Data Processing Terms

Last updated on September 20, 2024

These Data Processing Terms ("Terms") form part of the Terms of Service between Printful Inc. and its affiliated companies and subsidiaries ("Printful") and Merchants (defined below) regarding Printful's services. These Terms are binding between Printful and Merchants and constitute a data processing agreement. If there is a conflict between these Terms and the Agreement (defined below), these Terms will govern. If you do not agree to these Terms, do not use the Service (defined below).

1. Definitions

1.1. Capitalized terms not otherwise defined herein shall have the same meaning as set forth in the Agreement.

1.2. “Affiliate” means, for the sole purpose of these Terms and without prejudice to any applicable use or license restrictions, limitations in service scope or other limitations provided under the Agreement, any consolidated group entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity (and “control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity), or any entity otherwise expressly designated as an “affiliate” in the Agreement.

1.3. "Agreement" means the Terms of Service or separate written contract between Printful and the Merchant regarding the use of Printful's Service.

1.4. "Controller to Processor Clauses" means (i) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 2 (Controller to Processor); [and (ii) in respect of transfers subject to the United Kingdom GDPR (UK GDPR), the standard contractual clauses for the transfer of Personal Data to data processors established in third countries set out in the Commission Decision of 5 February 2010, or any equivalent clauses issued by the relevant competent authority of the UK, in each case as amended, updated or replaced from time to time (Standard Contractual Clauses).

1.5. "Data Subject", "Controller", "Processor", "Personal Data", "Personal Data Breach", "Supervisory Authority" and “Processing” have the meanings given in the GDPR.

1.6. “Data Importer” and “Data Exporter” have the meaning set forth in the Standard Contractual Clauses.

1.7. "Data Protection Laws" means all laws and regulations, including laws and regulations of the European Economic Area (EEA) and the United States and its states, applicable to the Processing of Personal Data when providing Services, including but not limited to: (a) the General Data Protection Regulation 2016/679 (the “GDPR”); (b) the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 et seq.), and its implementing regulations, each as amended from time to time (CCPA) (c) the Privacy and Electronic

Communications Directive 2002/58/EC; (d) the UK Data Protection Act 2018 (“DPA”), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (together with the DPA, the “UK GDPR”), and the Privacy and Electronic Communications Regulations 2003; and (e) any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data, in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

1.8. "Merchant" means any person, be it a legal entity or natural person, that uses Printful's Service to execute orders and/ or deliver its products to recipients, including the Merchant's customers.

1.9. "Parties" means Printful and the Merchant.

1.10. "Processor to Processor Clauses" means, as relevant, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 3 (Processor to Processor), or any equivalent clauses issued by the relevant competent authority of the UK in respect of transfers of Personal Data from the UK, in each case as in force and as amended, updated or replaced from time to time.

1.11. “Selling” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for monetary or other valuable consideration.

1.12. “Sharing” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for targeted advertising based on Data Subjects’ Personal Data.

1.13. "Services" means print-on-demand services offered by Printful to Merchants including printing for personal use or outsourcing the printing and delivering of products to Merchant’s customers, as well as branding, warehousing and fulfillment, design, merchandising, and other services that Printful may provide in accordance with the requirements of the Merchant.

1.14. “Third Countries” means, in relation to Personal Data transfers subject to the GDPR, any country outside of the scope of the data protection laws of the European Economic Area, excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time; and (ii)] 1 in relation to Personal Data transfers subject to the UK GDPR, any country outside of the scope of the data protection laws of the UK, excluding countries approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time.

2. Subject of the Terms

2.1. These Terms govern the relationship between Printful and the Merchant in respect of any processing

of Personal Data by Printful on behalf of the Merchant.

2.2. To the extent that Printful Processes Personal Data on behalf of the Merchant, the Merchant is the Controller and Printful is the Processor and shall only process this Personal Data on behalf of the Merchant.

2.3. The Merchant hereby appoints and instructs Printful to process the Personal Data as prescribed by these Terms, including with regard to the transfer of Personal Data to a Third Country or international organization.

