Additional Terms of Use for eConnect (Third Party Service)

INTRODUCTION

Solution and Description:

eConnect Invoice *- Solution e-invoicing, OCR+ (100% recognition), inbound and outbound invoicing, Peppol AccessPoint.*

Web-link: Solutions for e-invoicing | eConnect

SECTION A - Additions to Standard Terms

None Required

SECTION B - Additions to Unit4 – Processing Information, Security Measures and Sub-Processors

Data Processing Information (Including Sub-processors)

Part 1 – DETAILS OF PROCESSING

1. NATURE AND PURPOSE OF THE PROCESSING:

Personal data is processed in order to provide the Services;

- eConnect only processes personal data when it's necessary to provide service. To provide (tech)support to customers it is necessary to know contact and contact details.
- Outside of the processing in the context of providing service, eConnect processes personal data for business administration purposes.
- eConnect is not responsible for the data that is included on the invoice.

2. TYPES OF SERVICES AND THE PERSONAL DATA THAT IS PROCESSED:

Customer may submit Personal Data to enable **eConnect** to render the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include the following type of Personal Data depending on the type and scope of the Services:

- Customer/Employee names
- Customer address
- Customer contact details
- Customer Contract information

3. DESCRIPTION OF THE PROCESSING AND MEANS:

Processer will Process the aforementioned Personal Data in connection with the provision of the Services;

- eConnect never shares personal data with third parties, unless this is required by law.
- eConnect never shares personal data with employees, unless this is necessary to provide service.
- eConnect merely saves personal data with the above mentioned objectives.

4. RETENTION PERIOD

eConnect will keep the Personal Data **for the duration of the Agreement as long as eConnect is included in the Agreement**.

After the agreed retention, eConnect will return the personal data to the data controller, on a migration-capable format set by processor or immediately destroy the personal data without retaining a copy, upon first request of data controller

5. LOCATION OF PROCESSING:

See Part 3 below.

6. CONTACT DETAILS

For questions or comments about the Agreement and Schedules the contact person is

- eConnect International B.V.: By letter Pelmolenlaan 16A, 3447 GW WOERDEN, Netherlands

Part 2 - SECURITY MEASURES

1. IMPLEMENTED SECURITY POLICY, UPDATING AND IMPLEMENTING THE UPDATED SECURITY POLICY

eConnect undertakes to take all appropriate technical and organizational security measures prescribed within the legal framework to protect the Personal Data against loss or any form of unlawful Processing. Taking into account the state of the art and the costs of implementation, these measures guarantee an appropriate security level in view of the risks

associated with the processing and the nature of the Personal Data to be protected. The measures are also aimed at preventing unnecessary collection and further processing of personal data.

The measures taken by eConnect are included in an ISMS (Information Security Management System) that is certified in accordance with the ISO 27001 standard and also the NEN 7510 standard. The certificate can be found on eConnect's website: https://econnect.eu/nl/blog/everbinding-is-iso27001-gecertificeerd/

2. CONFIDENTIALITY CLAUSE IN EMPLOYMENT CONTRACTS;

The clause below is the translated version of the confidentiality clause included in all employment contracts at eConnect. eConnect is not liable for any change or loss of meaning due to translation of the clause.

14.1 Employees are held to strict confidentiality concerning everything that comes to their knowledge in connection with or through any job assigned to them by employer.

Employees shall consider all knowledge concerning business processes, business affairs, amount, type and names of clients as confidential.

14.2 Termination of the employment contract does not release employees from the obligations mentioned in this clause.

14.3 The employee cannot have copies of or notes on correspondence and other documents in the broadest sense, including but not limited to, computer programs, software-information, business processes, advice, (concept)contracts, in their personal belongings, or share these with third parties without consent from the managing board, unless this is necessary to carry out their job.

14.4 It is prohibited to leave client files, computers, diskettes, or other media with client or organization data, unattended in vehicles, offices and anywhere else.

14.5 Breach of this clause is an urgent reason for immediate resignation in the sense of article 7:678 paragraph 2 under i of the Dutch Civil Code (BW) and gives employer the right to take all legal action deemed necessary by him. Breach of this clause gives employer the right to demand immediately and without notice of default or summation, a €10 000,- fine. With this fine, employer does not waiver his right to compensation in case damages due to the breach are higher than aforementioned fine. Parties expressly declare to deviate from article 7:650 paragraph 3 of the Dutch Civil Code which is permitted under article 7:650 paragraph 6 of the Dutch Civil Code.

3. INTRUDER ALARM;

There is no physical storage of customer data in the eConnect offices since all systems are in the cloud. Our production systems are monitored continuously by our CloudOps-team and also by the Amazon and Azure teams.

