EveryonePrint
Data Privacy Notice

This EveryonePrint Data Privacy Notice ("Data Privacy Notice") covers our collection, use, and disclosure of the Customer Data (as defined below) by the EveryonePrint products and services (together the "Services"), such as through **EveryonePrint Chrome Extension**, the **EveryonePrint PC Client** and the **EveryonePrint Mobile Print app for iOS or Android**, that are licensed and used by EveryonePrint's customers and their users (collectively, "you," "your," or "customer"). For purposes of this Services Privacy Notice, "Personal Data" means any information relating to an identified or identifiable individual, including, for example, 'personal information' as defined under European GDPR Regulation (EC) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of 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), name, phone number, postal code or zip code, Device ID, User ID, IP address and email address.

1. WHO WE ARE

EveryonePrint A/S is a Danish corporation headquartered at Gladsaxevej 384D, 2860 Soeborg, Denmark incorporated in the Kingdom of Denmark with corporate registration no 27637167. For more information about EveryonePrint, please see the "About Us"section of our Site.

2. WHAT WE DO AND THIS DOCUMENT

The EveryonePrint Hybrid Cloud Platform (HCP) is a Subscription Based Enterprise Print Management solution, provided and installed either as a Cloud-Based, Private-Hosted or On-premise solution.

HCP enables an entire organization to utilize all print devices, process print jobs from any device stationary, laptop, tablet, or mobile. HCP is a powerful and easy to manage solution which highly cost-effective replaces traditional Print Management solutions.

Customer Data is subject to the restrictions set forth in the documentation and the underlying agreement between EveryonePrint and its customers ("EULA Agreement").

This document covers security and safety aspects relationship to the usage of the HCP solution, including issues related to regulation and compliance. As with any other Software as a Service (SaaS) solution, there is no single layer that protects customer data, but rather a well-architected solution that considers every layer from the physical security measures at the data center, all the way through the access privileges that determine what data an individual user can access.

3. DATA AND USAGE

The HCP solution transfer Customer Data between clients, servers, and print devices. During a temporary term, Customer Data is stored at the HCP server.

3.1 Data Processing

HCP will process data as described under *Type of data*. EOP will not access or use Customer Data, except as necessary to provide the Service Offerings initiated by Customer.

3.2 Type of data

The HCP solution contains three (3) types of data, as described below:

Application Configuration Data
Application configuration data contains the customer specific configuration of the installed solution. Data within this category is not classified as Customer Data and is not in violation with the ***General Data Protection Regulation - GDPR*** (EU)2016/679.

Print Job Metadata
Print Job Metadata contains information regarding print jobs, which are job specific information. Data within this category may be classified as Customer Data which may be covered by the ***General Data Protection Regulation - GDPR*** (EU)2016/679.

Document Content
Document content is the actual document content that any given end-user is processing through the HCP solution. This type of Customer Data may contain data which is covered by the ***General Data Protection Regulation - GDPR*** (EU)2016/679

3.3 Disclosure

EOP will not disclose Customer Data to any government, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends EOP a demand for Customer Data, EOP will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, EOP may provide Customer's basic contact information to the law enforcement agency. If compelled to disclosure Customer Data to a law enforcement agency, then EOP will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless EOP is legally prohibited from doing so.

3.4 EOP Personnel data access

EOP restrict its personnel from accessing Customer Data without authorization by EOP Management and without a reasonable cause. EOP have established appropriate contractual obligations upon its personnel, regarding confidentiality, data protection and data security.

4. COMPLIANCE AND REGULATIONS

At EveryonePrint, our ambition is to follow industry leading compliance and regulations standards. Since the provided SaaS solution process customer data, including potential sensitive and critical customer data, compliance and regulation is critical to become accepted by our worldwide partners and end-customers. With the introduction of the General Data Protection Regulation by the European Union, a new standard has been established, which currently sets the highest ambition level among all other compliance and regulation policies worldwide. By following the GDPR (EU)2016/679 standard, the HCP solution will meet most of the worldwide requirements found within similar compliance and regulation standards. For more information about HCP and GDPR, please see our GDPR-Whitepaper.

4.1 General Data Protection Regulation - GDPR (EU)2016/679

Prior to establishing the initial HCP account setup, end-customers may determine whether the need for GDPR compliance is needed (location of servers within the EU). The following describes the policies used by EOP to ensure a default configuration, which offers best possible performance for a wide range of our end-customers.

For Customers within the EU

Unless otherwise agreed between EOP and the Customer prior to account setup, all processing and storage of Customer Data within the HCP solution will be handled according to and in compliance with the EU regulation (EU)2016/679 with the HCP solution hosted at servers within the EU. Customer can request to have its Hosting Provider location moved to a location outside the EU, by signing the "HCP (EU)2016/679 Waiver or Option Agreement" provided by EOP upon request.

