EPOS Group A/S
Industriparken 27
DK-2750 Ballerup
Denmark

Data Processing Agreement

This Data Processing Agreement (hereinafter the “Agreement”) governs the data processing relationship between EPOS Group A/S (the Processor) and the licensed user of EPOS Manager software (the Controller)

- The Controller and the Processor hereinafter collectively referred to as the "Parties" and separately as a "Party".

1. Scope

1.1. The Processor acts as a data processor for the Controller, as the Processor process personal data for the Controller as set out in Appendix 1.1.2 "Personal data" means any information relating to an identified or identifiable natural person, see article 4(1) of Regulation (EU) 2016/679 of 27 April 2016 (the General Data Protection Regulation "GDPR"). If other confidential information than personal data is processed for the purpose of fulfilling the Agreement, any reference to "personal data" shall include the other confidential information.

2. The Controller’s Rights and Obligations

2.1. The Controller is responsible for the personal data which the Processor processes on behalf of the Controller.

2.2. It is the Controller’s responsibility to ensure that the Processor can process the personal data on behalf of the Controller on legitimate grounds. The Controller has the rights and obligations stated in this Agreement.

3. The Processor’s Obligations

3.1. The Processor shall only process personal data on behalf of the Controller and under the terms stated in the Agreement or provided that documented instructions are available from the Controller, see section 4 below.

3.2. The Processor shall keep a record with all the information necessary to demonstrate compliance with the GDPR and this Agreement.

3.3. The Processor must, at any given time and free of charge, make the information set out in section 3.2 above available to the Controller and any supervisory authority.

3.4. The Processor must promptly assist the Controller with the handling of any requests from data subjects under Chapter III of the GDPR, including requests for access, rectification, blocking or deletion. The Processor must also assist the controller by implementing appropriate technical and organizational measures, for the fulfilment of the Controller's obligation to respond to such requests.

3.5. The Processor must assist the Controller with meeting the other obligations that may be incumbent on the Controller according to EU or EU Member State law were the assistance of the Processor is implied, and where the assistance of the Processor is necessary for the Controller to comply with its obligations. This includes, but is not limited to, at request to provide the Controller with all necessary information about an incident under Clause 3.6 3.5.1(ii), and all necessary information for an impact assessment in accordance with article 35 and 36 of the GDPR.

3.6. The Processor cannot require separate payment for the time spent and for its additional expenses in relation to modifications and/or increasing of the instruction from the Controller.

4. Instructions

4.1. The Processor shall only process personal data in accordance with the Controller's instructions as set out in Appendix 1.

4.2. The Processor may not process or use the Controller's personal data for any other purpose than provided in the instructions, including the transfer of personal data to any third country or an international organization, unless the Processor is required to do so according to Union or member state law. In that case, the Processor shall inform the Controller in writing of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.3. If the Processor considers an instruction from the Controller to be in violation of the GDPR, or other Union or member state data protection provisions, the Processor shall immediately inform the Controller in writing about this.

4.4. If the Processor is subject to legislation of a third country, the Processor declares not to be aware of the mentioned legislation preventing the Processor from fulfilling the Agreement, and that the Processor will notify the Controller in writing without undue delay, if the Processor becomes aware of that such hindrance is present or will occur.

4.5. The Controller's instructions include any such processing that is required for the Processor's delivery of the services to the Controller. Instructions from the Controller which affects or changes the content of the agreed service to be provided, is handled in accordance with any applicable main service agreement.

4.6. The Processor is under no circumstances entitled to condition the full and unlimited compliance with the Controller's instructions on the Controller's payment of outstanding invoices etc. The Processor shall at no point in time have a right of retention (or similar) of the Controller's personal data.

4.7. The Processor can solely process personal data outside the scope of the instructions if this is required by mandatory EU law or national legislation. The Processor shall inform the Controller of such reason, unless such notification would be in breach of EU or EU Member state law.

5. Technical and Organizational Security Measures

5.1. The Processor shall implement appropriate technical and organizational measures to prevent that the personal data processed is:

(i) accidentally or unlawfully destroyed, lost or altered,

(ii) disclosed or made available without authorization, or

(iii) otherwise processed in violation of applicable laws, including the GDPR.

5.2. The Processor must also comply with the special data security requirements that apply to the Controller, see Appendix 2, and with any other applicable data security requirements that are directly incumbent on the Processor; including the data security requirements in the country of establishment of the Processor, or in the country where the data processing will be performed.