3. Details of Processing

To the extent that Printful Processes Personal Data on behalf of the Merchant, the following Processing details apply:

3.1 Systems storing or modifying Personal data must be regularly (no less than annually) tested for security vulnerabilities and other system weaknesses that can adversely affect confidentiality, integrity and/or availability of the Personal data ideally by a third party, but can also be performed by an in-house certified ethical hacker according to OWASP, OSINT or other testing/ auditing frameworks.

3.2 All identified security vulnerabilities or system weaknesses must be recorded and acknowledged by Printful within 24-hours. Remediation steps must be planned according to the vulnerability severity and possible impact.

3.3. Type of Personal Data. Personal Data relating to the Merchant's customers and any Personal Data in the Merchant’s Content (where applicable) and Personal Data revealed during the use of any Services, including name, email address, phone number, shipping address, and other information about Merchant’s customers, including images and data, which may appear on government-issued identity documents.

3.4. Nature and purpose of Processing. Printful processes Data in accordance with these Terms in order to provide the Merchant with the Service and otherwise ensure fulfilment of the obligations set out in the Agreement between the Merchant and Printful to the extent this involves the Processing of Personal Data. Printful only has access to the Personal Data that has been provided by the Merchant and uses such Personal Data in accordance with the Merchant's instructions as set out in these Terms.

3.5. Processing Limitations. Printful is prohibited from:

1. Selling or Sharing Personal Data obtained from Merchant;
2. Retaining, using, disclosing, or Processing Personal Data: (i) for any purpose, including any commercial purpose, other than to perform the Services provided under the Agreement and these Terms; (ii) outside of the direct business relationship between Merchant and Printful.
3. Combining, amending, or supplementing Personal Data with personal information received from another source unless directed to specifically by Merchant.

3.6. Duration of the processing. Data will be processed for the duration of the Agreement and Merchant's use of Services.

3.7. No sensitive Personal Data will be processed (unless provided in any Content).

3.8. For transfers to (sub-) processors, the subject matter, nature, and duration of the Processing will be provided on a case-by-case basis.

4. Obligations of the Merchant

4.1. The Merchant warrants that it has complied and continues to comply with the Data Protection Laws.

4.2. The Merchant confirms that the Personal Data transferred to Printful has been collected by the Merchant on a valid lawful basis and Merchant has obtained any necessary consents or given any necessary notices as prescribed by the Data Protection Laws, and that the Merchant is entitled to provide the Personal Data to Printful. Merchant expressly acknowledges that its use of Printful Services will not violate the rights of any Data Subject that has opted out of the sale or sharing of Personal Data, to the extent applicable under the Data Protection Laws.

4.3. The Merchant confirms that these Terms contain sufficient instructions to Printful regarding the processing of Personal Data, as well as the scope and purposes thereof.

4.4. If reasonably necessary, the Merchant may provide Printful with additional instructions regarding the processing of Personal Data other than those prescribed by these Terms. Such additional instructions must be reasonable for Printful to carry out, properly documented, in compliance with the Data Protection Laws and must also be accepted by Printful.

4.5. The Merchant shall be responsible for the accuracy of the Personal Data and keeping it up to date and shall inform Printful in case of any changes in the Personal Data. Merchant represents that its use of the Printful Services will not violate the rights of any Data Subject that has opted-out from the sale or other disclosure of Personal Data to the extent applicable under the Data Protection Laws.

4.6. Printful shall not be liable for any claims or complaints from Data Subjects regarding any action taken by Printful as a result of acting in accordance with instructions received from the Merchant. Further, the Merchant agrees that it will indemnify and hold harmless Printful on demand from and against all claims, liabilities, costs, expenses, loss or damage (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) incurred by Printful arising directly or indirectly from a breach of these Terms.

