EEA Data Processing Addendum

This Data Processing Addendum ("**DPA**") amends and forms part of the Terms of Service (the "**Agreement**") between POP, Inc. ("**POP**") and the customer identified in the table below ("**Customer**"). This DPA prevails over any conflicting term of the Agreement, but does not otherwise modify the Agreement.

POP:	Customer:
Name: Hayes Drumwright	Name:
Title: CEO	Title:
Address: 300 Spectrum Center Drive Suite 800 Irvine, CA 92618	Address:
Signature:	Signature:
Date: 10-31-18	Date:

Instructions. This DPA has been pre-signed by POP. To enter into this DPA, Customer must:

1) complete the signature table above by signing and providing the Customer legal entity name, place of business and signatory information;

2) sign the signature table above and initial **Appendix 1**, and **Appendix 2**; and

3) submit the completed and signed DPA to POP as part of the contract package.

This DPA will be effective only if executed in accordance with these instructions, and as of the day that POP receives a complete and executed DPA from Customer, or if later, the date of the Agreement.

1. **Definitions**

    1.1. In this DPA:

        a) "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" have the meaning given to them in the GDPR;

        b) "**Customer Personal Data**" means any data provided by Customer that constitutes Personal Data, the Processing of which is subject to Data Protection Law, for which Customer is a Controller or Processor, and which is Processed by POP to provide the Services;

        c) "**Data Protection Law**" means Data Protection Directive 95/46/EC, General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), and their national implementations in the European Economic Area ("**EEA**") and Switzerland, each as applicable, and as may be amended or replaced from time to time;

d) "**Data Subject Rights**" means Data Subjects' rights to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making in accordance with Data Protection Law.

e) "**International Data Transfer**" means any transfer of Customer Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland or the United Kingdom;

f) "**Privacy Shield**" means the self-regulatory framework administered by the U.S. Department of Commerce in accordance with EU Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ L 207, 1.8.2016, p. 1-112) and approved by the Swiss Federal Council on January 11, 2017.

g) "**Services**" means the services provided by POP to Customer under the Agreement;

h) "**Subprocessor**" means a Processor engaged by POP to Process Customer Personal Data; and

i) "**Standard Contractual Clauses**" means the clauses annexed to EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5-18).

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. Scope and applicability

2.1. This DPA applies to Processing of Customer Personal Data by POP to provide the Services.

2.2. The subject matter, nature and purpose of the Processing, the types of Customer Personal Data and categories of Data Subjects are set out in **Appendix 1**.

2.3. Customer is a Controller and appoints POP as a Processor on behalf of Customer. Customer is responsible for compliance with the requirements of Data Protection Law applicable to Customer as a Controller.

2.4. If Customer is a Processor on behalf of other Controller(s), then Customer: is the single point of contact for POP; must obtain all necessary authorizations from such other Controller(s); undertakes to issue all instructions and exercise all rights on behalf of such other Controller(s); and is responsible for compliance with the requirements of Data Protection Law applicable to Customer as a Processor.

2.5. Customer acknowledges that POP may Process Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, and product development.

3. Instructions

3.1. POP will Process Customer Personal Data to provide the Services and in accordance with Customer's instructions documented in this DPA, the Agreement, and any applicable statement of work.

3.2. Customer may reasonably issue additional instructions as necessary to comply with Data Protection Law. POP may charge a reasonable fee to comply with any additional instructions.

3.3. Customer acknowledges that one of the key features of the Services is to promote participation by enabling Data Subjects to answer questions without revealing their identity to Customer. Customer must not instruct POP to reveal the identity of any Data Subjects who have elected not to reveal their identity through the Services, and POP will not comply with such instruction unless Customer confirms in writing that the instruction is required by applicable law. Customer will defend and indemnify POP from and against every claim, liability, damage, loss, and expense, including

reasonable attorneys' fees and costs, arising out of or in any way connected with Customer's instruction to POP to identify a Data Subject.

3.4. Unless prohibited by applicable law, POP will inform Customer if POP is subject to a legal obligation that requires POP to Process Customer Personal Data in contravention of Customer's documented instructions.

4. **Personnel**

4.1. POP will ensure that all personnel authorized to Process Customer Personal Data are subject to an obligation of confidentiality.

5. **Security and Personal Data Breaches**

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, POP will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures listed in Appendix 2, with updates published at https://www.popinnow.com/policies/security.

5.2. Customer acknowledges that the security measures in Appendix 2 and referenced at https://www.popinnow.com/policies/security are appropriate in relation to the risks associated with Customer's intended Processing, and will notify POP prior to any intended Processing for which POP's security measures may not be appropriate.