5.3. The appropriate technical and organizational security measures must be determined with due regard for

(i) the current state of the art,

(ii) the cost of their implementation, and

(iii) the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

5.4. If subsequently – in the assessment of the Controller – mitigation of the identified risks require further measures to be implemented by the Processor, than those already implemented by the Processor pursuant to article 32 of the GDPR, the Controller shall specify these additional measures to be implemented in Appendix 2.

5.5. In Appendix 1, the Processor has stated the physical location of the servers, service centers etc. used to provide the data processing services. The Processor undertakes to keep the information about the physical location updated by providing a prior written notice of two months to the Controller. This does not require a formal amendment of Appendix 1, prior written notice by mail or email suffices.

6. Personal Data Breach

6.1. The Processor is obliged to inform the Controller without undue delay of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed or if the Data Processor has a reasoned suspicion or there is a threat thereof.

7. Notifications

7.1. The Processor must without undue delay after becoming aware of the facts in writing notify the Controller about

(i) any request for disclosure of personal data processed under the Agreement by authorities, unless expressly prohibited under Union or member state law,

(ii) any suspicion or finding of

(a) personal data breach by following the procedure set out in section 6 above, or

(b) other failure to comply with the Processor's obligations, or

(iii) any request for access to the personal data received directly from the data subjects or from third parties.

8. Transfer to Other Countries

8.1. If any personal data is transferred to another EU member state than the Controller's Member State, the Processor shall be responsible for compliance with any requirements that might be laid down in the given EU Member State's legislation.

8.2. The Processor is only allowed to transfer personal data to a third country or to international organizations in accordance with the Controller's instructions in Appendix 1, the Standard Contractual Clauses, or if the Controller otherwise has given documentable permission to a transfer of personal data to a third country or to international organizations. Regardless of this requirement, it is the Processor's responsibility to ensure that there is a legal basis for the transfer, including appropriate safeguards, in accordance with GDPR Chapter V, e.g. the EU

Commission's Standard Contractual Clauses for the transfer of personal data to third countries. These requirements also apply to any sub-processor approved in accordance with the procedure set out in section 9 below.

8.3. According to this clause 8 of this Agreement, the Controller accepts that the Processor may transfer personal data to countries outside of the EEA (third countries). By entering into this Agreement and in accordance with the stated in Appendix 3, the Controller hereby grants the Processor a power of attorney to enter into the necessary agreements i.e. the EU Standard Contractual Clauses for the transfer of personal data to third countries.

9. Sub-Processors

9.1. The Processor may engage a sub-processor. The Sub-processors currently engaged by the Processor and authorized by Controller are available at https://www.eposaudio.com/en/us/enterprise/technology/software/sub-processors Customer shall be notified by Processor in advance of any new Sub-processor being appointed by changes to this website.

9.2. Controller may object in writing to the appointment of an additional Sub-processor within five (5) calendar days after receipt of Processor's notice in accordance with the mechanism set out at Section 9.1 above. In the event that Controller objects on reasonable grounds relating to the protection of the Personal Data, then the parties shall discuss commercially reasonable alternative solutions in good faith. If no resolution can be reached, Processor will, at its sole discretion, either not appoint Sub-processor, or permit Controller to suspend or terminate the affected service in accordance with the Agreement.

9.3. Prior to the engagement of a sub-processor, the Processor shall conclude a written agreement with the sub-processor, in which at least the same data protection obligations as set out in the Agreement shall be imposed on the sub-processor, including an obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR and any other applicable legislation.

10. Confidentiality

10.1. The Processor shall keep personal data confidential.

10.2. If the Processor is a legal entity, all terms of the Agreement apply to any of the Processor's employees and the Processor must ensure that its employees comply with the Agreement.

10.3. The Processor must limit the access to personal data to employees for whom access to said data is necessary to fulfil the Processor's obligations towards the Controller.

10.4. The Processor shall not disclose the personal data to third parties or take copies of personal data unless strictly necessary for the performance of the Processor’s obligations towards the Controller according to the Agreement.

10.5. The Data Processor shall ensure that persons authorized to process personal data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to suitable statutory obligation of confidentiality.

11. Deletion, Return, or Destruction of Personal Data

11.1. Processor shall delete, return or destruct personal data in accordance with the Controllers instructions or upon Controller’s request.

11.2. The Controller is, at its own expense, entitled to and with assistance from an independent third party to inspect that deletion etc. has been done in accordance with the stated.

11.3. Regardless of section 11.1, the Processor is entitled, to the extent necessary in order to document performance of the service in accordance with the Agreement or to defend itself against any legal claims, to save a copy of the Controller's personal data. The Controller's personal data must in such case only be processed in connection with the above listed purposes and shall cease when these are non-existing.

