Data Privacy Statement of the ThinPrint Cloud Services Inc.

Preamble

This Data Privacy Statement applies to all products, services and websites distributed by ThinPrint Cloud Services Inc., 7600 Grandview Ave, Suite 200, Arvada, CO 80002, USA (hereinafter referred to as „TPCS“). Assuring the privacy of our users and the confidentiality and integrity of their information is of elemental importance to us at ThinPrint Cloud Services. Therefore, we agree on restricting our actions where technical restrictions are not yet implemented or not feasible as follows:

- We will not access the content of documents and print jobs without the explicit consent of the user who submitted them into the ThinPrint Cloud.
- We will not assemble information about a specific user's interaction with the ThinPrint Cloud unless required for troubleshooting or performance analytics to improve the platform.
- We will only access personally identifiable information when it is necessary to do our job and no alternative is practically available.
- TPCS adheres to the EU General Data Protection Regulation (GDPR)

Data collected by the TPCS website and cloud services

User data

The TPCS websites (e. g. www.thinprintcloud.com, cloudprinter.thinprint.com, www.ezeep.com, dash.ezeep.com and www.cloud-printing-alliance.com) contain a number of forms in which you must provide personal information if you use the corresponding services. In particular, this concerns registration, contact, offer, download and support forms as well as newsletter subscriptions. The data to be provided may include: first and last name, company name and address, position, phone number and e-mail address. We may use your e-mail address for purposes of direct marketing (information on products, newsletters, etc.). If you purchase services that are subject to a fee, you also must provide payment information. For this purpose, TPCS stores incoming invoice data.

In general, any and all information that allows us to individually identify people, are considered personal information. We always receive and transmit any and all personal data by way of encryption. If you purchase services that are subject to a fee, payments which refer to one of our cloud services, e.g. ezeep, are handled by Cortado Holding AG (Alt-Moabit 91 b, 10559 Berlin, Germany).

When using our cloud services, you use your e-mail address for registration. This is displayed in the apps for displaying the login status of the users.

Usage data

On your visit to a TPCS website, we send cookies, e.g. small electronic files consisting of a certain character string allowing us to identify your browser. Additional cookies are used for caching your credentials and user preferences. All TPCS cookies are recognizable by the string **thinprintcloud.com**, **ezeep.com** or **cloudprinter.thinprint.com**, which can be found in the name of the cookie. However, you have the option to set your browser to refuse cookies or to ask you every time a cookie is sent. If you only block cookies from so-called third-party providers, you can use all functions of the TPCS websites and cloud services unrestrictedly. You can easily find out how to change the cookie settings of your web browser using its help function.

Furthermore, TPCS servers automatically record usage data that your browser sends when you visit a website or that logs your use of *ezeep*, *ezeep Dash* or *ThinPrint Cloud Printer*. These so-called log data include your web request, IP address,

browser type, browser language, date and time of a request and cookies. These **log data** allow to clearly distinguish your browser from other browsers. If required, log data is used by TPCS only for purposes of evidence, customer support, error detection as well as for identifying and repelling hacker attacks. These data will be automatically deleted after 30 days.

Third parties

TPCS uses the following third parties for analytical purposes and/or to place their own interest-based ads on the web sites of these third-party providers Google LLC., 1600 Amphitheatre Parkway Mountain View, CA 94043, USA (for analytics + ads) and Mixpanel Inc. 405 Howard Street, Floor 2, San Francisco, CA 94105, USA (for analytics)

All data collected this way is anonymous for TPCS (usage data); in other words, TPCS does not see the individual user's personal data (user data).

However, these usage data may be stored and processed by the respective third party. If you also log-in to your relevant third-party account using the same web browser, the pertinent third-party provider could connect your usage data with your local account – thus your user data – and use for their own promotional purposes. To prevent that from happening, you can either block the third-party cookies via browser settings or use two different web browsers on the same device – one for logging in to your TPCS account and another one for logging in to the third-party provider account.

TPCS only uses the collected personal data as indicated for the purposes they were actually intended for. Apart from that, the purposes include the provision of TPCS' services and products for users and the development of new services and products.

To analyze the activities on its websites, TPCS uses the functions of Google Analytics. To ensure anonymization of IP addresses, Google provides an extension to the Google Analytics Code. Integrating the code extension "anonymizeIp". By using the code extension, the last 8 bit of the IP address will be deleted and therefore anonymized. This only permits a rough localization. TPCS anonymizes any and all IP addresses before their transmission to Google via Javascript with the code line "ga('set', 'anonymizeIp', true);" or "_gaq.push (['_gat._anonymizeIp']);" in your browser (see https://support.google.com/analytics/answer/2763052?hl=de). Another effective way to disable analytics and statistics features is the current Firefox browser with its tracking protection option; to use this, select *Options→ Privacy & Security→ Tracking Protection→ Always*.

