Data Processing Agreement

Version 2.0

between

the data controller (Customer)

and

Azets Insight A/S
Lyskær 3CD
DK-2730 Herlev
Denmark
Registration no. 25 07 48 23

(the data processor)

each a ‘party’; together ‘the parties’

Regarding the processing of personal data

Replaces all previously entered data processing agreements between the parties.

Table of Contents

Background and Purpose

1.1 The data processor (Supplier) and the data controller (Customer) have agreed the following Standard Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1.2 The Clauses are based on the Danish Data Protection Agency's Standard Contractual Clauses (version 1.1 - January 2020) in accordance with Article 28 (1). 3 of Regulation 2016/679 for the processing of personal data by the data processor.

Preamble

2.1 These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2.2 The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

2.3 In the context of the provision of Services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

2.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5 Four appendices are attached to the Clauses and form an integral part of the Clauses.

2.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

2.7 Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

2.8 Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

2.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.11 The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

The Rights and Obligations of the Data Controller

3.1 The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

3.2 The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3.3 The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

The Data Processor Acts According to Instructions

4.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.2 The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

Confidentiality

5.1 The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2 The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

Security of Processing

6.1 Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and 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, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a. Pseudonymisation and encryption of personal data;
b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.2 According to Article 32 GDPR, the data processor shall also - independently from the data controller - evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

6.3 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

Use of Sub-processors

7.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

7.2 The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

7.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least two (2) weeks in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

7.5 A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

7.6 Deleted (optional)

7.7 If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

Transfer of Data to Third Countries or International Organisations

8.1 Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

8.2 In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3 Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

a. transfer personal data to a data controller or a data processor in a third country or in an international organization
b. transfer the processing of personal data to a sub-processor in a third country
c. have the personal data processed in by the data processor in a third country

8.4 The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

8.5 The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2) (c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

Assistance to the Data Controller

9.1 Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

9.2 In addition to the data processor's obligation to assist the data controller pursuant to Clause 9.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Danish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the data controller's obligation to consult the competent supervisory authority, the Danish Data Protection Agency, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

9.3 The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1 and 9.2.

Notification of Personal Data Breach

10.1 In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

10.2 The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

10.3 In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4 The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

Erasure and Return of Data

11.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

11.2 The following EU or Member State law applicable to the data processor requires storage of the personal data after the termination of the provision of personal data processing services:

a. The Danish Accounting Act.

The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

Audit and Inspection

12.1 The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

12.2 Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7 and C.8.

12.3 The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

The Parties' Agreement on Other Terms

13.1 The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

Commencement and Termination

14.1 The Clauses shall become effective on the date of both parties' signature.

14.2 Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3 The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

14.4 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1 and Appendix C.4., the Clauses may be terminated by written notice by either party.

Data Controller and Data Processor Contacts/Contact Points

15.1 The parties may contact each other using the following contacts/contact points:

15.2 The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

On behalf of the data controller:
Pursuant to the main document of executed Agreement

On behalf of the data processor:

Telephone	+45 70 27 31 30
E-mail	gdpr-dk@azets.com

Appendix A Information about the Processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller; and **A.2.** The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing)	The data processor may only process personal data for the purposes necessary to fulfil the agreement with the data controller, including storage, collection, registration, systematisation, consolidation, deletion, archiving, etc. Purpose must be stated here or possibly in written addenda / supplementary agreements. Where the IT systems involved in the agreement for the provision of services offer the data controller the option of API integration, the following has been agreed: • The data controller accepts that the data controller and his/her employees, etc. has the option to install and use third-party app(s) that can communicate and exchange the individual's information, including personal data, with involved IT systems and that such data processing is covered by these instructions • The data controller imports the information necessary for the use of the services, and instructs the data processor to continuously and automatically obtain and/or exchange entered, imported, and/or information generated by the IT systems involved, including personal data • Upon the installation and acceptance of third-party app(s) by the data controller, an independent legal relationship arises between the data controller and the supplier of the third-party app(s) • The use of third-party app(s) is thus subject to the terms and conditions of the app providers in question and the data processor is not responsible for the data controller's use of such third-party apps as well as the processing and storage of personal data by the app providers in question after these have been transferred The data processor is obliged to continuously and automatically obtain personal data from relevant authorities to ensure that information for the use in the services is kept up to date at all times. The data processor is obliged to process personal data as required by law, including in connection with a legal decision, regulatory requirements, the data controller's bankruptcy, death, or the like. The data processor is obliged to comply with the disclosure obligation in the Danish Bookkeeping Act by giving authorities access to data. The data processor is also entitled to anonymise personal data for statistical purposes. The data processor is entitled to include personal data in the data processor's usual backup procedure. The data processor and its sub-processors reserve the right to disclose data to the data controller's authorised signatories for as long as the service agreement is active. During the ongoing service agreement and after its termination, the sub-processor is entitled to process application data in anonymised form for the purpose of maintaining and developing the application, including security measures and user experiences.
A.3. The processing may include the following types of personal data about data subjects	The processing may include: • non-sensitive personal information • sensitive personal data • confidential personal data Specific categories of personal data are listed in Appendix D.2 in connection with the Services.

