Rakuten Advertising

GENERAL DATA PROTECTION REGULATION ADDENDUM TO THE GENERAL TERMS AND CONDITIONS
(GDPR Article 28 Controller to Processor terms)

Last updated: December 7, 2021

By using the Services, Supplier Technology, and/or entering into any Order Form, Company agrees to the Supplier General Data Protection Regulation Addendum to the Terms and Conditions (the "**C2P Addendum**"). Supplier and Company are each a "Party" and collectively the "Parties."

This C2P Addendum is an integral part of the Terms and Conditions**.** Any words or terms not otherwise defined in this Addendum have the same meaning as in the Terms and Conditions**.** In the event of a conflict between definitions in the Terms and Conditions and this Addendum, the definitions within this Addendum control.

1. Definitions.

(a) "**Company**" means the entity(ies) as defined in the Order Form.

(b) "**Company Personal Data**" means Personal Data controlled by Company and disclosed to Rakuten Advertising (or collected by Rakuten Advertising on behalf of Company) in circumstances where Rakuten Advertising is instructed by Company to act as the Processor of such Personal Data and as further set out at Schedule 1 hereto.

(c) "**Data Protection Law(s)**" means all worldwide data protection and privacy laws and regulations applicable to the Company Personal Data, including, where applicable, EU/UK Data Protection Law and the Swiss DPA.

(d) "**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

(e) "**European Territories**" means together the European Economic Area ('EEA"), United Kingdom, and Switzerland.

(f) **"Personal Data,**" "**Process/Processing,**" "**Controller,**" "**Processor,**" "**Data Subject**" and "**Supervisory Authority**" shall have the same meanings given to them in EU/UK Data Protection Law.

(g) "**Rakuten Advertising**" means the following Rakuten Advertising entities: Rakuten Marketing LLC organized and existing under the laws of Delaware, USA successor to LinkShare Corporation ("**RM United States**"), Rakuten Marketing Europe Limited successor to LinkShare Limited ("**RM Europe**"), Rakuten Marketing Australia Pty Limited successor to LinkShare Australia Pty Ltd ("**RM Australia**"), or Rakuten Brazil Holdings, LLC successor to LinkShare Brazil Holdings, LLC ("**RM Brazil**").

(h) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of Company Personal Data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Company Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of Company Personal Data from Switzerland to any other country which is not determined to provide adequate protection for Personal Data by the Federal Data Protection and Information Commission or Federal Council (as applicable).

(i) "**Standard Contractual Clauses**" means: (i) where the EU GDPR or Swiss DPA applies, the contractual

clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

(j) "**Sub-processor**" means a third party engaged directly by Rakuten Advertising to Process Company Personal Data on Rakuten Advertising's behalf.

(k) "**Swiss DPA**" means the Swiss Federal Act on Data Protection 1992 (including as amended or superseded).

2. Role of the Parties.

In order to receive the Services under the Terms and Conditions, as set out in the Order Form, Company discloses Company Personal Data to Rakuten Advertising (or Rakuten Advertising collects Company Personal Data on behalf of Company). For the purposes of this DPA, Company is the Controller of the Company Personal Data and Rakuten Advertising is the Processor of the Company Personal Data.

3. Company's Controller Obligations.

In its role as Controller of the Company Personal Data, Company shall:

(i) comply at all times with Data Protection Law(s);

(ii) ensure that it has all necessary rights (including, where required, consent of Data Subjects) to disclose Company Personal Data to Rakuten Advertising for Rakuten Advertising to Process the Company Personal Data under the Terms and Conditions (or for Rakuten Advertising to collect Company Personal Data on behalf of Company), including Rakuten Advertising's use of cookies and tracking technologies, as set out in Schedule 1 to this DPA; and

(iii) fulfil its transparency obligations and shall ensure that the Company Sites that Company promotes through its use of the Services display a privacy policy which complies with Data Protection Laws and which includes information regarding Rakuten Advertising's processing of the Company Personal Data for online advertising as anticipated under this DPA.

4. Rakuten Advertising's Processor Obligations.

(a) The nature, purpose, subject matter, duration of Rakuten Advertising's Processing of the Company Personal Data, and the types of Company Personal Data Processed and the categories of Data Subjects are as set out in Schedule 1 to this DPA and Rakuten Advertising shall only process the Company Personal Data in accordance with this DPA.