11.4. The Processor must ensure that the sub-processors do not process personal data after the termination of the Agreement, unless section 11.3 applies.

12. Information, Supervision, and Audit

12.1. The Processor shall upon request provide the Controller with sufficient information to enable the Controller to ensure that the Processor complies with its obligations under the Agreement.

12.2. The Processor must provide information related to the provision of the services to authorities or the Controller's external advisors, including auditors, if this is necessary for the performance of their duties in accordance with EU or EU Member state law.

12.3. The Processor must give authorities who by EU or EU Member State law have a right to enter the Controller's or the Controller's supplier's facilities, or representatives of the authorities access to the Processor's physical facilities.

12.4. The Processor must without undue delay after becoming aware of the facts in writing notify the Controller about any request for disclosure of personal data processed under the Agreement by authorities, unless expressly prohibited under EU or EU Member State law.

12.5. The Controller is entitled at its own cost to have an audit by an independent expert of the Processor's handling of personal data. This expert shall have access to the Processor's data processing facilities and receive the necessary information in order to be able to audit whether the Processor complies with its obligations under the Agreement, including ensuring that the appropriate technical and organizational security measures have been implemented. The expert shall upon the Processor's request sign a customary non-disclosure agreement, and treat all information obtained or received from the Processor confidentially and may only share the information with the Controller.

13. Liability

13.1. Notwithstanding any other agreement between the Parties, a Party is liable to the other Party for any direct loss due to acts of negligence or omission from the Party in question, including for breach of security. The Parties are however not liable to each other for indirect losses, consequential losses and damages.

13.2. Notwithstanding section 2.1, and without limitation, any liability towards data subjects shall be regulated in accordance with applicable law, including article 82 of the GDPR.

14. Term and Termination

14.1. The Agreement enters into force at the time of acceptance by the Controller and remains in force until terminated.

14.2. The Controller may suspend the transfer of data and/or terminate the contract with immediate effect, as stipulated in Clause 5 of the Standard Contractual Clauses.

14.3. On termination or expiration of any main agreement (if any) for the provision of services between the Parties, this Agreement and the Standard Contractual Clauses, shall simultaneously cease to be in effect.

14.4. In case of termination of the Agreement, the Processor shall immediately transfer or delete personal data in accordance with section 11.2-11.4 above.

14.5. Notwithstanding section 14.1-14.3, this Agreement shall remain in effect as long as the Processor is processing, including keeping copies of, the Controller's personal data covered by this Agreement.

14.6. Notwithstanding section 14.1-14.3, this Agreement shall remain in effect as long as the Processor is processing, including keeping copies of, the Controller's personal data covered by this Agreement.

14.7. To the extent the Processor is in possession of Personal Data being processed on behalf of the Controller when the Agreement expires, the Processor shall, at the request of the controller, make such Personal Data available for the Controller. If such request has not been received in writing by the Processor, the Processor shall delete such Personal Data within 60 days after the termination of the agreement, unless legally prohibited from doing so.

15. Priority and Severability

15.1. In the event of conflict between this Agreement and any other agreement between the Parties, the provisions of this Agreement shall prevail. However, the Agreement shall not apply if and to the extent the EU Commission's Standard Contractual Clauses for the transfer of personal data to third countries are concluded and such clauses set out stricter obligations for the Processor and/or for sub-processor.

15.2. If any provision of this Agreement or any related instruction is held to be invalid, illegal, or unenforceable, the remaining provisions hereof shall be unaffected thereby and remain valid and enforceable as if such provision had not been set forth herein. The Parties agree to substitute for such provision a valid provision or instruction that most closely approximates the intent of such severed provision or instruction.

16. Governing Law

16.1. The Data Processing Agreement shall be governed by the laws of Denmark, excluding any private conflict laws.

16.2. Any dispute arising from the Data Processing Agreement must be settled by [the City Court of Copenhagen].

17. Selling and Sharing Collected Personal Data

17.1. The Data Processor do not sell personal data collected by EPOS Manager to third parties. EPOS Group A/S only share aggregated data(Non-personally identifiable information) to third-parties.

17.2. Notwithstanding clause 17.1, the Data Processor is authorized to disclose/share personal data to/with Demant A/S, Kongebakken 9, 2765 Smørum, Denmark, CVR 71186911 ("Demant A/S") or any other entity within the Demant Group as long as such disclosure serves a legitimate

purpose, which may include but is not limited to assisting EPOS Group A/S in relation to audits, handling personal data breaches, assisting in complying with applicable data protection law including GDPR, especially Chapter 3 and articles 32-36 of the GDPR.