	The processing does not include: • genetic or biometric data • racial or ethnic origin, or political, philosophical, or religious beliefs • sexual orientation
A.4. Processing includes the following categories of data subject	The processing may include the data controller's: • current and former employees • fee recipients • prospective employees • customers, suppliers, and other business partners • members of housing associations (including cooperative housing associations, owners' associations, homeowners' associations, and similar), as well as the housing associations' employees, board members, tenants/residents/subtenants, suppliers, and other business partners • owners of rental properties/tenancies and their employees, board members, tenants/residents/subtenants, suppliers, and other business partners The connection to the Services is specified in Appendix D.3.
A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration	The data processing of personal data follows the duration specified in any active Service agreement, as well as the data controller's instructions in Clause 11.1 and 11.2. However, subject to the exceptions set out in Clause C.4 (Storage periods/erasure routines).

Appendix B Authorised Sub-processors

B.1. Approved Sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADRESS	DESCRIPTION OF PROCESSING
Azets Insight SRL	VAT RO24813426 Org. J32/1906/2008	Str. Nicolaus Olahus, nr. 5 Et. 9-10 550370 Sibiu, Romania	Administrative assistance
Azets Insight AS	Org. Nr. 983 338 917	Drammensveien 151 NO-0101 Oslo	Hosting/operation of the applications: • Azets Invoice/Reporting • Visma Business where all data is hosted by the sub-processor AWS in Stockholm (EU-North-1) and Ireland (EU-West-1).
Azets Labs A/S	CVR no. 10 40 77 45	Lyskær 3 CD DK-2730 Herlev	SaaS: Hosting/operation, development and maintenance of the applications: • Azets EPOS Løn, where all data is stored with its sub-processor AWS in Stockholm (EU-North-1) and Ireland (EU-West-1) • Workcyclus APV products, where all data is stored with its sub-processor Azure in West Europe (Netherlands)
Azets Perspektiv A/S	CVR nr. 43 09 57 57	Lyskær 3C, st. DK-2730 Herlev	SaaS: Hosting, development, and maintenance of the application Azets Perspektiv, including the Mit Perspektiv modules, as well as the application Azets Perspektiv Time. All data is stored in Denmark, where the sub-processor's hardware is located in two (2) external data centres (housing).
Azets Software AB	Org. no. 559273-6937	Ekensbergvägen 113 SE-171 41 Solna	SaaS: Hosting, development, and maintenance of the application Azets Cozone Portal/Activity/Drive/Employee. All data is stored with its sub-processor AWS in Stockholm (EU-North-1) and Europe Ireland (EU-West-1).
e-Boks A/S	CVR no. 25 67 41 54	Hans Bekkevolds Allé 7 DK-2900 Hellerup	Digital receipt of payslips from PostNord Strålfors A/S (method 2 “Azets” and 3 “Customer name”), temporary storage and distribution to recipients in e-Boks in connection with payroll administration in the applications EPOS Løn, Azets EPOS Løn and Azets Perspektiv. All data is stored with its sub-processor in Denmark.
EG Danmark A/S (EG Bolig)	CVR no. 84 66 78 11	Lautrupvang 24 DK-2750 Ballerup	SaaS: Hosting/operation, development, maintenance, and support of the property management system ProBo. All data is hosted by its sub-processor in Europe.
Findity AB	Org. no. 556838-8200	Engelbrektsgatan 20 SE-771 30 Ludvika	SaaS: Hosting, development and maintenance of the expense system Azets Expense.

NAME	CVR	ADRESS	DESCRIPTION OF PROCESSING
			All data is stored in Sweden, where the sub-processor's hardware is located in two (2) external data centres (housing).
Freshworks Inc.	Org. no. 33-1218825	2950 S. Delaware Street, Suite 201,94403 San Mateo, CA USA	SaaS: Hosting, development and maintenance of Freshdesk (support system). All data is stored with its sub-processor AWS in multiple availability zones in Frankfurt (EU-Central-1), each located at a minimum distance of 35 km.
PostNord Strålfors A/S	CVR no. 10 06 86 57	Hedegaardsvej 88 DK-2300 København S	• Digital receipt, temporary storage and forwarding of payslips to e-Boks A/S (method 2 “Azets” and method 3 “Customer name”) in connection with payroll administration in the applications EPOS Løn, Azets EPOS Løn and Azets Perspektiv • Digital receipt, temporary storage, and distribution of payslips to recipients in e-Boks (method 1 “Your Employer”) in connection with payroll administration in the applications EPOS Løn, Azets EPOS Løn and Azets Perspektiv • Digital receipt, temporary storage, and distribution of payslips to recipients in mit.dk in connection with payroll administration in the applications EPOS Løn, Azets EPOS Løn and Azets Perspektiv • SaaS: Hosting, operation, development, maintenance and support of the eDistribution solution for forwarding communications to the data controller in public digital mailboxes (such as Virk.dk, e-Boks, and mit.dk) All data is stored in Denmark and with its sub-processor in Sweden.
Twoday Danmark A/S	CVR no. 29 97 33 34	Sundkaj 125 DK-2150 Nordhavn	SaaS: Hosting/operation, development, maintenance, and support of the Addo Sign application for legally valid digital signing and distribution of documents following the validation of users’ identities. All data is hosted by its sub-processor in Denmark.
Unik System Design A/S	CVR. no. 17 51 26 92	Boulevarden 19E, DK-7100 Vejle	SaaS: Hosting/operation, development, maintenance, and support of the property management system Unik Bolig CE / HabiCen. All data is hosted by its sub-processor in Denmark.