(b) In its role as Processor of the Company Personal Data, Rakuten Advertising shall:

(i) Process the Company Personal Data in accordance with the Company's written instructions as set out in the Terms and Conditions (including Order Forms) and this DPA. If Rakuten Advertising is required by law to Process or disclose the Company Personal Data for any other purpose, it shall notify Company as soon as the law permits it to do so;

(ii) inform Company if it believes the Company's instructions infringe the Data Protection Laws or any other applicable law;

(iii) comply with applicable obligations of Processors as required under EU/UK Data Protection Law;

(iv) not subcontract any processing of the Company Personal Data to a third party Sub-processor without the prior written consent of Company, which consent, where Company is a Processor, shall reflect the instructions of its controller. Notwithstanding this, Company consents to Rakuten Advertising

engaging third party Sub-processors from an agreed list to process Company Personal Data provided that Rakuten Advertising: (i) provides at least ten (10) business days' prior notice of the engagement of any subprocessor to be added to the list or the termination of any subprocessor to be removed from the list (including details of the processing it performs or will perform), which may be given by posting details of such engagement or termination at the following URL: https://rakutenadvertising.com/legal-notices/subprocessors (ii) procures that all Sub-Processors are subject to written terms that protect the Company Personal Data, in substance, to the same standard provided by the terms of this DPA; and (iii) remains fully liable for any breach of this DPA that is caused by an act, error or omission of its Sub-processor. Company may object to Rakuten Advertising appointment of a new Sub-Processor on reasonable grounds relating to the protection of the Company Personal Data, by notifying Rakuten Advertising in writing within the relevant ten (10) business day notice period. Upon receipt of such objection from Company, Rakuten Advertising shall make a commercially reasonable change to the Sub-Processor or to the Services to avoid using such Sub-Processor for the processing of Company Personal Data. If Rakuten Advertising is unable to make such change within a reasonable period of time, which shall not exceed thirty days, Company may terminate those services which cannot be provided by Rakuten Advertising without the use of the objected-to Sub-Processor by providing written notice to Rakuten Advertising;

(v) have in place and maintain throughout the term appropriate technical and organizational security measures to protect Company Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. The appropriate technical and organizational security measures by Rakuten Advertising and its third parties shall be commensurate with the nature of Company Personal Data to be protected and with regard to the state of the art and cost of implementation, the nature, scope, context and purposes of the Processing;

(vi) ensure that all Rakuten Advertising employees are informed of the confidential nature of the Company Personal Data and bound by a legal obligation of confidentiality;

(vii) notify Company without undue delay after it becomes aware of a Personal Data breach within Rakuten Advertising's environment or under its control and which affects Company Personal Data;

(viii) taking into account the nature and use of Company Personal Data in providing Services (and to the extent the Company does not otherwise have access to the relevant information), reasonably assist Company in complying with its obligations as Controller under EU/UK Data Protection Law in relation to Data Subject rights, Personal Data breach notifications and data protection impact assessments.

(ix) upon Company's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Terms and Conditions, make available to Company that is not a competitor of Rakuten Advertising (or Customer's independent, third-party auditor that is not a competitor of Rakuten Advertising) a copy of Rakuten Advertising's then most recent published third-party audits or certifications, as applicable.

(x) on termination or expiry of the Terms and Conditions, securely destroy the Company Personal Data and certify to Company that it has done so, unless legal or regulatory obligations prevent it from destroying all or part of the Company Personal Data. In that case, Rakuten Advertising shall use its reasonable measures to protect confidentiality of the Company Personal Data and will not actively further Process such data.

5. International Data Transfers.

The Parties hereby acknowledge and agree that in providing the Services, conducting the Actions and otherwise fulfilling Order Forms, Personal Data may be transferred from European Territories to the United States or other territory(ies) whose level of protection for Personal Data differs from that of the European Territories. Where Company makes a Restricted Transfer to Rakuten Advertising for the purposes of the Services, such transfer shall be subject to the appropriate Standard Contractual Clauses, as follows:

(a) in relation to Company Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 4(b)(iv) of this DPA;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed the laws of Luxembourg;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Luxembourg;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA; and

(b) in relation to Company Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(i) For so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of Personal Data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("**Prior C2P SCCs**") for transfers of Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between Company and the Rakuten Advertising entity to which a Restricted Transfer is made on the following basis:

(A) Appendix 1 shall be completed with the relevant information set out in Schedule 1 to this DPA;

(B) Appendix 2 shall be completed with the relevant information set out in Schedule 2 to this DPA; and

(C) the optional illustrative indemnification Clause will not apply.

