INCONTEXT PRIVACY POLICY

Author:	**Michel Wery**
Date of last change:	**26-06-2019**
Data protection officer:	**Name:** Michel Wery **Function:** Finance Manager **e-mail:** privacyofficer@incontext.nl **Tel nr.:** +31 35 628 68 48

1. Introduction

This privacy policy sets out the organizational and technical measures taken to protect the (personal) data of our clients, employees and all other parties with whom we co-operate.

This privacy policy has three parts:
- The Security Plan
- The Continuity Plan
- The Exit Plan

In addition, InContext has drawn up a Privacy Statement which you can find on our website. In this Privacy Statement we have described, among other things:
- Which groups InContext processes personal data for.
- Which personal data is processed.
- For what purposes and on what legal basis.
- A list of sub-processors with whom we have agreements.
- Our cookie policy.
- Retention periods.

2. The Security Plan

Technical and organizational measures taken by InContext to protect personal data and to keep it protected against loss, unauthorized access, mutilation or unlawful processing, as well as guaranteeing the (timely) availability of the data.

a.) measures to ensure that only authorized personnel have access to the Personal Data for the purposes described.

Registered accounts
InContext gives its employees and sub-processors access via registered accounts in combination with a personal password. Access rights are granted to these accounts based on the function group to which the employee belongs. The use of these accounts is adequately logged and these accounts only give access to personal data required by the relevant person as needed.

Password policy
The password must meet the following criteria:
- At least 7 characters long
- Expires every 3 months
- Must be a combination of uppercase letters, lowercase letters and numbers or symbols

Personal data (participant data) provided by clients
The InContext Project desk is the only department to receive participant data from our clients. They are responsible for correctly applying the privacy agreements / legislation to this data.

- Participant data is stored by the Project Desk department in a protected participant folder.
- Participant lists are not shared via e-mail with facilitators. Any communication with the participants after a training session is done via the Project Desk department.
- Facilitators are responsible for returning papers* with personal data used in an intervention.
- The Project desk department destroys participant data, both digital and hard copy.

**papers include: attendance lists / list of participants, Facet5 and TeamScape reports, (copies) certificates*

b.) measures regarding data storage and security of devices

Physical measures to secure the property
InContext's premises are secured with access keys and an alarm. Employees have access via a key and an individually identifiable tag in order to switch security on and off.

Server room
InContext has a secured server room and only specifically authorized staff members and Card Services have the access key.

Data storage
The data is stored exclusively in Dutch data centers.

Office 365 (Outlook)
- Exchange Online: divided among centers within Europe: the Netherlands, Finland, Ireland and Austria.
- Azure Active Directory (for synchronization of computer and mail passwords): The Netherlands, Ireland and the United States but is subject to European legislation.

Device Encryption
Control based on Sophos:
- For Mac OS, FileVault2 is activated, the entire hard disk is encrypted and cannot be released without recovery key or password from the user.
- For Windows, Bitlocker is activated, the entire hard disk is encrypted and can only be released with the automatically generated recovery key. This changes with every new request to unlock.

Alienation / data leak / loss of devices
Employees are obliged to report alienation, a (potential) data leak and / or loss directly to the appointed privacy officer.

Devices are erased remotely when they are lost or stolen:
- JAMF: via the MDM system, all MacBooks can be locked and deleted remotely. The prerequisite for this is that the device has an internet connection.
- SecureFileSync: via the management portal, InContext can remotely withdraw the data from the device. We can also do this with the servers. The same condition applies, that the device is connected to the internet.

3. The Continuity Plan

a.) measures to ensure the timely availability of Personal Data.

Obligation for employees to use centralized storage
InContext obliges its employees to store documents on the server in the designated customer folders and participant folders. This ensures that the continuity of the projects is secured and not dependent on individuals.

Backup server
InContext uses an external backup server in the cloud. A copy of the server is made every night. This ensures data in the event of a server interruption / crash.

4. The Exit Plan

The exit plan sets out how the personal data we process on behalf of our clients is removed at the moment the relationship is ended.

Transferability to the client
InContext obliges its employees to store documents on the server in the designated customer folders and participant folders. If a client submits a request to transfer their personal data, InContext is able to do this without delay.

Destruction operations and their reporting
Participant lists are not saved for longer than 4 weeks after completion of an implementation / intervention.
- Physical participant lists are destroyed via a sealed paper container that is emptied by a party specialized in it.
- Digital participant lists are removed from the server by the Project Desk department.
- Any e-mail contact between our facilitators and participants will be deleted annually before the end of the year. We also require our employees / freelancers to confirm the removal to us in writing.