Your approval for the collection of personal data / Revocation

If you register for a specific service on the TPCS websites – for example *ezeep Dash* or *ThinPrint Cloud Printer* –, we ask for your personal data (see above). If such data shall be used for a purpose other than originally indicated, we request your consent for us doing so. However, you may refuse to give your prior consent. Without your express prior consent, TPCS will not use your personal information for other purposes than indicated and in connection with the respective services or products.

You are at all times entitled to refuse to provide personal information or to revoke provided personal data. Please be aware though that in such case TPCS might not be able to offer you all available services. If you terminate your account or if you revoke personal data, which is required for processing valid contractual relations between you and TPCS, we will delete any personal data promptly after termination of the contractual relations.

EU-General Data Protection Regulation (GDPR)

Transfer of personal information to third parties for billing, invoicing or communication services are performed within the GDPR framework.

Without your consent, TPCS will only transfer or disclose your personal data upon presentation of a search warrant, judicial order, judicial decree or another form of lawful cases regulated by law. In such cases, the legal basis lies in the *compliance with a legal obligation* (Art. 6 para. 1 (c) GDPR).

In all other cases the legal basis for consumer accounts lies in the *performance of a contract* (Art. 6 para. 1 (b) GDPR) and for business accounts in the *purposes of legitimate interests* pursued by TPCS (Article 6 para. 1 (f) + Recital 47 GDPR).

Data security

TPCS uses adequate security measures to prevent unauthorized access or change, transfer or deletion of personal information. Such measures include, but are not limited to, internal review of our data collection practices, data storage and processing as well as technical and organizational security measures to prevent access to the systems we use to store such sensitive data.

Access to such data is internally limited to such members of staff who for the operation, development, and improvement of TPCS services and products require knowledge of such data. Such members of staff are required to adhere to special confidentiality requirements. If such members of staff, however, breach the secrecy requirements, they have to face consequences under labor law and/or criminal prosecution.

EU-US and Swiss-US Privacy Shield

TPCS complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. TPCS has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/ .

To provide you with our services, we provide personal information to third parties to perform services on our behalf. This applies in particular to: establishing and maintaining contact, invoicing and receiving payment for services provided, statistical evaluation of service (anonymized data set) and incidental review of service to improve service or troubleshooting. This applies to the following data categories:

- Contact information:
  gender, name, e-mail address, phone number, website, job title, name of organization the individual is associated with in regard to using our service, mailing address
- Activity information:
  print history, activity logs
- Payment information:
  invoices, payment preferences, payment history, payment information (through third party processors)

If we transfer personal information received under the Privacy Shield to a third party, the third party's access, use, and disclosure of the personal data must also be in compliance with our Privacy Shield obligations, and we will remain liable

under the Privacy Shield for any failure to do so by the third party unless we prove that we are not responsible for the event giving rise to the claim.

TPCS has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regards to unresolved Privacy Shield complaints concerning data transferred from the EU and Switzerland. TPCS is subject to the investigatory and enforcement powers of the US Federal Trade Commission (FTC).

In certain circumstances, the Privacy Shield Framework provides the right to invoke binding arbitration to resolve complaints not resolved by other means, as described in Annex I to the Privacy Shield Principles. Furthermore, we may be required to disclose personal information handled by us under the Privacy Shield in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Enforcement

TPCS regularly checks compliance with this Data Privacy Statement. If you have any questions, comments, requests for information, rectification, processing restrictions, portability or erasure of data, please feel free to contact us (see below). **You have the right to object to the processing of your personal data or to revoke your consent at any time.** In addition, you have the right to complain to the relevant recourse authority (see above).

Offer to conclude a Data Protection Agreement

In your capacity as a business customer within the European Economic Area, on your instructions and within the framework of the service provision personal data is collected, processed and/or used by TPCS. According to Art. 28 of the GDPR the contracting authority - .e.g. you - is responsible for complying with the data protection rules. You can fulfill this obligation by concluding a Data Protection Agreement with TPCS, which meets the legal requirements of the GDPR. Upon request TPCS will be happy to provide you with a draft of a Data Protection Agreement along with a Data Processing Addendum describing our technical and organizational security measures to protect personal data. Once provided to you, you only have to check and sign these documents. If you have any concerns, inquiries or if you need further information or assistance, we are happy to assist you.

Alterations and amendments

Please note that this Data Privacy Statement may be altered and/or amended from time to time. Without your express consent, though, TPCS will not restrain your rights under the current Data Privacy Statement. Amendments and/or alterations concerning the Data Privacy Statement will be announced by TPCS on the websites. Earlier versions of the Data Privacy Statement will be filed and will be available for reference upon your request.

Contact

Contact information for complaints and inquiries as well as for requests for information, rectification, processing restrictions, portability or erasure of personal data:

Mail:

ThinPrint Cloud Services, Inc.
7600 Grandview Ave, Suite 200
Arvada, Colorado, 80002
USA

E-mail:
privacy@thinprintcloud.com

Representative in the European Union according to Art. 27 of the GDPR:
ThinPrint GmbH
Alt-Moabit 91a
10559 Berlin
Germany
E-mail:
dataprotection@thinprint.com

Denver, November 2018