(ii) Where sub-clause (b)(i) above does not apply, but Company and Rakuten Advertising are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

(A) The EU SCCs, completed as set out above in Clause 5(a) of this DPA shall also apply to transfers of Company Personal Data, subject to sub-clause (B) below; and

(B) The UK Addendum shall be deemed executed between Company and the Rakuten Advertising entity to which the Restricted Transfer is made, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Company Personal Data;

(iii) If neither sub-clause (b)(i) or sub-clause (b)(ii) applies, then Company and Rakuten Advertising shall cooperate in good faith to implement appropriate safeguards for transfers of the relevant Company Personal Data as required or permitted by the UK GDPR without undue delay;

(c) in relation to Company Personal Data that is protected by the Swiss DPA, the EU SCCs will apply as set out in Clause 5(a) amended as follows:

(i) references to 'Regulation (EU) 2016/679' in the EU SCCs will be deemed to refer to the Swiss DPA;

(ii) references to specific articles of 'Regulation (EU) 2016/679' will be deemed replaced with the equivalent article or section of the Swiss DPA,

(iii) references to 'EU', 'Union' and 'Member State' will be deemed replaced with 'Switzerland',

(iv) references to the 'competent supervisory authority' and 'competent courts' are replaced with the 'Swiss Federal Data Protection Information Commissioner' and 'applicable courts of Switzerland' (as applicable),

(v) in Clause 17, the EU SCCs will be governed by the laws of Switzerland, and

(vii) in Clause 18(b), disputes shall be resolved before the competent courts of Switzerland;

(d) in the event that any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

6. International Transfers – Processor to Controller ("P2C") Restricted Transfers

Where the Rakuten Advertising entity that is party to this C2P Addendum is based in the European Territories and makes a Restricted Transfer of Company Personal Data on a Processor-to-Controller basis to Company based outside the European Territories for the purposes of providing the Services, then, such transfer shall be subject to the appropriate Standard Contractual Clauses, as follows:

a) in relation to Company Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Four will apply;
(ii) in Clause 7, the optional docking Clause will not apply;
(iii) in Clause 11, the optional language will not apply;
(iv) in Clause 17, the EU SCCs will be governed by the laws of Luxembourg;
(v) in Clause 18(b), disputes shall be resolved before the courts of Luxembourg;
(vi) in Annex I, Parts A and B: with the information set out in Schedule 1 to this DPA;

b) in relation to Company Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(i) For so long as it is lawfully permitted to rely on the standard contractual clauses for the transfer of personal data to Controllers set out in the European Commission's Decision 2004/915/EC of 27 December 2004 ("Prior C2C SCCs") for transfers of personal data from the United Kingdom, the Prior C2C SCCs shall apply on the following basis:

(A) in Clause II (h): the Company (as data importer) and Rakuten Advertising (as data exporter) choose option (iii);

(B) in Annex B: with the information set out in the relevant part of Schedule 1 to this DPA; and

(C) the "Illustrative Commercial Clauses (Optional)" shall be deemed deleted.

(ii) Where sub-clause (b)(i) above does not apply, but Rakuten Advertising (as data exporter) and Company (as data importer) are lawfully permitted to rely on the EU SCCs for transfers of Company Personal Data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("UK Addendum") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

(A) The EU SCCs, completed as set out above in clause 6(a), shall also apply to

transfers of such Company Personal Data, subject to sub-clause (B) below;

(B) The UK Addendum shall be deemed executed between Rakuten Advertising (as data exporter) and Company (as data importer), and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Company Personal Data.

(iii) If neither sub-clause (b)(i) or sub-clause (b)(ii) applies, then the Rakuten Advertising and Company shall cooperate in good faith to implement appropriate safeguards for transfers of such Company Personal Data as required or permitted by the UK GDPR without undue delay.

c) in relation to Company Personal Data that is protected by the Swiss DPA, the EU SCCs will apply as set out in Clause 6(a) amended as follows:

(i) references to 'Regulation (EU) 2016/679' in the EU SCCs will be deemed to refer to the Swiss DPA;

(ii) references to specific articles of 'Regulation (EU) 2016/679' will be deemed replaced with the equivalent article or section of the Swiss DPA,

(iii) references to 'EU', 'Union' and 'Member State' will be deemed replaced with 'Switzerland',

(iv) references to the 'competent supervisory authority' and 'competent courts' are replaced with the 'Swiss Federal Data Protection Information Commissioner' and 'applicable courts of Switzerland' (as applicable),

(v) in Clause 17, the EU SCCs will be governed by the laws of Switzerland, and

(vii) in Clause 18(b), disputes shall be resolved before the competent courts of Switzerland;

d) in the event that any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

7. Indemnification.

Company shall defend, indemnify and hold harmless Rakuten Advertising from and against any and all liabilities, damages, loses, demands claims, suits or judgments resulting from a third party claim arising out of Company's breach of its warranties or any of its obligations under this DPA or the Data Protection Laws.

