Security of Data and Privacy Policy

United States

Bouk Merchants

Before you use the products and services, please read these terms carefully. By executing the agreement or master agreement (herein referred to as "agreement") with Bouk or using the services, platform, and/or products, you, and any entities that you represent and all your franchisees and/or affiliates (if any) ("you" or "merchant") agree to be bound by the terms contained herein in addition to the terms in the agreement (as defined herein). The terms of this agreement apply only to the subject matter herein.

SECTION A

DEFINITIONS.

1. **Personal Data** - This is information about a recognized or known individual that is utilized to determine or track that person (a natural person's identity), either alone or in combination with additional personal or distinguishing data that is connected or associated to that person. Personal Data also includes any additional data about a precise individual that is defined as Personal Data by the data protection rules prevalent in the jurisdictions where that person resides.

2. **Process** or **Processing** - The recording, utilization, accessibility to, publication, storing, transmission, or other handling of Personal Data of any private citizen that the discloser permits to use or access a service is referred to as this.

3. **Systems** - means a Party's computer systems or network (including third-party systems such as Amazon Web Services) that host, process or store the Discloser's Personal Data.

4. Privacy and Security Laws - This refers to U.S. federal, state, and municipal regulations, as well as non-U.S. laws, that govern the safety and confidentiality of Personal Data and are applicable to Bouk and/or Merchant, as the case may be.

5. **Security Incident** - This refers to illegal accessibility to or collection of Personal Data held on User's devices, resulting in the breach of Personal Data for which Discloser is liable.

SECTION B

PROCESSING PERSONAL DATA.

1. Personal Data can be obtained and then used to deliver, assist, and optimize the Services, enforce the Contract and further the Merchant-Bouk business relationship, adhere to rules, and act in conformity with the Discloser's written instructions or otherwise in compliance with the Agreement Terms during the provision and use of the Offerings. Discloser gives Recipient right to obtain, utilize, retain, and transmit Personal Data for the exclusive purpose of delivering or administering the services.

2. Upon becoming aware of any confirmed unauthorized or unlawful breach of security that leads to the destruction, loss, alteration, or unauthorized disclosure of or access to Discloser Personal Data, Recipient shall notify Discloser.

SECTION C

COMPLIANCE WITH PRIVACY AND INFORMATION SECURITY REQUIREMENTS.

1. If relevant, the recipient must adhere to all applicable privacy and confidentiality laws, as well as the EU-US Privacy Shield Framework established by the US Department of Commerce for the capture, utilization, and storage of Personal Data from the European Economic Area. In addition, Recipient must adhere to the United States-Swiss Safe Harbor framework, or its alternative, as laid forth by the United States Department of Commerce for the acquisition, processing, and storage of Personal Data from Switzerland, if applicable. The CCPA and TCPA are examples of privacy and security laws.

2. Recipient shall ensure appropriate technical and organizational security measures directly correlated with the sensitivity of the Personal Data processed on Discloser's behalf, which are intended to shield the safety, trustworthiness, and privacy of such Personal Data, as well as prevent unauthorized or malicious destruction, damage, modification, and unauthorized disclosure or access.

3. Access; Contacts - Only Members who have a cogent reason to access Personal Data in order to offer, support, and enhance the Products and Services shall have access to Personal Data.

SECTION D

RESPONSE. TO **SECURITY INCIDENT**

Recipient shall, In the event Recipient discovers a Security incident;

1. Notify discloser of the discovery of the security Incident. Such notice shall summarize the known circumstances of the Security Incident and the corrective action taken or to be taken by Recipient.

2. Conduct an investigation of the circumstances of the Security Incident.

3. Use commercially reasonable efforts to remediate the Security Incident.

4. Use commercially reasonable efforts to communicate and cooperate with Discloser concerning its response to the Security Incident.

5. Allow Discloser to run a security audit to assess whether the Security Incident has been resolved at Recipient's sole expense.

SECTION E

DISCLOSER OBLIGATIONS.

Discloser acknowledges that it has a legal basis for allowing Recipient to process Personal Data, and/or that Discloser has made such disclosures and acquired such permit and approvals for Recipient to lawfully treat Personal Data.

SECTION F

RESTRICTED AREAS.

Intending Merchants/Sellers who reside in California and the European Economic Area are presently not eligible to utilize Bouk platforms and services. You accept to only use Bouk Platforms and Services in the areas/regions/states/locations where Bouk operates. If you live in California or the European Economic Area ("EEA"), please, kindly do not download/use/access the Bouk Platform or Services, neither should you give nor enable Bouk receive personal information from you a California resident or EEA citizen.