4.7. The Merchant shall provide Printful with additional information or documentation requested in furtherance of its legal obligations and legitimate interest in ensuring that the Merchant’s end customers are not the target of trade, financial, and economic sanctions, and do not appear on a sanctions-related list, including lists maintained by the U.S. Department of Treasury’s Office of Foreign Assets Control

("OFAC"), the U.S. Department of State, the U.S. Department of Commerce, the EU, or Her Majesty's Treasury of the UK.

5. Obligations of Printful

5.1. To the extent that Printful Processes Personal Data on behalf of the Merchant, Printful shall always follow these Terms, or as otherwise instructed by the Merchant in writing in accordance with Clause [4]. If Printful is required to Process such Personal Data by applicable law, Printful shall inform the Merchant of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

5.2. Printful shall immediately inform the Merchant if, in its opinion, a Processing instruction infringes Data Protection Laws.

5.3. Printful shall implement the appropriate technical and organizational measures specified in Schedule 1 (Technical and Organisation Security Measures).

5.4. Printful shall ensure that its personnel authorized to Process Personal Data under these Terms have committed themselves to confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

6. Assistance to the Merchant

Considering the nature of the Processing, Printful will provide all reasonable assistance to the Merchant, insofar as possible, for the fulfilment of the Merchant's obligations as the Controller in relation to:

1. Any requests from Data Subjects in respect of access to, or rectification, erasure, restriction, portability, blocking or deletion of their Personal Data in accordance with Data Protection Laws that Printful processes on behalf of the Merchant. In the event that a Data Subject sends such a request directly to Printful, Printful will promptly forward such request to the Merchant;
2. The investigation of any Personal Data Breach in relation to the Personal Data Processed on behalf of the Merchant and, if applicable, the notification to the relevant Supervisory Authority and Data Subjects regarding such Personal Data Breach (where required); further, Printful shall notify the Merchant of any Personal Data Breach without undue delay after becoming aware of a Personal Data Breach; and
3. Where appropriate, the preparation of data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority.

7. Sub-processors and Data Transfer

7.1. For Printful to be able to meet its obligations prescribed by the Agreement and to administer and provide the Service, the Merchant hereby grants Printful general written authorization to engage sub-processors. Merchant can obtain the list of current sub-processors engaged by Printful by contacting the registered account email address at the end of these Terms or through the Merchant's account with Printful. The list will include the identities of sub-processors, provided services and country of location.

7.2. The Sub-processors list may be modified from time to time, including by adding or replacing sub-processors thereon without additional notice to the Merchant. Merchant waives notice of and consents to Printful's use of such new sub-processors.

Merchant may object to Printful's use of a Sub-processor by notifying Printful in writing. In the event Merchant objects to a Sub-processor, as permitted in the preceding sentence, Printful will use commercially reasonable efforts to make available to Merchant a change in the services or recommend a commercially reasonable change to Customer's configuration or use of the services to avoid Processing of Personal Data by the objected-to Sub-processor without unreasonably burdening the Merchant. If Printful is unable to make available such change, the Merchant may as its sole remedy, terminate the portion of the Service which cannot be provided by Printful without the use of the objected-to Sub-processor, provided that the Parties shall always first use their mutual reasonable endeavors to resolve the issue at hand and Merchant acknowledges that any termination shall be used as a last resort only.

7.3. Printful hereby confirms that its sub-processors are contractually or otherwise in a binding form required to comply with data Processing obligations which are no less onerous on the relevant sub-processor than the obligations on Printful as prescribed by these Terms.

7.4. The Merchant acknowledges and agrees Printful may appoint an Affiliate or third party subcontractor to Process the Merchant's Personal Data in a Third Country, in which case Printful shall execute the Processor to Processor Clauses, if applicable and available, with any relevant subcontractor (including Affiliates) it appoints on behalf of the Merchant.