8. Survival.

This DPA shall survive termination or expiration of the Terms and Conditions.

Rakuten Advertising

SCHEDULE 1
TO THE DATA PROCESSING ADDENDUM
RAKUTEN ADVERTISING AS A DATA PROCESSOR
DATA PROCESSING DESCRIPTION

This Schedule forms part of the DPA and describes the processing that Rakuten Advertising will perform on behalf of Company.

A. LIST OF PARTIES

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

1.	**Name:**	The entity(ies) as defined in the Order Form.
	Address:	The notice address as defined in the Order Form.
	Contact person's name, position and contact details:	The contact person's information as defined in the Order Form.
	Activities relevant to the data transferred under these Clauses:	Use of the Company Personal Data involves the online and offline behaviour of end users as they interact with advertisements promoted through Rakuten Advertising
	Signature and date:	See above
	Role (controller/processor):	Controller

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

1.	**Name:**	Rakuten Marketing Europe Ltd
	Address:	71 Queen Victoria Street, 7th Floor, London, England, EC4V 4AY
	Contact person's name, position and contact details:	Ra-legalnotices@mail.rakuten.com
	Activities relevant to the data transferred under these Clauses:	Use of the Company Personal Data involves the online and offline behaviour of end users as they interact with advertisements promoted through Rakuten Advertising.
	Signature and date:	See above
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred:	End users who visit Company's, publishers' and advertisers' websites and other internet and mobile enabled platforms owned or controlled by Company, publishers and advertisers within the Rakuten Advertising advertising ecosystem.
Categories of Personal Data transferred:	Online identifiers from end users' device(s), identifiers created by Rakuten Advertising, Company and customers within the Rakuten Advertising advertising ecosystem.
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:	N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous for the duration of the Terms and Conditions.
Nature of the processing:	Commercial purposes including: to trace end users from a Company's Site to an advertiser platform to process commissions, to serve personalized advertisements to end users, to analyse and create online behavioural advertising, and to prevent fraud.
Purpose(s) of the data transfer and further processing:	To facilitate the provision of Services by Rakuten Advertising to Company.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	For Affiliate: up to 49 months for reporting/tracking activities.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	

Rakuten Advertising

Schedule 2
Technical and Organisational
Security Measures

Description of the technical and organisational measures implemented by the processor(s) / 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.

Measure	Description
Measures of pseudonymisation and encryption of Personal Data	Encryption is implemented for all target data, both electronic transmissions and physical electronic media, prior to sending outside the environment. Sensitive data is encrypted at rest. Backup Encryption: Active/active data, 256 bit AES encryption, Vault and Console solution for key management and crypto controls. Back-up tapes and other media is decommissioned or destroyed when no longer in use via NIST standards.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Rakuten Advertising is subject to the Rakuten Group Regulations which are an ISO 72001 and NIST 800-53 based set of policies and controls that are required for all Rakuten Group companies. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services are part of the required RGR controls and Rakuten Advertising is audited for compliance annually.
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	By design, there are no single points of failure in the RAN system architecture. The core platform technology operates in 2 geographically separated production parallel environments, so in the event of the loss of one data center, the system fails over to the other. The failover process is tested twice annually. Tracking functionality operates with 6x redundancy. All databases are backed up regularly and the system operates with an RTO of 4 hours and RPO of 0.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Rakuten Advertising performs annual privacy and data security/cybersecurity risk assessments, along with continuous network and application penetration testing conducted by a dedicated internal team, and annual penetration testing by an independent third party. Please note that audit and penetration test results are confidential per security policy and may not be shared with external parties.
Measures for user identification and authorisation	User identification and authorization is handled using a set of custom security components requiring a username and password to access all necessary system functions and reporting capabilities. SSO and MFA options will be made available in 2022.
Measures for the protection of data during transmission	Data is encrypted in transit using TLS 1.2 with AES 256 encryption.
Measures for the protection of data during storage	Data is processed and stored within the US in one of our two data centres (we have one on the East Coast in Reston, Virginia and one on the West Coast in Las Vegas, Nevada. Production data is stored on disks