5.3. POP will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data. If POP's notification is delayed, it will be accompanied by reasons for the delay.

6. **Subprocessing**

6.1. Customer hereby authorizes POP to engage Subprocessors. A list of POP's current Subprocessors is available at https://www.popinnow.com/policies/gdpr.

6.2. POP will enter into a written agreement with Subprocessors which imposes the same obligations as required by Data Protection Law.

6.3. POP will notify Customer, via subscribed contacts, prior to any intended change to Subprocessors. Customer may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following POP's notification of the intended change. Customer and POP will work together in good faith to address Customer's objection. If POP chooses to retain the Subprocessor, POP will inform Customer at least thirty (30) days before authorizing the Subprocessor to Process Customer Personal Data, and Customer may immediately discontinue using the relevant parts of the Services, and may terminate the relevant parts of the Services within thirty (30) days.

7. **Assistance**

7.1. Taking into account the nature of the Processing, and the information available to POP, POP will assist Customer, including, as appropriate, by implementing technical and organizational measures, with the fulfilment of Customer's own obligations under Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities; and notify a Personal Data Breach.

7.2. POP will maintain records of Processing of Customer Personal Data in accordance with Data Protection Law.

7.3. POP may charge a reasonable fee for assistance under this **Section 7**. If POP is at fault, POP and Customer shall each bear their own costs related to assistance.

8. **Audit**

   8.1. POP must make available to Customer all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested by Customer and performed by an independent auditor as agreed upon by Customer and POP.

   8.2. POP will inform Customer if POP believes that Customer's instruction under **Section 8.1** infringes Data Protection Law. POP may suspend the audit or inspection, or withhold requested information until POP has modified or confirmed the lawfulness of the instructions in writing.

   8.3. POP and Customer each bear their own costs related to an audit.

9. **International Data Transfers**

   9.1. Customer hereby authorizes POP to perform International Data Transfers, at POP's option: to any country deemed adequate by the EU Commission; on the basis of an organization's binding corporate rules or Privacy Shield certification; or pursuant to the Standard Contractual Clauses referred to in **Section 9.2**.

   9.2. If Customer is located in the EEA or Switzerland, then by signing this DPA, Customer and POP conclude the Standard Contractual Clauses, which are hereby incorporated into this DPA and completed as follows: "data exporter" is Customer; "data importer" is POP; the governing law in Clause 9 and Clause 11.3 of the Standard Contractual Clauses is the law of the EU member state in which Customer is established; Appendix 1 and 2 to the Standard Contractual Clauses, are **Appendix 1** and **2** to this DPA, respectively; and the optional indemnification clause is struck.

   9.3. If POP's compliance with Data Protection Law applicable to International Data Transfers is affected by circumstances outside of POP's control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Customer and POP will work together in good faith to reasonably resolve such non-compliance.

10. **Notifications**

    10.1. Customer will send all notifications, requests and instructions under this DPA to POP's Legal Department via email to privacy@popinnow.com.

11. **Liability**

    11.1. Where POP has paid damages or fines, POP is entitled to claim back from Customer that part of the compensation, damages or fines, corresponding to Customer's part of responsibility for the damages or fines.

12. **Termination and return or deletion**

    12.1. This DPA is terminated upon the termination of the Agreement.

    12.2. Customer may request return of Customer Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, POP will delete all remaining copies of Customer Personal Data within one hundred eighty (180) days after returning Customer Personal Data to Customer.

13. **Modification of this DPA**

    13.1. This DPA may only be modified by a written amendment signed by both POP and Customer.

14. **Invalidity and severability**

    14.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

DESCRIPTION OF THE PROCESSING

1. **Data Subjects**

The Customer Personal Data Processed concern the following categories of Data Subjects (please specify):

#	Category
1	Employees of Customer, including current and former employees, as well as temporary staff, interns, and contractors and consultants who perform services for Customer.
2	Prospective, current, and former customers of Customer who are natural persons.
3	Any natural persons Customer chooses to engage through the Services.

2. **Categories of Customer Personal Data**

The Customer Personal Data Processed concern the following categories of data (please specify):

#	Category
1	Email address
2	First and/or Last Name
3	IP address
4	POPin Answers, Comments, and Votes
5	Mobile OS version

3. **Sensitive data**

The Customer Personal Data Processed concern the following special categories of data (please specify):

#	Category
1	The Services are not intended to Process special categories of data.

4. **Processing operations**

The Customer Personal Data will be subject to the following basic Processing activities (please specify):

#	Operation
	An authorized Customer representative can ask a question to any group of other Customer representatives in order to source feedback on any topic
	POP will evaluate feedback for sentiment, themes, and trends
	POP's Sales and Customer Success teams will engage in a consultative role on the POPin questions and results

POP will implement the following types of security measures:

Security Assessments and Compliance

Data Centers

POPin's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

Physical Security

POPin utilizes ISO 27001 and FISMA certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely.