For Non-EU Customers

For Non-EU Customer's the HCP Hosting Provider location will as default be within Customers local geographical region (U.S or Asia).
Non-EU Customer who works within the EU or in any way managing Customer Data which involves EU residents, the HCP solution can prior to the initial account setup be requested to become compliance with the GDPR (EU)2016/679 regulation. This requires the Customer to enter the "HCP (EU)2016/679 Waiver or Option Agreement" provided by EOP upon request.

Relocation of established account setup

The HCP solution can be relocated on request by end-customer. However, movement of an already in-production environment is associated with consultancy charges and fees, corresponding to the working hours needed to execute the relocation.

Safety & Security Practices

To ensure GDPR compliance, EOP maintains a number of internal procedures governed by the Data Protection Officer, including:

- Management of events involving Customer Data
- Access logging
- Reviewing safety & security practices

5. INFRASTRUCTURE

All data as defined under Section ***Definition of data and usage*****,** will be managed within the HCP solution and temporarily stored within the Hosting Provider in use.

5.1 Hosting Provider compliance

The HCP solution is unless otherwise agreed, installed at a Hosting Provider that comply and are certified under key industry standards, such as ISO/IEC 27001:2005. Furthermore, all servers and network environment have the SSAE 16/ISAE 3402 attestation. In addition, the server platform complies with HIPAA Business Associate Agreement (BAA),

a United States law which applies to healthcare entities with access to patient information (called Protected Health Information, or "PHI").

5.2 Data Storage

Data Storage within the HCP solution will as default be managed through a Hosting Provider within Customers local geographical region (EU, U.S or Asia).

Customer may optionally specify any other geographic region(s) of the Hosting Provider in which Customer Data will be stored. At present, the available major regions are Europe (EU), Asia, and the United States. For compliance reasons please also refer to Section ***Compliance and regulations***.

Customer may decide to allocate local storage for temporary **Document Content**. The usage of local storage will either reduce the amount of external data traffic or complement the HCP solution with a failover option in case of connectivity problems between Customer and Hosting Provider.
Typically, *Application Configuration Data* and *Print Job Metadata* is stored in the cloud, either hosted or on premise, while *Document Content* is stored locally within the customer network.

5.3 Data Redundancy

HCP's hosting provider may transfer Customer Data within a major geographic region (e.g., within Europe, U.S. or Asia) for data redundancy or other purposes.
HCP's hosting provider will not transfer Customer Data outside the major geographic region(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia).

5.4 Data Retention

Document Content will only temporarily be stored until each job has been completed successfully or expired. Customer can enter into an optional "Document Content Storage Agreement", should it be required by the Customer to retain Document Content for a longer period of time. However, when entering into such agreement, the Customer will be solely responsible for any compliance issues this change of storage policy may cause. *Print Job Metadata will* only temporarily be stored for debugging and reporting purposes. By default, a print job will expire after 32 hours. This retention period can be changed by the administrator.

5.5 Data Disposal

When *Document Content* has been erased within the HCP solution, it will no longer be recoverable from within the application.

5.6 Backup and Recovery

Within the server side of the HCP solution, backup and recovery processes have been established to ensure high availability and a fault tolerant platform with zero point of failure. The HCP operations team have established monitoring tools and procedures which ensures full transparency and surveillance of the platforms operational status. In case of platform or software regression issues, a full disaster recovery procedure is established to ensure

minimal platform down-time. Real-time information on system performance and interruptions is available at https://status.everyoneprint.com

5.7 Application Configuration and Customization

The HCP solution can be customized and configured to support Customer chosen structures, which will allow Customer to meet Customer specific compliance and regulation policies.
This includes configuration of specific and/or multiple locations for Data Storage and Data Processing. Furthermore, the Data Storage can be separated into Customer-specific structures, which will ensure Customer Data are processed separately, if needed.