4. SECURE METHOD FOR STORAGE OF DATA FILES;

There are many different types of data storage. All data is protected according to ISO27001 and NEN7510 standards.

5. LOGICAL ACCESS CONTROLS WITH THE HELP OF WHAT PEOPLE KNOW, SUCH AS PASSWORD OR PERSONAL ACCESS CODE;

The customers have the option for 2-factor authentication.

Our employees are enforced to use 2-factor Authentication for login.

6. LOGICAL ACCESS CONTROLS WITH THE HELP OF WHAT PEOPLE CARRY, SUCH AS A SECURITY PASS;

From the point of view of employee security, there is a need for controlled access to the office of eVerbinding. In addition, a minimal amount of physical information and equipment of value can be found in the office.

7. CONTROL ON ASSIGNED RIGHTS;

Rights and access to different functionalities and information are granted to different employees based on their job description. eConnect may only provide the Personal Data to those employees within its organization who need the Personal Data to perform their work in the context of the performance of the Agreement.

The obligations of eConnect arising from this Processor Agreement apply in full to its employees, who become aware of the Personal Data under the authority of eConnect.

8. LOGGING AND CONTROLLING THE ACCESS TO THE SYSTEM (INCLUDING MONITORING SIGNS OF UNAUTHORISED ACCESS TO THE PERSONAL DATA);

Microsoft Azure monitors and logs employee login activity. Also in the eVerbinding products logging of changes is implemented.

9. RECOVERY MEASURES;

For our internal documents we rely on the Microsoft Office 365 enterprise measurements for file storage in Sharepoint and Teams. For the customer data there are disaster and recovery plans in place.

10. THE PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA;

The eVerbinding products in general are not processing personal data. There is no structured storage of personal data, or at least it's limited to the bare minimum. Therefore pseudonymisation is not applicable.

11. THE ABILITY TO ENSURE THE ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES;

Also in this case, the measures taken by eConnect are included in an ISMS (Information Security Management System) that is certified in accordance with the ISO 27001 standard and also the NEN 7510 standard.

We monitor our services extensively. Besides our CloudOps team there are automated webtests executed from 4 locations in the world every 5 minutes. Our internal office-applications are mostly out-sourced.

12. THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT;

Internal incident management procedures:

7.1 eConnect will inform the Controller immediately and prior to the provision if a competent (government) body has made a request based on the law for the provision of Personal Data.

7.2 eConnect will at all times inform the Controller adequately and without disproportionate delay if an incident occurs with regard to the processing of the Personal Data that has consequences for data subjects and / or for the Controller. Processor informs Controller of the nature of the infringement, the consequences of the infringement and to which Data Subjects these consequences apply.

7.3 eConnect will keep the Controller informed of any new developments surrounding the incident and of the measures that eConnect is taking to limit the consequences of the incident and prevent recurrence.

7.4 The term "incident" as used in this Article 7 includes any unauthorized or unlawful processing, or a security incident in which Personal Data has been lost or unlawful processing cannot reasonably be ruled out.

7.5 Any report of the incident to the Dutch Data Protection Authority will be made by the Controller.

7.6 eConnect provides the Controller with assistance in fulfilling its obligations regarding the obligation to report data leaks ('Meldplicht Datalekken').

13. A PROCESS FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANIZATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING.

Every year, the effectiveness of our ISMS (Information Security Management System) is audited by an independent certification authority. In such an audit proof must be given to ensure the effectiveness and continues improvement of our procedures.

The standard measurements, like authorizations, logging, access rights, secure connections, storage and detecting weak spots, are investigated by accredited security experts.

Part 3 – SUB-PROCESSORS

List of potential sub-processors and locations of processing are as follows:

sub-processor (company name, location etc)	Processing location	Type of service by sub-processor
Amazon Web Services	The eConnect platform is entirely cloud-based. Cloud servers used are based in European Economic Area (EEA).	Data processing in order to facilitate services to Unit4 Customers. No data is stored or processed in breach with the GDPR or any Dutch national data protection legislation. No data is stored or processed with any other goal than providing service or to comply with applicable legislation.

Google Cloud Services	The eConnect platform is entirely cloud-based. Cloud servers used are based in European Economic Area (EEA).	Data processing in order to facilitate services to Unit4 Customers. No data is stored or processed in breach with the GDPR or any Dutch national data protection legislation. No data is stored or processed with any other goal than providing service or to comply with applicable legislation.
Microsoft Azure	The eConnect platform is entirely cloud-based. Cloud servers used are based in European Economic Area (EEA).	Data processing in order to facilitate services to Unit4 Customers. No data is stored or processed in breach with the GDPR or any Dutch national data protection legislation. No data is stored or processed with any other goal than providing service or to comply with applicable legislation.