural person.*

Measures for ensuring accountability

- *Disaster Recovery Testing is conducted quarterly.*
- *Pluralsight is ISO 27001 certified which includes an annual review, by an ANAB accredited third party, of our security practices. Additionally; as part of this certification, it is required Pluralsight also conducts an annual internal audit and an external penetration test conducted.*
- *Pluralsight possesses a SOC II Type II report, which is the assessment of Pluralsight's security controls conducted by a third party.*

Measures for allowing data portability and ensuring erasure

- *Erasure Requests: Pluralsight has added a "delete my account" feature, thus facilitating learner requests to be forgotten. When a learner deletes their account, all data associated with that account in the product will no longer be identifiable to a natural person.*

Measures for assisting the data exporter with data subject access requests

Data importer will assist data exporter in meeting its obligations under the GDPR by either (i) providing Customer the ability within the Platform to access, correct or delete personal data or restrict its processing; or (ii) if such functionality is not available

within the Platform, make personal data available to data exporter, or as applicable, make such corrections, deletions, or restrictions on data exporter's behalf.

For transfers to (sub-) processors, also *describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

Pluralsight contractually binds its sub-processors to technical and organizational measures substantially equivalent to those to which Pluralsight has committed herein.

Pluralsight's Exceptions and Conditions to
State of West Virginia's Request for Quote #0210
for Online Technical Training (the "RFQ")

As part of its response to the State of West Virginia (the "State"), Pluralsight, LLC ("PS") submits the following conditions and/or exceptions with respect to the above-mentioned RFQ.

GENERAL CONDITIONS: Any software as a service ("SaaS") provided by PS to the State shall be governed by the terms and conditions of PS's current Data Privacy Agreement ("DPA") which is attached for your review. If requested by the State, PS will negotiate in good faith regarding the possible inclusion of additional or modified provisions in the PS's DPA whether such terms arise from the State's RFQ document or otherwise.

SPECIFIC CONDITIONS AND EXCEPTIONS: Without in any way limiting the generality of the foregoing, PS's response to the RFQ is subject to the following specific conditions and exceptions. Again, PS is willing to discuss these conditions and exceptions, as well as any other proposed terms, with the State.

RFQ Document- General Terms and Conditions

8. Insurance – PS maintains a comprehensive insurance program and can generally meet the listed requirements, however, there may be certain technical aspects of the insurance clause that would need to be negotiated as part of the final contract.

13. Pricing –
PS requests the deletion of this section.

And replacing it with the following:
PS can agree to fixed pricing for a 12 month period and not for the entire term of the agreement. PS reserves the right to increase or decrease any fees at any time; however, the increase or decrease will not become effective until the end of a 12 month period.

14. Payment in Arrears –
PS requests the deletion of this section and replacing it with the language below:
The only payment arrangement acceptable to PS is payment for goods/services will be made for 12 months, payable in advance.

19. Cancellation –
PS requests a cure period in which to correct any non-conformance.

26. Subsequent Forms –
PS requests the deletion of this section:
The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or

Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

27. Assignment-
PS shall retain the right to assign its rights without approval from the State in the event of a merger or acquisition.

28. Warranty-
PS requests the deletion of this section:
"The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship."

And replaces it with the following:

PS is not liable for any loss or injury of the State or its users arising out of or caused, in whole or in part, by (i) the State's or its users' use or application of the knowledge gained from PS's platform or the services, (ii) any computer virus not originating from PS's platform, or (iii) any unauthorized use of the PS's Platform by the State or by any of its users as described in this Agreement. EXCEPT AS OTHERWISE INDICATED, THE PLATFORM IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY, ACCURACY, ADEQUACY, COMPLETENESS, CURRENCY, CORRECTNESS, OR VALIDITY OF ANY INFORMATION, SOFTWARE, MATERIAL OR CONTENT PROVIDED BY OR THROUGH THE PLATFORM RESTS WITH THE USER.

Functionality. PS does not warrant that the content or functions of PS's platform will meet the State's requirements or that the operation of PS's platform will be uninterrupted or error free. PS's platform (including without limitation its blogs and any interactive features) may include content provided by third parties, including materials provided by other users, bloggers, or third-party licensors, syndicators, aggregators, and reporting services. All statements and opinions expressed in these materials, and all articles and responses to questions and other content, other than the content provided by PS, are solely the opinions and the responsibility of the person or entity providing those materials. These materials do not necessarily reflect the opinion of PS. PS is not responsible or liable to the State, its users, or any third party, for the content or accuracy of any materials provided by any third parties.

36. Indemnification –
PS requests the deletion of this section:
The Vendor agrees to indemnify, defend, and hold harmless the
State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services,

materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

And replacing it with the following language:

By PS. PS will indemnify, defend, and hold harmless the State, its directors, officers, employees, agents, and Affiliates (each, a **"State Indemnitee"**) from and against any and all third-party liabilities, claims, damages and losses, including all reasonable attorneys' fees, costs, and expenses (collectively, **"Claims"**), arising out of or connected with any Claims that the PS platform infringes, misappropriates, or violates any third party's intellectual property rights (**"Infringement Claim"**), except for any such infringement, misappropriation, or violation that arises out of any act or omission by the State, users, or any agent, or Affiliate of the State in violation of the terms and conditions of this agreement or any sales order, including without limitation, those prohibitions set forth in Section 2.5. In the event of any such Infringement Claim, PS may, at its option: (i) obtain the right to permit the State to continue using the PS platform, (ii) modify or replace the relevant portion(s) of the PS platform with a non-infringing alternative having substantially equivalent performance within a reasonable period of time, or (iii) terminate this Agreement as to the infringing portion of the PS platform and refund to the State any prepaid, unused fees for such infringing portion of the PS platform hereunder. Notwithstanding the foregoing, PS will have no liability for any Infringement Claim of any kind to the extent that it results from: (1) modifications to the PS platform made by a party other than PS, (2) Customer Data or the combination of the PS platform with non-PS products, or (3) the State's use of the Platform other than in accordance with the documentation and this agreement. The indemnification obligations set forth herein are PS's sole and exclusive obligations, and the State's sole and exclusive remedies, with respect to infringement or misappropriation of third-party intellectual property rights of any kind. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or suit brought against the U.S. pursuant to its jurisdictional statute 28 U.S.C. § 516.

By the State. Unless otherwise prohibited by law, the State will indemnify, defend, and hold harmless PS and its directors, officers, employees, agents, and affiliates (each, a **"PS Indemnitee"**) from and against any and all third-party claims arising out of or connected with any act or omission by the State, State's user or any employee, agent or contractor of the State in violation of the terms and conditions for any and all third party claims, actions and demands alleging State data infringes or misappropriates the intellectual property rights of a third party or violates applicable law.

Software as a Service Addendum-

PS requests the State to review the attached DPA in lieu of Addendum included in the RFQ. PS's DPA is specifically tailored to PS's platform and products/services and more accurately applicable.