7.5. Where Printful Processes Personal Data in any Third Country and is acting as a Data Importer, Printful shall comply with the Data Importer's obligations set out in the Controller to Processor Clauses, which are hereby by reference incorporated into and form part of these Terms. The Merchant shall comply with the Data Exporter's obligations in such Controller to Processor Clauses:

1. for the purposes of Annex I of the Controller to Processor Clauses, the Parties agree that the Processing details set out in Clause 3 shall apply.
2. for the purposes of Annex II of such Controller to Processor Clauses, the technical and organizational security measures set out in Schedule 1 (Technical and Organization Security Measures) shall apply; and
3. for the purposes of: (i) Clause 9 of such Controller to Processor Clauses, Option 2 ("General written authorization") is deemed to be selected and the notice period specified in 7B shall apply; (ii) Clause 11(a) of such Controller to Processor Clauses, the optional wording in relation to independent dispute resolution is deemed to be omitted; (iii) Clause 13 and Annex I.C, the

competent Supervisory Authority shall be the location of the Data Exporter (iv) Clause 17, Option 1 is deemed to be selected and the governing law shall be Latvia unless otherwise expressly agreed between the Parties; (v) Clause 18, the competent courts shall be Latvia unless otherwise expressly agreed between the Parties.

8. Audit

8.1. Upon the Merchant's written request, Printful shall provide sufficient information to demonstrate compliance with the obligations laid down in these Terms and Data Protection Laws. This information shall be provided to the extent that such information is within Printful's control and Printful is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

8.2. If the information provided upon the Merchant's request in the Merchant's reasonable judgment is not sufficient to confirm Printful's compliance with these Terms, then Printful agrees to undergo data Processing audits.

8.3. Such audits are allowed to be carried out by an independent third party with good market reputation, provided that it has sufficient experience and competence to carry out data Processing audits, and election of such auditor must be mutually agreed by both the Merchant and Printful.

8.4. The timing and other practicalities related to any such audit or inspection are determined by Printful, and any such audits are provided only at the expense of the Merchant. Printful reserves the right to charge the Merchant for any additional work or other costs incurred in connection with such audits. The Merchant may request an audit no more than once every 2 years.

8.5. The Merchant and independent third party will have to sign a confidentiality agreement, which includes an obligation not to disclose business information in its audit report, and the final report will also have to be provided to Printful.

9. Return and deletion of Data

Subject to applicable legal retention obligations, upon termination of the Agreement and Merchant's use of the Services, Printful will return or delete any Personal Data without keeping a copy, in accordance with the procedures and timeframes applied by Printful from time to time, and if requested, confirm such deletion to Merchant in writing. Notwithstanding the foregoing, Printful is permitted to aggregate, de-identify, or anonymize personal information so that it no longer meets the definition of Personal Data under applicable Data Protection Laws, and may use such aggregated, de-identified, or anonymized data for its own research and development purposes. Printful will not attempt to or actually re-identify any previously aggregated, de-identified, or anonymized data without the specific written instructions of the Merchant.

10. Governing Law

These Terms shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement unless required otherwise by applicable Data Protection Law.

11. Modifications

Printful reserves the right, at its discretion, to modify these Terms. In case of material changes, Printful will notify the Merchant in writing.

Schedule 1
Technical and Organizational Security Measures

Printful shall take, among others, the following technical and organizational measures to ensure the physical security of Personal Data and control system entry, access, transfer, input, availability and separation of Personal Data:

1. Measures of pseudonymisation and encryption of Personal Data

1.1 All Personal data must be encrypted during transit and at rest.

1.2 At rest Personal data must be encrypted using industry-leading versions of AES, RSA, or equivalent encryption algorithms.

1.3 Personal data at transit must be encrypted using industry-leading versions of TLS 1.2+, FTPS, SFTP, and other leading data encryption algorithms for transmitting Personal data.

1.4 To the extent possible, all Personal data should be pseudonymised no more than 180 days after the moment Personal data has been received.

1.5 All Personal data must be deleted or returned after this agreement has been terminated, after submitting a written request. This provision shall not apply to Personal Data that the Printful is required to retain to comply with applicable legal requirements. Printful will in such a case block the Personal Data for further use, ensure the secured storing of such Personal Data including appropriate access controls, and not use such Personal Data for any other purpose than such compliance purposes.