For additional information see: https://aws.amazon.com/security

System Security

System Configuration

System configuration and consistency is maintained via custom configuration management software that is version controlled, peer reviewed, and tested thoroughly before implementing in our Production environment. We use AWS Best Practice tools to enforce Infrastructure and Application security.

System Authentication

Operating system access is limited to the POPin Development Team and requires username, key, and IP authentication. Operating systems do not allow password authentication to prevent password brute force attacks, theft, and sharing.

Network Security

Segmentation

POPin Production and Staging environments network segments are completely isolated and independent of each other. There is no data sharing between them. All Customer data is only hosted in the Production environment.

Firewalls

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to.

Port Scanning

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

Application Security

The POPin Platform is a Multi-Tenant architecture, however user access is granted on a 'per-Question' basis. User verification and password recovery are done via time limited single use links/tokens sent to the registered email. Production servers are outfitted to send secure cookies and other security related headers and have been vetted to conform to OWASP Security Best Practices.

SSO

Customers can simplify their access to our application by using our secure SAML2 SSO integration.

Data Security

Customer Data

All data is encrypted at rest using AWS Best Practices. Only our POPin Development Team can access data directly and only after username, key, and IP authentication.

Vulnerability Management

System

POPin is notified of vulnerabilities through internal and external assessments, system patch monitoring, and third party mailing lists and services. Each vulnerability is reviewed to determine if it is applicable to POPin's environment, ranked based on risk, and assigned accordingly.

We continually apply the latest security updates to all operating systems and applications, in order to mitigate exposure to vulnerabilities. This process allows POPin to keep the environment up-to-date.

Application

We undergo penetration tests, vulnerability assessments, and source code reviews to assess the security of our application, architecture, and implementation. Our third party security assessments cover all areas of our platform including testing for OWASP Top 10 web application vulnerabilities. POPin works closely with external security assessors to review the security of the POPin platform and apply best practices.

Issues found in POPin applications are risk ranked, prioritized, assigned accordingly for remediation, and POPin's Development Team reviews each remediation plan to ensure proper resolution.

Backups

Customer Data

Customer Data stored in our POPin platform are automatically backed up every night to secure, access controlled, and redundant storage. We use these backups to automatically bring our application back online in the event of an outage.

POPin Platform

From our instance images to our databases, each component is backed up to secure, access-controlled, and redundant storage. We apply AWS Best Practices to ensure High-Availability of our Infrastructure and Primary Databases.   In addition to standard backup practices, POPin's infrastructure is designed to scale and be fault tolerant by automatically failing over to healthy instances and reducing the likelihood of any issues being visible to the user.

Disaster Recovery

Customer Data

The POPin platform is designed to automatically failover to Synced and Redundant databases in the event of the failure of our Primary Databases.

POPin Platform

The POPin platform is designed for stability, scaling, and inherently mitigates common issues that lead to outages while maintaining recovery capabilities. Our platform maintains redundancy to prevent single points of failure and utilizes multiple data centers designed for resiliency. In the case of an outage, the platform is deployed across multiple data centers using current system images and data is restored from backups. POPin reviews platform issues to understand the root cause, impact to customers, and improve the platform and processes.

Customer Data Retention and Destruction

Within 30 days of a written data deletion request, by an authorized representative of the tenant company, we will remove tenant related data from the DB. Backed up data will be rotated out of our archives within 30 days after deletion from the DB.

Decommissioning hardware is managed by our infrastructure provider using a process designed to prevent customer data exposure. AWS uses techniques outlined in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data.

For additional information see: https://aws.amazon.com/security

Privacy

POPin has a published privacy policy that clearly defines what data is collected and how it is used. POPin is committed to customer privacy, transparency, and the anonymity of our users.

We takes steps to protect the privacy of our customers and protect data stored within the platform. Some of the protections inherent to POPin's products include authentication, access controls, data transport

encryption, HTTPS restrictions to our platform, and all customer data encrypted at rest. For additional information see: https://popinnow.com/privacy-policy

Access to Customer Data

General POPin staff do not access or interact with customer data or applications as part of normal operations. Our POPin Customer Success (CS) team does review your data on your behalf as needed, but generally at the request of the customer, for support purposes or where required by law. Customer data is access controlled and all access restricted to the POPin CS or Developer Team.