NAME	CVR	ADRESS	DESCRIPTION OF PROCESSING
Visma e-conomic A/S	CVR no. 29 40 34 73	Gærtorvet 1-5 DK-1799 København V	SaaS: Hosting/operation, development, maintenance, and support of the application, e-conomic. All data is hosted by its sub-processors in the Netherlands (Google Cloud).
Visma IMS A/S	CVR no. 25 86 20 15	Søren Frichs Vej 440 DK-8230 Åbyhøj	SaaS: Hosting, operation, development and maintenance of the ESDH system IMS Case. All data is stored with its sub-processors in Denmark and Switzerland.
Wolters Kluwer Danmark A/S	CVR no. 13 38 62 93	Sturlasgade 3 DK-2300 København S	Support in the use of the following licensed products: • "Årsafslutning Professionel" for the preparation of annual reports, including manual upload for submission of financial data via iXBRL to the Danish Business Authority (Erhvervsstyrelsen). • "Skat Professionel Nova" for the preparation of tax returns as well as the compilation of income and wealth statements. All data is stored in Denmark by the data processor; however, in exceptional support situations, data may be temporarily exchanged with sub-processors for the purpose of analysing and testing system-related issues.
Zebon ApS	CVR no. 32 36 64 49	Nordre Strandvej 119 A DK-3150 Hellebæk	SaaS: Hosting, operation, development and maintenance of the expense system zExpense. All data is stored in Denmark, where the sub-processor's hardware is located in two (2) external data centres (housing).
Zenegy Danmark ApS	CVR no. 38 36 60 41	Slotsmarken 16 DK-2970 Hørsholm	SaaS: Hosting, operation, development and maintenance of the application Azets Simplify. All data is stored with its sub-processor Microsoft Azure in the Netherlands.

The connection to the Services is specified in Appendix D.4.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled - without the data controller's explicit written authorisation - to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Appendix C Instruction Pertaining to the Use of Personal Data

C.1. The subject of/instruction for the processing	The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following: See Appendix A item A.1 / A.2. The data controller accepts that, in connection with any customer-specific and free-text fields in the IT solution(s), including associated documents, no other personal data may be entered than those specified in Appendix A item A.3. Should the data controller enter personal data other than those specified in Appendix A, the data controller must immediately notify the data processor thereof and update the instructions in the Provisions. The data controller accepts, in connection with the data processor's handling of digital documents from public digital mailboxes to the data controller, that the sender determines the content. Thus, digital documents may contain both ordinary and sensitive personal data in an undefined scope beyond what is specified in Appendix A item A.3.
C.2. Security of processing. The level of security must reflect:	The processing of data includes personal data, as mentioned in Appendix A item A.3 / A.4 and which may be - but not necessarily - covered by Article 9 of the Data Protection Regulation on "special categories of personal data", for which reason a "high" security level must be established. The data processor is entitled and obliged to make decisions about which technical and organisational security measures must be implemented to establish the necessary (and agreed) level of security. The data processor guarantees to the data controller that the data processor will implement the appropriate technical and organisational security measures in such a way that the data processor's processing of personal data meets the requirements of the personal data law regulation in force at any given time. The data processor shall however - in any case and as a minimum - implement the measures described in item C.2.1 - C.2.15, which have been agreed with the data controller.
C.2.1 Pseudonymisation and encryption of personal information	The data processor is obliged to implement and maintain appropriate technical and organisational measures to ensure that personal data is pseudonymised, where relevant for services. The data processor is obliged to implement and maintain appropriate technical and organisational measures to ensure that personal data is encrypted or otherwise protected against, among other things, unauthorised access and/or manipulation, particularly in connection with transmission via open networks and/or external communication connections. The level of encryption must be appropriate to effectively prevent unauthorised access to personal data. See item C.2.7.