1. 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

2.1 Systems processing Personal data must have a working disaster recovery plan and incident response plan in case of any incidents.

1. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

3.1 Systems storing or modifying Personal data must be regularly (no less than annually) tested for vulnerabilities and other system weaknesses that can adversely affect confidentiality, integrity and/or availability of the Personal data ideally by a third party, but can also be performed by an in-house certified ethical hacker according to OWASP, OSINT or other testing/ auditing frameworks.

3.2 All identified vulnerabilities must be recorded and remediation steps planned according to the vulnerability severity and possible impact.

3.3 After submitting a written request, the Personal Data Importer must provide the Personal Data Exporter with the most recent security testing report.

1. Measures for user identification and authorization

4.1 Access to Personal data must be strictly controlled and rights must be granted based on a “Need to know'' principle, with each user activity that can impact confidentiality, integrity and/or availability strictly monitored. Each such user must use secure authentication practices in order to restrict access. Authentication must include the username, and password that meets the newest NIST 800-63B password guidelines and also contains a secure token or MFA element.

4.2 If Personal data is being accessed remotely (through the internet) then VPN (IPSec tunnel) must be used at all times.

1. Measures for ensuring the physical security of locations at which Personal data are processed

5.1 All Personal data must be stored in a cloud service provider that has a valid ISO27001 certificate or in the case of a private data center, rooms must be physically protected by all of the best practices for physical security e.g. Separate server room, 24/7/365 physical guards at the location and video surveillance, each access to the server room must be strictly logged in order to ensure that Personal data cannot be physically tampered with.

1. Measures for ensuring events logging

6.1 All Personal data-related activities that can impact confidentiality, integrity, and/or availability must be strictly logged. Event logs must be periodically analyzed to monitor any confidentiality, integrity, and/or availability-impacting activity. Event logs themselves must be protected from unauthorized changes.

1. Measures for ensuring system configuration, including the default configuration

7.1 All infrastructure processing Personal data in any way must have a system configuration that has been hardened from a security perspective (all nonessential services disabled/uninstalled). These configurations must be managed in a way that will restrict any unauthorized changes to configurations without a proper approval process and strict logging of every configuration change.

1. Measures for internal IT and IT security governance and management

8.1 Personal Data Importers must have the following documents in place (or other policies that contain controls from these documents): IT security policy, Acceptable use policy, Data classification policy, Disaster recovery plan, Incident response plan, User access policy, Remote access policy, IT risk assessment, and Third-party security policy.

8.2 All IT policies, procedures, and plans that impact the processing of any Personal data must be reviewed at least annually or just after an IT incident.

1. Measures for ensuring data minimization

9.1 Personal data processing must fall under these principles:

(a) adequate – sufficient to properly fulfill the stated purpose;

(b) relevant – has a rational link to that purpose;

(c) and limited to what is necessary – more than what is needed for the purpose is held.

1. Measures for ensuring accountability

10.1 Data protection policies must be adopted and implemented describing Personal data processing activities.

10.2 Data Importers must have a dedicated data protection officer appointed to oversee Personal data processing, carry out data protection impact assessments for Personal data, and report Personal data breaches to appropriate institutions and Data Exporters.

10.3 Data Importers must adopt and maintain written contracts with organizations that process Personal data on the Data Importer's behalf.

1. Measures for allowing data portability and ensuring erasure

11.1 All Personal data must be stored in such a way that all Personal data must be aggregated into a structured and machine-readable format. If a request for data portability is approved, then Personal data could be sent outside of the data processor network to the next data processor. In this case, Personal data must be encrypted using industry-leading versions of AES, RSA, or equivalent encryption algorithms for encryption and transmission must be done using an IPSEC tunnel (VPN).

1. Measures for sub-processors (where applicable)

12.1 All involved sub-processors must comply with all the same measures as described for Data Importers.

Part 3: List of Sub-Processors