	(spinning disk and ssd) in a 3PAR SAN Array managed by Oracle ASM (Automatic Storage Management) Co-location, with access controls, SVP and Senior Tech Ops Managers control access list, access to db storage least privilege model. We use Oracle encryption, file system encryption, SSL to protect data and the security posture of our network perimeter are Routers, Firewalls, Ips, Vlans. Additionally, we use Palo Alto PA5280 with Threat Prevention Subscription. From a vulnerability standpoint, security teams have continuous internal and external scanning running, vulnerabilities are given an internal score that is compared to CVSS. To detect and report any non-standard patterns, malicious activity and anomalies, Rakuten Advertising leverages anomaly detection software. Finally, we align with NIST, security standards and are in the process of getting an external ISO27001 certification. Rakuten Advertising has an information Security Incident Response Team and a business continuity program via active/standby data centers, with bursts to the cloud. Data is protected by: Encryption of the data transport channel (TLS 1.2) Encryption of data at rest (AES 256 encryption) Network access controls (Network access through the firewall requires port level allow listings, or VPN access, wireless network access required VPN/certificate MFA and a registered MAC address)
Measures for ensuring physical security of locations at which Personal Data are processed	Protection of physical access to the building (registration and proper identification required, CCTV in place, facilities use mantraps, biometric scanning, access lists and government ID required for access) User Authentication (system access follows the principle of least privilege, access rights are audited quarterly and when employee roles change, privileged access requires VP approval and server access is timeboxed using keys that expire) Recording of actions (actions are logged and stored for a minimum of 3 months, user IDs are tied to each user's LDAP record and system IDs are assigned to specific components, ID usage is logged and audited to check for inappropriate use)
Measures for ensuring events logging	All log entries must include the following attributes: (a) the time and date of the event, (b) the application associated with the event, (c) the user or process initiating the event and, if applicable, the subject acted upon, (d) the remote IP address of the initiating user or process, (e) success or failure indication, and (f) a detailed description of the event. Information systems that implement multiple logs must allow correlation of log activity across these logs via a unique ID. All successful and failed login attempts must be logged. All changes to security policy must be logged. All account creations, deletions, and modifications must be logged.

	Granting, revoking, and modification of privileges and roles must be logged. Information systems must not log confidential and sensitive personal data such as government issued IDs, passwords, etc. All failed access attempts to data, functions and services must be logged. All password resets, self-service or administrative, must be logged. All account lockouts must be logged. Internet exposed information system should write logs to a protected, non-Internet exposed information system. Access to audit logs and audit trails should be logged. Information systems should implement a log analysis function that allows searching of security log data filtered by fields available within the log. Information systems should implement a mechanism that reports a listing of all user accounts currently defined within the system. Information system should implement a mechanism that reports a listing of all roles and the users assigned to those roles currently defined within the system. Log timestamps should be set to the Coordinated Universal Time (UTC) and Daylight-Saving Time (DST) should not be applied. Logs are stored in a centralized Graylog instance where they are protected from unauthorized access or tampering.
Measures for ensuring system configuration, including default configuration	Server image access is tightly controlled and only images that have been hardened by the Rakuten Advertising TechOps and security operations teams are allowed.
Measures for internal IT and IT security governance and management	Rakuten Advertising's systems are subject to the Rakuten Group Regulations which are a set of security policies based on the ISO 27001 and NIST standards. All Rakuten Group companies must comply with the regulations and are subject to annual compliance audits.
Measures for certification/assurance of processes and products	Our data centers are ISO 27001 certified, SOC2 compliant, and follow NIST standards. We are currently in the process of getting an external ISO 27001 certification.
Measures for ensuring data minimisation	All Rakuten Advertising systems are audited annually, a process which includes a review of all data dictionaries to confirm compliance with regional regulations and continued necessity of the data handled by each system.
Measures for ensuring data quality	All data collected by the integration infrastructure is subject to security, formatting, and syntax validation in the tracking layer prior to system processing. Once processed, the data in aggregate form undergoes additional validation processing to ensure that it is not related to fraudulent activity.
Measures for ensuring limited data retention	Please see the section on data retention here: https://go.rakutenadvertising.com/hubfs/Services-Privacy-Policy-English.pdf

	Also, as noted earlier, all Rakuten Advertising systems are audited annually, a process which includes a review of all data dictionaries to confirm compliance with regional regulations and continued necessity of the data handled by each system.
Measures for ensuring accountability	All Rakuten Advertising employees and contractors are required to review and confirm acceptance of the company's policies at the start of employment. Rakuten Advertising also provides regular privacy trainings to all employees. A comprehensive training is delivered at least once per year that includes test-based certification of retention of knowledge and employee sign-off/acknowledgement that they will comply with privacy policies. The trainings cover privacy policy and data protection/data security.
Measures for allowing data portability and ensuring erasure]	Data is handled in accordance with regional law, and the company's data handling policies and implementation of the data handling policies are reviewed at least annually to ensure compliance. Erasure and recycling, or destruction of data handling media is performed per NIST standards.

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).

Measure	Description
N/A	