C.2.2 Ensuring the confidentiality, integrity, availability and robustness of processing systems and services	The confidentiality obligation of the data processor's employees is specified in item C.2.6. Technical security of the data processor: • Virus definitions are updated daily • Local firewall on PCs and servers is enabled • Network is protected by a firewall • Ongoing internal and external vulnerability scans to ensure optimal configuration • Employees and externally affiliated consultants have external access to networks via encrypted connections with MFA • Data on all PCs is encrypted • Complex passwords are used • Exchange of personal data with the data controller and others takes place via encrypted connections, for example, SFTP or web portals • Ongoing backup of data Organisational security of the data processor: • Authorization procedures, access rights, logging, etc. in accordance with the data processor's internal IT procedures • Employees and externally affiliated consultants receive security training and comprehensive instructions and guidelines regarding the processing of personal data and IT security
C.2.3 Recovery of personal data and operation (includes all systems unless specified)	The data processor is obliged to implement and maintain appropriate technical and organisational measures to ensure timely restoration of access to personal data in the event of physical incidents (e.g. power outages, fire, flooding, lightning strikes, etc.) and/or technical incidents (e.g. system crashes), including through contingency plans, procedures, etc. The data processor is obliged to implement and maintain documented contingency procedures that ensure the re-establishment of services without undue delay in the event of operational disruptions. Payroll administration on the application Azets Perspektiv, including Mit Perspektiv modules and the application Azets Perspektiv Time: • The data processor has contingency preparedness and a disaster recovery solution. The solution is "standby," meaning that the hardware platform is established and ready to be used for re-establishment/restoration. The target is re-establishment within twenty-four (24) hours. The application Azets Expense (travel expense management): • The data processor has contingency preparedness and a disaster recovery solution. The solution is "standby," meaning that the hardware platform is established and ready to be used for re-establishment/restoration. The target is re-establishment within twenty-four (24) hours.
C.2.4 Procedure for regular testing, assessment and evaluation of the effectiveness of technical and organisational security measures to ensure processing safety	The data processor is obliged to implement and maintain appropriate technical and organisational measures for the regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the security of processing. The data processor conducts annual controls of sub-processors by reviewing data processing agreements for the individual sub-processors as well as performing a risk assessment. Any identified issues will be followed up (see item C.8).

C.2.5 Staff access to personal data	The data processor ensures, through formal approval processes and recurring access controls, that only people with a documented work-related need have access to personal data. The data processor must, without undue delay, revoke authorisations (including access rights) for users who no longer have a work-related need for authorisation.
C.2.6 Confidentiality (includes all systems unless specified)	All employees of the data processor and externally affiliated consultants are subject to a contractual duty of confidentiality regarding everything the employee becomes aware of during their work for the data processor, concerning all business-related and confidential information about parties with whom the data processor has relations. The duty of confidentiality also applies after the termination of the employment relationship. Monitoring and management of digital mailboxes with the application eDistribution: • All employees of the sub-processor in Denmark with access to personal data must be subject to PET security clearance at the classification level "Confidential". The security clearance must be maintained throughout the employee's employment with the sub-processor.
C.2.7 Data protection during transmission and at rest (includes all systems unless specified)	The data processor is obliged to implement and maintain appropriate technical and organisational measures to ensure that personal data is protected against, among other things, unauthorised access and/or manipulation. Encryption of the transport layer must at all times meet the Danish Data Protection Agency's minimum requirements. Payroll administration on the application EPOS Løn: • External file delivery to and from the solution takes place via SFTP • Web service communication between EPOS Løn and EPOS HR is encrypted • The solution is a client-server solution accessed via the data processor's network. Data within the solution is protected by multi-level access control. Cisco ISE ensures that only authorised employees can access the payroll environment. Access also requires logical access to data through AD groups and direct user permissions in the database Payroll administration on the application Perspektiv, including Mit Perspektiv modules: • External file delivery to and from the solution takes place via SFTP Applications EPOS Løn, EPOS HR, and EPOS Recruitment: • External file delivery to and from the solution takes place via SFTP • For hosted customers, the dedicated database is accessed via a secure portal with MFA by named users. All communication to and from the solution is encrypted, either via web services, HTTPS requests, or through the web solution Application EPOS Management: • The application is an encrypted add-on between the Customer's Excel and EPOS HR. Data is sourced solely from EPOS HR Application Addo Sign: • The solution is accessed in encrypted form via web

