INCONTEXT PRIVACY BELEID

Auteur:	**Michel Wery**
Datum laatste wijziging:	**11-01-2019**
Functionaris gegevensbescherming:	**Naam:** Michel Wery **Functie:** Finance Manager **e-mail:** privacyofficer@incontext.nl **Tel nr.:** +31 35 628 68 48

1. Introductie

Dit privacy beleid beschrijft de organisatorische en technische maatregelen die zijn genomen om (persoons)gegevens van onze opdrachtgevers, medewerkers en alle overige partijen waarmee wij samenwerken te beschermen.

Onderdelen van dit privacy beleid zijn:
- Beveiligingsplan
- Continuïteitsplan
- Exit plan

Hiernaast heeft InContext een Privacy statement opgesteld welke u kunt vinden op onze website. In dit Privacy statement hebben wij onder andere beschreven:
- Voor welke groepen InContext persoonsgegevens verwerkt.
- Welke persoonsgegevens worden verwerkt.
- Voor welke doeleinden en op welke wettelijke grondslag.
- Een lijst met sub-verwerkers waarmee wij overeenkomsten hebben gesloten.
- Ons cookiebeleid.
- Bewaartermijnen.

2. Beveiligingsplan

Technische en organisatorische maatregelen die InContext heeft genomen om persoonsgegevens te beveiligen en beveiligd te houden tegen verlies, onbevoegde kennisname, verminking of onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid van de gegevens te garanderen.

a.) maatregelen om te waarborgen dat alleen bevoegd personeel toegang heeft tot de Persoonsgegevens voor de doeleinden die zijn beschreven.

Op naam gestelde accounts
InContext geeft haar medewerkers en sub-verwerkers toegang via op naam gestelde accounts in combinatie met een persoonlijk wachtwoord. Aan deze accounts worden toegangsrechten verleend op basis van functiegroep waartoe de medewerker behoord. Het gebruik van deze accounts wordt adequaat gelogd en waarbij die accounts alleen toegang geven tot die persoonsgegevens waartoe de toegang voor de betreffende persoon noodzakelijk is.

Wachtwoord beleid
Het wachtwoord dient te voldoen aan de volgende criteria:
- Minimaal 7 tekens lang
- Verloopt elke 3 maanden.
- Moet een combinatie zijn van hoofdletter, kleine letter en cijfer of vreemd teken

Persoonsgegevens (deelnemersdata) verstrekt door opdrachtgevers
Uitsluitend de InContext afdeling Projectdesk ontvangt deelnemersgegevens van onze opdrachtgevers. Zij zijn verantwoordelijk voor het juist toepassen van de privacy afspraken/wetgeving op deze gegevens.

- Deelnemersgegevens worden door de afdeling Projectdesk opgeslagen op een afgeschermde deelnemersmap.
- Deelnemerslijsten wordt niet gedeeld via e-mail met facilitators. Eventuele communicatie met de deelnemers na afloop van een training verloopt via de afdeling Projectdesk.
- Facilitators zijn verantwoordelijk voor retourneren van papieren* met persoonsgegevens die gebruikt zijn bij een interventie.
- De afdeling Projectdesk vernietigt deelnemersgegevens, zowel digitaal als hard copy.

**met papieren wordt bedoeld: presentielijst/deelnemerslijst, Facet5 en TeamScape rapport, (kopie) certificaat*

b.) maatregelen ten aanzien van data opslag en beveiliging van devices

Fysieke beveiligingsmaatregelen van het pand
InContext heeft haar pand beveiligd met toegangssleutel en alarm. Medewerkers hebben toegang via een sleutel en een individueel identificeerbare tag om de beveiliging in- en uit te kunnen schakelen.

Serverruimte
InContext heeft haar serverruimte afgesloten en alleen specifiek daartoe geautoriseerde personeelsleden en Card Services hebben de toegangssleutel.

Data storage
De data zijn uitsluitend opgeslagen in Nederlandse datacenters.

Office 365 (Outlook)
- Exchange Online: verdeeld over centra binnen Europa: Nederland, Finland, Ierland en Oostenrijk.
- Azure Active Directory (t.b.v. synchroniseren van wachtwoorden van de computer en de mail): Nederland, Ierland en Verenigde Staten maar valt onder Europese wetgeving.

Device Encryption
Aansturing op basis van Sophos:
- Voor Mac OS is FileVault2 geactiveerd, hierbij word de volledige harddisk versleuteld en kan deze niet zonder herstel sleutel of wachtwoord van de gebruiker vrijgegeven worden.
- Voor Windows is Bitlocker geactiveerd, hierbij wordt de volledige harddisk versleuteld en kan alleen met de automatisch gegenereerde herstelsleutel vrijgegeven worden. Deze verandert bij iedere nieuwe aanvraag tot ontgrendelen.

Vervreemding / data lek / vermissing devices
Medewerkers zijn verplicht vervreemding, een (potentieel data lek en/of vermissing direct te melden bij de daartoe aangestelde privacy officer.

Op afstand worden devices gewist bij ontvreemding of vermissing:
- JAMF: via het MDM-systeem kunnen alle MacBooks op afstand vergrendeld en gewist worden. De voorwaarde hiervoor is dat het apparaat internetverbinding heeft.
- SecureFileSync: via het beheerportaal kan InContext op afstand de data terugtrekken vanaf het apparaat. Dit kunnen wij ook bij de servers doen. Hiervoor geldt dezelfde voorwaarde en die is dat het apparaat verbonden is met het internet.

3. Continuïteitsplan

a.) maatregelen om de tijdige beschikbaarheid van de Persoonsgegevens te garanderen.

Verplichting medewerkers documenten centraal op te slaan
InContext verplicht haar medewerkers om documenten op de server op te slaan in de daartoe bestemde klantmappen en deelnemersmappen. Hierdoor is de continuïteit van de projecten gewaarborgd en niet persoonsafhankelijk.

Back-up server
InContext maakt gebruik van een externe back-up server in de cloud. Iedere nacht wordt een kopie van de server gemaakt. Hierdoor zijn gegevens gewaarborgd in geval van een server interruptie/ crash.

4. Exit plan

Het exit plan beschrijft hoe persoonsgegevens, die wij namens onze opdrachtgevers verwerken, worden verwijderd op het moment dat de relatie wordt verbroken.

Overdraagbaarheid aan opdrachtgever
InContext verplicht haar medewerkers om documenten op de server op te slaan in de daartoe bestemde klantmappen en deelnemersmappen. Ingeval een opdrachtgever een verzoek indient de persoonsgegevens over te dragen is InContext in staat dit onverwijld te doen.

Vernietigingshandelingen en de verslaglegging hiervan
Deelnemerslijsten worden niet langer bewaard dan 4 weken nadat een uitvoering/interventie is afgerond.
- Fysieke deelnemerslijsten worden vernietigd via een afgesloten papiercontainer die wordt geleegd door een daarin gespecialiseerde partij.
- Digitale deelnemerslijsten worden van de server verwijderd door de afdeling Projectdesk.
- Eventueel e-mailcontact tussen onze facilitators en deelnemers wordt jaarlijks voor het jaareinde gewist. Tevens eisen wij van onze medewerkers/freelancers dat zij de verwijdering schriftelijk aan ons bevestigen.