EveryonePrint HCP Data Guidelines

1.1 General Definitions

"**HCP**" shall mean, EveryonePrint Hybrid Cloud Platform, the solution provided, covered by this document.

"**EOP**" shall mean, EveryonePrint A/S, the company owning, developing, and issuer of "Right-to-use/Licenses" of the HCP solution.

"Customer" shall mean a corporate customer of the partner/reseller with whom this document is shared.

"**Customer Data**" shall mean the "personal data" that is processed through to the usage of the HCP solution by the customer.

"**Hosting Provider**" shall mean the datacentre that EOP utilize for its HCP solution.

"**Document Content Storage** Agreement" shall mean an optional add-on agreement for customers wishing to store Document Content beyond the standard default policy.

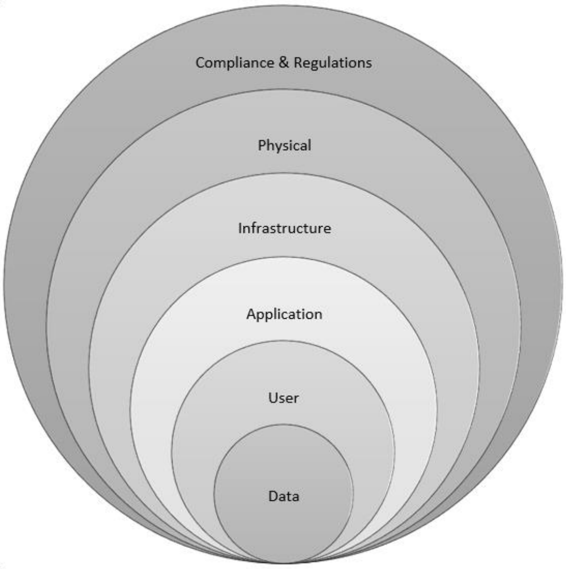
1.2 EveryonePrint Hybrid Cloud Platform

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.

1.3 Purpose of this document

This document covers security and safety aspects in 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.



Contents

1.4 Type of data

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

1.4.1.1 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.

1.4.1.2 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.
Data collected includes -***Document Name, Document type, Driver Setting details, Created Time and Username***

1.4.1.3 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

1.5 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.

1.6 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.

1.7 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.

1.8 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.

1.8.1.1 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.

1.8.1.2 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.

1.8.1.3 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.

1.8.1.4 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

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.

1.9 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").

1.10 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 fall- over option in case of connectivity problems between Customer and Hosting Provider.

1.11 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).

1.12 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 until each job has been completed successfully or expired, after which it is pseudonymized and logged for debugging and reporting purposes.

By default, a print job will expire after 32 hours. This retention period can be changed by the administrator.

1.13 Data Disposal

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

When the customer decides to leave the product a data sanity will be conducted based on the agreement with the customer.

1.14 Version History

June 2019 -Version 1.0

Note - This document does not create any warranties, representations, contractual commitments, conditions from EveryonePrint, its affiliates, suppliers or licensors. The responsibilities and liabilities of EveryonePrint to its customers are controlled by contractual agreements, and this document is not part of, nor does it modify, any agreement between EveryonePrint and its partners or customers.