	• All communication to and from the solution is encrypted, either via HTTPS requests through the web solution or via API communication using VOCES certificates Application IMS Case (ESDH system): • The solution is accessed in encrypted form via web • All communication to and from the solution is encrypted, either via HTTPS requests through the web solution or via API communication
C.2.8 Physical security of locations where personal data is processed	The data processor is obliged to implement and maintain appropriate physical, technical and organisational measures to secure the physical locations where personal data is processed against, among other things, unauthorised access and/or manipulation of data. Physical access security has been established to ensure that only authorised persons can obtain physical access to premises and data centres where personal data is stored and processed.
C.2.9 Backup	Backup of systems, configuration files and data must take place so that relevant data can be re-established. The backup copies are stored in such a way that they are not accidentally or illegally (for example by fire, flood, accident, theft or the like) destroyed, lost, degraded, come to the knowledge of unauthorised persons, misused or otherwise treated in violation of the rules and regulations in force at any time for the processing of personal data. Including amongst others: • The same guidelines apply to backup copies as to any other processing of personal data under Agreement and this data processing agreement • Backups are stored geographically separate from the primary data centre • The data processor continuously checks that backups are readable Backup covers the data processor's entire environment, including databases, with the purpose of enabling complete reconstruction. Accordingly, the backup is not intended for the restoration of individual customer data.
C.2.10 Password policy and control of rejected access attempts (includes all systems unless specified)	The data processor is obliged to implement and maintain appropriate technical and organisational measures to ensure that passwords are of appropriate length and complexity to prevent them from being guessed. Passwords must be unique to each individual employee and externally affiliated consultant. The data processor is obliged to log rejected login attempts and to block further attempts after a defined number of consecutive failed access attempts. Application Azets Simplify: • Passwords are encrypted using SHA256 with a unique salt Application Addo Sign: • Passwords are hashed and salted
C.2.11 Home workplaces	The data processor is obliged to implement and maintain appropriate technical and organisational measures to ensure that personal data is protected against, among other things, unauthorised access and/or manipulation when accessed from home or remote workplaces. Access to personal data from home or remote workplaces must

	include encryption of communication connections and authentication of the individuals accessing the data. All computers are encrypted and password protected. Access to the data processor's systems takes place via a VPN connection with MFA. Any printing is minimised to the greatest extent possible and must be shredded after use. Employees and externally affiliated consultants must regularly undergo mandatory awareness training in accordance with item C.2.12.
C.2.12 Awareness training	The data processor is obliged to ensure that employees and externally affiliated consultants regularly (and at least annually) undergo mandatory training in IT security and data protection.
C.2.13 Change management	The data processor is obliged to have formal change management procedures in place to ensure that any change is duly authorised, tested and approved prior to implementation.
C.2.14 Logging (includes all systems unless specified)	The data processor is obliged to implement and maintain appropriate technical and organisational measures that ensure logging so that incidents can be tracked. Logs must contain timestamps and, where relevant, user ID, terminal ID, and network addresses. As a minimum, the following security incidents must be logged: • Rejected access attempts • Successful and rejected authentication attempts resulting from account lockout triggered by the access control system Access to personal data must be logged to such an extent that the log data can be used to prevent and avert unauthorised access to personal data. Where relevant, access to personal data must be logged, including which data is accessed, how the data is processed, as well as time and identity information. Logs are stored for a maximum of thirteen (13) months. In the event of incidents, the storage period may be extended. The backup archive is stored for a maximum of six (6) years (cf. Appendix D regarding Clauses 11.1 and 11.2). During the same period, the data processor is entitled to include the personal data in the data processor's regular backup procedure. Payroll administration on the application Perspektiv Løn, including Mit Perspektiv modules, as well as the application Perspektiv Time: • Logs are stored for a maximum of one hundred and eighty (180) days. In the event of incidents, the storage period may be extended. • During the same period, the data processor is entitled to include the personal data in the data processor's regular backup procedure. Property administration on the application Unik Bolig CE / HabiCen: • Logs are stored for a minimum of six (6) months. • During the same period, the data processor is entitled to include the personal data in the data processor's regular backup procedure.

	Application Azets Expense (travel expense management): • Logs are stored for a maximum of thirty (30) days. In the event of incidents, the storage period may be extended. • During the same period, the data processor is entitled to include the personal data in the data processor's regular backup procedure.
C.2.15 Data protection advisor and IT security personnel	The data processor must ensure that there is a focus on information security within its own organisation, with a defined allocation of roles and responsibilities. The data processor is obliged to appoint one or more data protection officers, as described in the General Data Protection Regulation. The data processor is obliged to have dedicated resources in place to maintain the data processor's IT security.
C.3. Assistance to the data controller	The data processor shall, to the extent necessary and reasonable, assist the data controller in fulfilling its obligations when processing personal data covered by the provisions of Clauses 9 and 10 by implementing such technical and organisational measures as may contribute to the data controller's ability to respond to requests for the exercise of the rights of data subjects.
C.4. Storage period/erasure procedures (includes all systems unless specified)	Personal data is stored for a maximum of six (6) years in accordance with the requirements of the Danish Bookkeeping Act (cf. Appendix D regarding Clauses 11.1 and 11.2). Upon termination of services relating to the processing of personal data, the data processor shall either delete or return the personal data in accordance with Clause 11.1, unless the data controller – after signing these provisions – has changed the original choice. Such changes must be documented and retained in writing, including electronically, in connection with the Clauses. Preparation of annual reports and tax returns on the applications Årsafslutning Professionel and Skat Professionel Nova: • For data exceptionally made available by the data processor to a sub-processor for the purpose of resolving a support task, the data is deleted by the sub-processor at the end of the month following three (3) months after the completion of the support task. Property administration on the application Unik Bolig CE / HabiCen: • Upon termination, the data processor must delete all personal data processed on behalf of the data controller no later than ninety (90) days after the termination of the service agreement, unless the data controller instructs the data processor to return all personal data no later than thirty (30) days after termination. Application Workcyclus (Workplace Assessment): • Personal data is, as standard, retained for three (3) months after the termination of the service agreement, after which it is deleted by the sub-processor. Applications zExpense (Expenses) and Azets Expense (Expenses): • Upon termination, the data controller must, within three (3) months after termination of the service agreement, export all data, including images of invoices, receipts and similar, via the application's export facility to Excel to comply with the Bookkeeping Act and/or to transfer the data to another system. Digital receipt, temporary storage, and forwarding of payslips to e-Boks A/S and/or delivery of payslips in e-Boks and mit.dk (PostNord):

