

ThreatMetrix Data Processing Addendum

Last updated: March 28, 2018

1. Definitions

1. “Data Protection Laws” means all data protection laws and regulations, including the GDPR and any implementing, derivative or related legislation, rule or regulation of the European Union (“Union”), a Union member state (“Member State”), or the United Kingdom (“UK”), applicable to the processing of personal data under the Agreement.
2. “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) from 25 May 2018.
3. The lowercase terms “controller”, “data subject”, “personal data”, “personal data breach”, “processing”, and “processor” will have the meanings ascribed to them in the Data Protection Laws, and where the relevant Data Protection Laws use the term ‘personal information’, ‘data controller’ or ‘data processor’, they shall be read as personal data, controller and processor, respectively.

2. Scope

1. This Data Processing Addendum (“DPA”) applies to the processing of personal data, within the scope of the Data Protection Laws, by ThreatMetrix on your behalf under the Agreement. This DPA does not apply where ThreatMetrix is a controller of personal data.

3. Processing

1. ThreatMetrix shall implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the relevant Data Protection Laws and ensure the protection of the rights of the data subject and the standard of protection will be at least comparable to the protection required under the relevant Data Protection Laws.
2. ThreatMetrix shall not engage another processor without your prior specific or general written authorization. In the case of general written authorization, ThreatMetrix shall inform you of any intended changes concerning the addition or replacement of other processors, thereby giving you the opportunity to object to such changes in the manner more specifically set forth herein.
3. The processing of personal data on your behalf by ThreatMetrix shall be governed by this DPA. In particular, ThreatMetrix shall:
 1. process the personal data only on your documented instructions, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union, UK or Member State law to which ThreatMetrix is subject; in such a case, ThreatMetrix shall inform you of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
 2. ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
 3. take all measures required pursuant to Article 32 of the GDPR;
 4. respect the conditions referred to in paragraphs 2.2 and 2.4 for engaging another processor;
 5. taking into account the nature of the processing, assist you by taking appropriate technical and organizational measures, insofar as this is possible, for the fulfilment

- of your obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
6. assist you in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to us;
 7. at your choice, delete or return to you all the personal data after the end of the provision of services relating to processing and delete existing copies unless Union, UK or Member State law requires storage of the personal data;
 8. make available to you all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by you or another auditor you mandate.

ThreatMetrix shall immediately inform you if, in ThreatMetrix's opinion, an instruction from you to us infringes the GDPR or other Union, UK or Member State data protection provisions.

4. Where ThreatMetrix engages another processor for carrying out specific processing activities on your behalf, the same data protection obligations as set out in this DPA shall be imposed on that other processor by way of a contract or other legal act under Union, UK or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil those data protection obligations, ThreatMetrix shall (subject to the terms of the Agreement) remain fully liable to you for the performance of that other processor's obligations.
5. The subject matter of the processing is the personal data provided in respect of the Services under the Agreement. The duration of the processing is the duration of the provision of the Services under the Agreement. The nature and purpose of the processing is in connection with the provision of the Services under the Agreement. The types of personal data processed are the personal data provided by you to ThreatMetrix in respect of the Services under the Agreement and may include names; account markers; e-mail addresses; shipping addresses; contact details; government-issued identification; date of birth; place of birth; IP address; and other types of personal data submitted through the Services. The categories of data subjects are your representatives, users of the Services, and clients, prospects, suppliers, business partners and others whose personal data is submitted to the Services.
6. The Agreement including this DPA, along with your use and configuration in the Services, are your complete and final documented instructions to us for the processing of personal data. Additional or alternate instructions must be agreed upon separately by the parties. ThreatMetrix will ensure that its personnel engaged in the processing of personal data will process personal data only on your documented instructions, unless required to do so by Union, UK, Member State or other applicable law.
7. On expiry or termination of your use of the Services, ThreatMetrix shall delete or return personal data in accordance with the terms and timelines set forth in the Agreement, unless Union, UK, Member State or other applicable law requires storage of the personal data.

4. Subprocessing

1. You hereby provide us general authorization to engage other processors for the processing of personal data in accordance with this DPA. ThreatMetrix shall maintain a list of such processors at <https://risk.lexisnexis.com/terms/subprocessors>, which ThreatMetrix may update from time to time. At least 14 days before authorizing any new such processor to process personal data, ThreatMetrix shall update the list on its website. You may object to the change without penalty by notifying us within 14 days after the website is updated and describing your reasons to object. Without prejudice to any applicable refund or termination

rights you have under the Agreement, ThreatMetrix shall use reasonable endeavors to avoid processing of personal data by such new processor to which you reasonably object.

5. Data Subject Rights

1. ThreatMetrix shall, to the extent legally permitted, promptly notify you of any data subject requests ThreatMetrix receives and reasonably cooperate with you to fulfil your obligations under the Data Protection Laws in relation to such requests. You shall be responsible for any reasonable costs arising from ThreatMetrix providing assistance to you to fulfil such obligations.

6. Transfer

1. ThreatMetrix shall ensure that, to the extent that any personal data originating from the UK or European Economic Area ("EEA") is transferred to a country or territory outside the UK or EEA that has not received a binding adequacy decision by the European Commission or a competent national data protection authority, such transfer shall be subject to appropriate safeguards in accordance with the Data Protection Laws (including Article 46 of the GDPR).

7. Security of Processing

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, ThreatMetrix shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including those set forth in the Agreement and inter alia as appropriate:
 1. the pseudonymization and encryption of personal data;
 2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
 4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. ThreatMetrix shall take steps to ensure that any natural person acting under the authority of either party who has access to personal data does not process them except on instructions from you, unless he or she is required to do so by Union, UK or Member State law.

8. Personal Data Breach

1. ThreatMetrix shall notify you without undue delay after becoming aware of a personal data breach and shall reasonably respond to your requests for further information to assist you in fulfilling your obligations under the Data Protection Laws (including Articles 33 and 34 of the GDPR as applicable).

9. Records of Processing Activities

1. ThreatMetrix shall maintain all records required by the Data Protection Laws (including Article 30(2) of the GDPR as applicable) and, to the extent applicable to the processing of personal data on your behalf, make them available to you as required.

10. Audit

1. Audits shall be:

1. subject to the execution of appropriate confidentiality undertakings;
2. conducted no more than once per year, unless a demonstrated reasonable belief of non-compliance with the Agreement has been made, upon thirty (30) days written notice and having provided a plan for such review; and
3. conducted at a mutually agreed upon time and in an agreed upon manner.

11. Conflict

1. If there is any conflict or inconsistency between the terms of this DPA and the Agreement, the terms of this DPA shall control to the extent required by law.