18. List of Appendixes

- Appendix 1: The Processed Data
- Appendix 2: Security
- Appendix 3: Power of Attorney

EPOS Group A/S
Industriparken 27
DK-2750 Ballerup
Denmark

Appendix 1 – The Processed Data

This Appendix 1 constitutes the Controller's instruction to the Processor in connection with the Processor's data processing for the Controller and is an integrated part of the Agreement.

The processing of personal data:

Name, company registration no. and address	EPOS Group A/S CVR no.: 39820242 Industriparken 27 DK-2750 Ballerup Denmark
The purpose, nature and duration of processing	The Processor collects and processes personal data and other data from users of the Software to allow the Controller to distribute client software and product software and carry out maintenance of associated products and configuration of products belonging to associated users. Further, the Processor collects log error data for troubleshooting and improving end user experiences. The data collected will also allow the Controller to analyze the usage of the units. The data will be processed until the Controller terminates the agreement with the processor.
The category of the data subject	[E.g. customers/end users] [E.g. employees]
Categories of personal data	Re b) I: name, email address, IP address, MAC address, machine name. Other non-personal data collected related to usage of: • Software • Products • Call activity statistics • Softphone • Host information where products are used. • Application logs • AD user information detection flows – no user data. • Meta data from update jobs and tenant configuration from EPOS Manager.

	Re b) II: name, email address, telephone number, MAC address, machine name, IP Address. Other non- personal data collected related to usage of: • Software • Products • Call activity statistics • Softphone • Host information where products are used. • Application logs • AD user information detection flows – no user data. • Meta data from update jobs and tenant configuration from EPOS Manager.
Special categories of data: • Data the sub-processor must process on behalf of the Processor • Data concerning civil registration numbers (in Danish CPR-nr.) • Sensitive data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or sex life or sexual orientation • Data related to criminal Records	Re b) I: none Re b) II: none
Locations, including name of country/countries of processing	Ballerup, Denmark Location of Sub-processors as mentioned in Sec 9.1
If possible, the expected deadlines for deletion of the categories of information	Re b) I • 60 days after the request of deletion Re b) II • 60 days after the request of deletion

EPOS Group A/S
Industriparken 27
DK-2750 Ballerup
Denmark

Appendix 2 - Security

Security measures (see section 5 in the Agreement). It should be noted that below are not exhaustive and that EPOS Group A/S follows best practice e.g., ISO 27001.

- Data confidentiality: Cryptography policy that covers data-at-rest and data-in-transit shall be in place. The policy shall be in line with accepted industry standards such as AES. Data is natively encrypted at rest in Microsoft Azure database and in transit it is encrypted using HTTPS protocol.
- Device and media controls: Malware protection policy that covers endpoints and servers shall be in place. Microsoft Azure Platform as a service is used which ensures that the endpoints and servers have the appropriate malware protection policy.
- Network security: A network security policy shall be in place that covers network and connected networks and to all equipment connected to those networks physically or via wireless. All communication to the servers is done using HTTPS protocol.
- Security management: Vulnerability- assessment and patching policy shall be in place. It must be ensured that known software vulnerabilities are addressed and have a security patching strategy. Microsoft Azure takes care of the security management of the servers.
- Access control: A policy that covers Unique User ID, Password Rules, Automatic Logoff, Account Lockout Policy, Access Monitoring shall be in place. Individual logins are available along with automatic log off and account lock policy.
- Access management: A policy that covers Partners and Subcontractor Access, Role Based Access, Privileged Access Rights, Access Request and Authorization Procedure, Access Termination procedure, Identity and Access reviews shall be in place.

Data is accessible only by authorized people in the system.

EPOS Group A/S
Industriparken 27
DK-2750 Ballerup
Denmark

Appendix 3 - Power of Attorney

Introduction

According to clause 8 of this Agreement, the Controller explicitly accepts that the Processor may transfer personal data to countries outside of the EEA (third countries).

Scope of the Power of Attorney

The Controller hereby grants to the Processor a power of attorney to enter into the agreements necessary for the transfer of personal data to third countries. The purpose of this power of attorney is to ensure an adequate level of protection of the personal data which the Controller has transferred to the Processor for processing in accordance with the Agreement.

The power of attorney covers the adoption of the EU Commission's Standard Contractual Clauses (as described in clause 8 of the Agreement) on behalf of the Controller in order for the Standard Contractual Clauses to apply directly to the data processing carried out on behalf of the Controller by one or more sub-processors established outside the EEA and engaged by the Processor.

The power of attorney covers the adoption of the said Standard Contractual Clauses in unchanged form only.

Other Issues

The Processor may not grant or transfer this power of attorney to a third party. The power of attorney is governed by Danish law.