	• Personal data is, as standard, stored for thirty (30) days, after which it is deleted at the sub-processor. However, the data processor has entered into an agreement with the sub-processor for the use of the "Resend function" defined with a retention period of one (1) year via the sub-processor's Connect solution. • Metadata (which may contain personal data) is deleted according to the sub-processor's standard deletion procedures after ninety (90) days. Digital receipt of payslips from PostNord Strålfors A/S and/or the data processor, temporary storage and distribution to recipients (e-Boks and mit.dk): • Personal data is retained until the payslip is transferred to the end user's digital mailbox. When the payslip is placed in the end user's digital mailbox, the sub-processor's processing of personal data on behalf of the data controller ceases. Monitoring and clearing of digital mailboxes using the application eDistribution: • Personal data is retained for ninety (90) days after distribution to the data controller's digital mailboxes, after which it is deleted. Application Addo Sign: • Personal data is, as standard, retained for forty (40) days after the document has been signed by all parties, after which it is deleted by the sub-processor. Notwithstanding the foregoing, the data processor is entitled, to the extent necessary to document the delivery of services covered by the service agreement or to defend against legal claims, to retain a copy of the data controller's personal data. In such cases, the personal data may only be processed for the stated purpose.
C.5. Processing location (includes all systems unless specified)	The processing of the personal data covered by the Provisions may not take place at any other locations than the following, without the prior written approval of the data controller, apart from the sub-processors and/or their sub-processors listed in Appendix B: • The data processor's current locations in Denmark • Home and remote workplaces (employees of the data processor and externally affiliated consultants) The applications EPOS Løn, EPOS HR, EPOS Recruitment, and EPOS Management: • The housing of the data processor's hardware is located at the data center of: ○ Global Connect A/S, Hørskætten 5, DK-2630 Taastrup, Hall 11.
C.6. Instruction on the transfer of personal data to third countries	If the data controller does not, either in these Clauses or subsequently, provide a documented instruction regarding the transfer of personal data to a third country, the data processor shall not be entitled to make such transfers within the framework of these Clauses.
C.6.1 Cloud provider and data transfer mechanism	If the data processor uses a cloud provider in connection with the provision of Services (cf. Appendix B), only data centres located within the EU/EEA may be used.
C.7. Procedures for the data controller's audits, including inspections of the processing of personal data being performed by the data processor	The data controller or a representative of the data controller shall have access to conduct inspections, including physical inspections, of the locations from which the data processor processes personal data, including physical premises and systems used for or in connection with the processing of personal data. Such inspections may be conducted whenever the data controller deems it necessary.

(includes all systems unless specified)	However, this does not apply to the data processor's home workplaces.
	
	The data controller must give the data processor at least thirty (30) days' prior notice before carrying out an inspection.
	
	If the data controller or a representative of the data controller carries out an inspection at the premises of the data processor, he or she must present valid photo identification. The individual's identity and purpose must be confirmed by the data controller's designated contact person before access to confidential information is granted.
	
	The data controller or its representative must comply with all security requirements applicable at the location.
	
	The data controller shall bear its own costs in connection with a physical inspection. The data processor is obliged, against payment, to allocate the necessary resources (primarily time) required for the data controller to carry out its inspection.
	
	The data controller has the right to carry out an annual written audit of the data processor's compliance with these Clauses if there is no annual ISAE 3000 and/or ISAE 3402 or equivalent audit report. The method for the written audit is based on a questionnaire sent by the data controller to the data processor. Depending on the scope, the written audit may be a chargeable service, which must be agreed between the parties prior to commencement.
	