5.8 Transfer and communication of data within regions

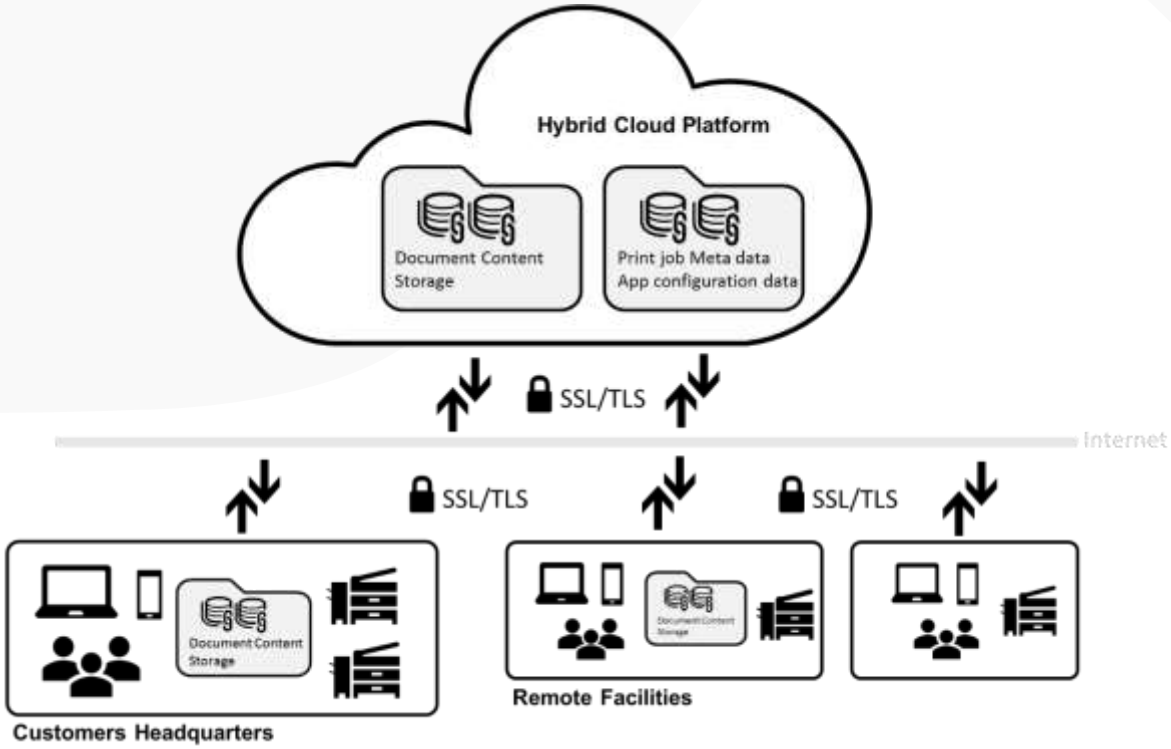
Customer may specify the HCP region(s) where Customer Data will be processed within the HCP solution, including the EU, U.S. or ASIA Region (each a "Region"). Once Customer has made its choice, EOP will not transfer Customer Data from Customer's selected Region(s) except as necessary to comply with the law or a valid and binding order of a law enforcement agency, such as a subpoena or court order. See section ***COMPLIANCE AND REGULATIONS*** for more information about regional default policies.

6. APPLICATION SAFETY

6.1 Application resilience

Upon each release of new developments and application improvements, EOP validates the HCP solutions vulnerability. These assessments have been deployed for vulnerability, configuration and compliance assessments and is based on widely known industry technologies, which helps prevent network attacks that can cause unwanted persons to penetrate the solution and its Customer Data. This validation includes all elements of the HCP solution from server applications, client applications and drivers to Mobile device applications. During development of the HCP solution, "Privacy by Design" is a foundation of the architecture and design of the solution.

To protect data between Customers and the HCP Hosting Provider, all data is transferred using Secure Sockets Layer (SSL)/Transport Layer Security (TLS), creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. All data in transit always encrypted via SSL/TLS.



6.2 Safety & Security by Design

EOP develops the HCP solution with intent to maximize safety & security, including availability of data, access management, and resilience to risk of breaches. EOP adheres to the best practices in the industry for development and testing principles, complemented by external security evaluation.

5. COMMUNICATIONS AND NOTIFICATIONS TO CUSTOMERS AND USERS

5.1 Legal Requirements

EveryonePrint may access Customer Data and Personal Data contained in Systems Operations Data as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect or defend our rights or property of EveryonePrint or users of the Services, protect the safety of others, to investigate fraud, or respond to government requests, including public and government authorities outside a user's country of residence, for national security and/or law enforcement purposes.

Changes to this Data Privacy Notice. This Data Privacy Notice is subject to occasional revision, and if we make any substantial changes in the way we use Personal Data, we will take appropriate measures to inform our customers, consistent with the significance of the changes we make. We will obtain consent to any material Data Privacy Notice changes if and where this is required by applicable data protection laws.

The date of the most recent update to this Data Privacy Notice can be found by checking the “last updated” date displayed at the top of this Services Privacy Notice.

5.2 How to Contact Us

If you have questions about how your Personal Data is collected, stored, shared, used, or to exercise any data or data rights please contact our Data Protection Officer (“DPO”) as follows. Email inquiries may be addressed to: compliance@everyoneprint.com.

Written inquiries may be addressed to:

EveryonePrint A/S
Attn: Legal
Gladsaxevej 384D
2860 Soeborg
Denmark