Vetty

VETTY GDPR AND UK DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") supplements Vetty's Terms of Service available at https://vetty.co/customer-terms-of-service/, as updated from time to time between Customer and Company, or other written agreement between Customer and Company governing Customer's use of the Services (the "Agreement") when the GDPR or UK Data Protection Act ("UKDPA") applies to Customer's use of the Services. Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 10 of this DPA.

1. Data Processing.
    a. Scope and Roles. This DPA applies when Company processes information it receives from Customer. In this context, Company will act as processor to Customer, who can act either as controller or processor.
    b. Inaccurate or Outdated Data. If Company becomes aware that information transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. As allowed by law, Company will cooperate with Customer to erase or rectify inaccurate or outdated information transferred under the Standard Contractual Clauses.
    c. Details of Data Processing.
        i. Subject matter. The subject matter of the data processing under this DPA is information required to conduct background screening.
        ii. Duration. The duration of the data processing under this DPA is defined in the Agreement and subject to data retention requirements of the Fair Credit Reporting Act and other consumer protection laws and regulations
        iii. Purpose. The purpose of the data processing under this DPA is Customers' use of the Services for background screenings.
        iv. Nature of the processing. The nature of the data processing under this DPA involves receiving, verifying, analyzing and returning data in connection with the Services.

   v. Categories of data. The type of the data processing under this DPA is personal information about data subjects that Customer transfers to Company. This may include sensitive information, i.e., criminal convictions and offenses. Company handles and protects this information in accordance with the policies and practices in Section 4 of this DPA.

   vi. Categories of data subjects. The data subjects are candidates, employees, and independent contractors about whom Customer is making employment-related decisions.

2. Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR and UKDPA.
3. Customer Instructions. The parties agree that this DPA and the Agreement constitute Customer's documented instructions regarding Company's processing of information. Company will process information only in accordance with these Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of these instructions (if any) require prior written agreement between Company and Customer.
4. Confidentiality Obligations of Company Personnel. Company restricts its personnel from accessing information in Reports without authorisation as described in our Information Security Policy and Procedures. Company imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.
5. Security of Data Processing. Company takes robust measures to secure all data that it receives, houses, and transmits. Company is SOC 2 certified (report available upon request). Our data security measures include the following:
   a. We implement the following policies (available upon request) relating to data security:
      - Acceptable Use Policy
      - Access Control and Termination Policy
      - Change Management Policy
      - Code of Conduct
      - Configuration and Asset Management Policy
      - Data Classification Policy

- Data Retention and Disposal Policy
- Encryption and Key Management Policy
- Information Security Policy
- Network Security Policy
- Business Continuity and Disaster Recovery Policy
- Risk Assessment and Treatment Policy
- Secure Development Policy
- Security Incident Response Plan
- Vulnerability and Patch Management Policy

b. We employ security tools within our production environment to identify traffic and alert us to potential security events.

c. We implement logical access security software, infrastructure, and architectures over protected information assets to protect them from security events.

d. All information transmitted using our network is secured using a minimum of 128-bit SSL encryption.

e. We store and back up all of our data in the AWS cloud, and it is all protected using a minimum of 128-bit SSL encryption. We do not store data locally.

6. Sub-processing.

a. Authorized Sub-processors. Customer provides general authorisation to Company's use of sub-processors to provide processing activities on behalf of Customer ("Sub-processors") in accordance with this Section. Customer may obtain a current list of Company's Sub-processors by emailing legal@vetty.co.

b. Sub-processor Obligations. Where Company uses a Sub-processor as described in this section:

i. Company will restrict the Sub-processor's access to information to only to what is necessary to provide or maintain the Services;

ii. Company will enter into a written agreement and Standard Contractual Clauses with the Sub-processor; and

iii. Company will remain responsible for its compliance with the obligations of this DPA.

7. Security Incident Notification.

a. Security Incident. Company will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

b. Company Assistance. To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), Company will cooperate with and assist Customer by including in the notification under Section 6(a) such information about the Security Incident as Company is able to disclose to Customer, taking into account the nature of the processing, the information available to Company, and any restrictions on disclosing the information, such as confidentiality.

c. Unsuccessful Security Incidents. Customer agrees that an unsuccessful Security Incident will not be subject to this Section 6. An unsuccessful Security Incident is one that results in no unauthorized access to information received from Customer or to any of Company's equipment or facilities storing information, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

d. Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means Company selects, including via email. It is Customer's responsibility to ensure Customer's administrators maintain accurate contact information on Company's Customer portal and secure transmission at all times. Company's obligation to report or respond to a Security Incident under this Section 6 is not and will not be construed as an acknowledgement by Company of any fault or liability of Company with respect to the Security Incident.

8. Transfers of Personal Data.

a. Application of Standard Contractual Clauses. The Standard Contractual Clauses will only apply to information that is transferred, either directly or via onward transfer, to any Third Country, (each a "Data Transfer"). When information is transferred from the UK, the UKDPA applies.

i. When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

ii. When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that Customer will fulfill Company's obligations to Customer's controllers under the Processor-to-Processor Clauses.

9. Disputes. The governing law and choice of forum for any disputes under the Standard Contractual Clauses will be Ireland (under the GDPR) and England and Wales (under the UKDPA). The competent supervisory authority will be Ireland.
10. Termination of the DPA. This DPA will continue in force until the termination of the Agreement (the "Termination Date").
11. Entire Agreement; Conflict. This DPA incorporates the Standard Contractual Clauses and UKDPA IDTA Addendum by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control. Nothing in this document varies or modifies the Standard Contractual Clauses.
12. Definitions. Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

a. "controller" has the meaning given to it in the GDPR.

b. "Controller-to-Processor Clauses" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and located here: **VETTY CONTROLLER PROCESSOR CLAUSES document.**

c. "EEA" means the European Economic Area.

d. "GDPR" means Regulation 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).

e. "IDTA Addendum" means the International data transfer addendum to the European Commission's standard contractual clauses for international data transfers issued under Section 119A of the Data Protection Act 2018 and following Parliamentary approval came into force on March 21, 2022, and here: **VETTY IDTA Addendum.**

f. "processing" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

g. "processor" has the meaning given to it in the GDPR.

h. "Processor-to-Processor Clauses" means the Standard Contractual Clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and located here: **VETTY PROCESSOR TO PROCESSOR CLAUSES document.**

i. "Security Incident" means a breach of Company's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, data received from Customer.

j. "Standard Contractual Clauses" means (i) the Controller-to-Processor Clauses, or (ii) the Processor- to-Processor Clauses, as applicable.

k. "Third Country" means a country outside the EEA not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).