	If the data controller requires information or assistance regarding security measures, documentation, or general information about how the data processor processes personal data, and such request goes beyond what is required under applicable data protection legislation, the data processor may charge a fee for such additional services.
	
	Payroll administration on the application EPOS Løn and EPOS HR in connection with BPO payroll processing in the application EPOS Løn:
	
	• The data processor may annually, at its own expense, obtain an audit report from an independent third party regarding its compliance with the General Data Protection Regulation, data protection requirements under other EU legislation, or national law of Member States, and these Clauses.
	• The parties agree that the following type of audit report (or any equivalent or replacement audit report) may be used in accordance with these Clauses for the following areas:
	  ○ BPO payroll administration on the application EPOS Løn: ISAE 3402 Type II
	  ○ EPOS HR in connection with BPO payroll processing on the application EPOS Løn: ISAE 3402 Type I
	• Audit reports must be provided to the data controller upon request without undue delay for information purposes.
	• Upon request and without undue delay, the data processor must submit a mitigation plan for any exceptions noted in the audit reports.
	• If the data controller challenges the scope and/or methodology of the audit reports and requests a new audit report under a different framework and/or with a different methodology, this shall be done against payment.
	• Audit reports are confidential and must not be shared with unauthorised parties.
	
	Payroll administration on the application Azets EPOS Løn:
	
	• The data processor may annually, at its own expense, obtain an audit report from an independent third party regarding its compliance with the General Data Protection Regulation, data protection requirements under other EU legislation or national law of Member States, and these Clauses.

	• The parties agree that the following type of audit report (or any equivalent or replacement audit report) may be used in accordance with these Clauses for the following area: ○ BPO payroll administration on the application Azets EPOS Løn: ISAE 3402 Type II (start-up year, however, Type I) • Audit reports must be provided to the data controller upon request without undue delay for information purposes. • Upon request and without undue delay, the data processor must submit a mitigation plan for any exceptions noted in the audit reports. • If the data controller challenges the scope and/or methodology of the audit reports and requests a new audit report under a different framework and/or with a different methodology, this shall be done against payment. • Audit reports are confidential and must not be shared with unauthorised parties.
C.8. Procedures for audits, including inspections of the processing of personal data being performed by sub-processors (includes all systems unless specified)	The data processor or a representative of the data processor may carry out an annual physical inspection of the sites from which sub-processors process personal data, including physical locations and systems used for or in connection with such processing, to verify the sub-processors' compliance with the General Data Protection Regulation, other EU legislation, or national laws of the Member States, and these Clauses. In addition to the annual inspection, the data processor shall carry out inspections when deemed necessary. Based on the results of the inspection, the data controller is entitled, at its own expense and risk, to request the implementation of additional measures to ensure compliance with the GDPR, other EU data protection laws, national laws, and these Clauses. The data controller may challenge the framework and/or methodology of the inspection and, in such cases, may at its own expense and risk request a new inspection under a different framework and/or method. The parties agree that the following types of audit reports or equivalent certifications may be used to verify compliance by the relevant sub-processors: Payroll Administration on the Application EPOS Løn: • ISAE 3402 Type II Datacentre (backup) • ISO/ISEC 27001 Payroll Administration on the Application Azets EPOS Løn: • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018 • AWS ISO/IEC 9001 • AWS SOC 1 Report • AWS SOC 2 Security, Availability & Confidentiality • AWS SOC 2 Confidentiality Type I • AWS SOC 3 Security, Availability & Confidentiality Payroll Administration on the Application Perspektiv including Mit Perspektiv Modules and Perspektiv Time: • ISAE 3402 Type II General IT-controls housing & firewall • ISAE 3402 Type II General IT-controls operations/capacity/network services • ISAE 3402 Type II General IT-controls application • ISAE 3000 Type II Data Processor Statement housing & firewall • ISAE 3000 Type II Data Processor Statement application Payroll and Finance Administration on the Application Azets Simplify:

	• ISAE 3402 Type II Finance Administration on the Application Visma Business: • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018 • AWS ISO/IEC 9001 • AWS SOC 1 Report • AWS SOC 2 Security, Availability & Confidentiality • AWS SOC 2 Confidentiality Type I • AWS SOC 3 Security, Availability & Confidentiality • ISO 9001 (QMS) Finance Administration on the Application e-conomic: • ISO/IEC 27001 (Data Centre) • ISAE 3000 Type II • ISAE 3402 Type II Property Administration on the Application ProBo: • ISAE 3402 Type II or • ISAE 3000 Type II Application Azets Cozone Portal/Activity/Drive/Employee: • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018 • AWS ISO/IEC 9001 • AWS SOC 1 Report • AWS SOC 2 Security, Availability & Confidentiality • AWS SOC 2 Confidentiality Type I • AWS SOC 3 Security, Availability & Confidentiality Applications EPOS Løn, EPOS HR, and EPOS Recruitment: • ISAE 3402 Type II Datacentre • ISO/IEC 27001:2013 Information Security Management System Application Workcyclus (Workplace Assessment): • Microsoft Azure SOC 2 Type II Certificate (Access Security) Application zExpense (Travel Expense Management): • ISAE 3000 Type II Application Azets Expense (Travel Expense Management): • PCI DSS Delivery of Payslips to e-Boks and mit.dk: • ISAE 3000 Type II (PostNord Strålfors A/S) • ISO 27001 and ISO 27701 (e-Boks A/S and Netcompany A/S) Application Addo Sign: • ISAE 3402 Type II (Data Centre) • ISAE 3000 Type II (Data Centre) • ISO/IEC 27001 (Data Centre) Application IMS Case (ESDH system): • ISAE 3000 Type I Application Freshdesk (Support System): • ISO/IEC 27001

	• ISO/IEC 27001 • ISO/IEC 27701 • SOC 2 Confidentiality Type II • SOC 3 Security, Availability & Confidentiality • AWS ISO/IEC 27001 • AWS ISO/IEC 27017 • AWS ISO/IEC 27018 • AWS ISO/IEC 9001 • AWS SOC 1 Report • AWS SOC 2 Security, Availability & Confidentiality • AWS SOC 2 Confidentiality Type I • AWS SOC 3 Security, Availability & Confidentiality The above audit reports shall be made available to the data controller upon request, free of charge and without undue delay, for informational purposes. The audit reports are confidential and may not be shared with unauthorised persons.

Appendix D The Parties' Terms of Agreement on Other Subjects

Appendix D.1: Supplement to the Clauses

In addition to the Clauses, the parties have agreed the following:

Regarding Clause 11.1 and 11.2:

The data processor keeps bookkeeping and accounting material in a secure manner for five (5) years from the end of the financial year to which the material relates, unless the data controller confirms in writing to take over responsibility for this.

Regarding Clause 13.1:

Liability:

The data controller shall be liable for damages caused by processing that is in violation of applicable data protection legislation.

The data processor shall only be liable for direct and documented damages caused by processing where the data processor has breached these Clauses and/or applicable data protection legislation specifically directed at the data processor's obligations.

For the avoidance of doubt, the parties agree and acknowledge that each party shall be responsible for and held liable to pay all administrative fines and damages imposed on it relating to data subjects, in accordance with applicable data protection legislation.

Regarding Clause 14.3 – Amendments to the Data Processing Agreement
The Data Processing Agreement is continuously updated in the data processor's website with new Services, adjustments made by the Danish Data Protection Agency (*Datatilsynet*) to the standard contractual clauses, and related updates to connections and version history. The latest version of the Data Processing Agreement will at all times be available in the Trust Centre and shall apply unless specific provisions have been expressly deviated from in the Service Agreement or in a written addendum to the Service Agreement. Continued use of the Services following an update to the Data Processing Agreement constitutes acceptance thereof.

Regarding Clause 14.5
As the Clauses are incorporated as an appendix to the Agreement between the parties, the present document is not separately signed by the parties.

Regarding Clause 15.2
The data controller's contact person(s) is specified in the Agreement.

Appendix D.2: Connection between Services and Personal Data

The following connection exists between the contracted Services and the personal data specified in Appendix A.3:

	Payroll Processing on the application Epos Payroll	Payroll Processing on the application Azets Epos Payroll	Payroll Processing on the application Perspektiv	Payroll Processing on the application Azets Simplify	Payroll Processing on The Data Controller' s Payroll System	Reimbursement Application	Pension Management	eKapital Reporting Employee Share Scheme	Finance Administration on the application Azets Simplify	Finance Administration on the application Visma Business	Finance Administration on the application e-conomic	Finance Administration on the Data Controllers ERP-system	Property management, including chairman assistance and related services	HR assistance	Digital monitoring and emptying of digital mailbox	SaaS application Azets Cozone Employee (exchange of data)	SaaS application EPOS Payroll	SaaS Application Azets EPOS Payroll	SaaS Applications EPOS Løn, HR, Recruitment, and Management	SaaS Application Workcyclus (Workplace Assessment)	SaaS Application Azets Expense	SaaS Application zExpense
Non-sensitive personal information, including but not limited to:																						
Employee name, employee number, and organizational affiliation	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Employment start- and end date	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Contact information, including name, telephone number, email address, title, and address	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Name and contact information of the employee's next of kin	+	+	+	+	+	-	-	-	-	-	-	-	+	-	-	-	+	+	-	-	-	-
Date of birth, gender, and marital status	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-
Salary information and working hours	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-
Pension, banking, and tax information, including ATP contributions and social security contributions	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+	-	-	-	-
Time and absence information, including: - illness, child's illness, parental leave, military service, public duties, periodic employment, etc. - vacation and leave (including extra leave, care days, etc.) - information regarding Section 56 agreements and partial return-to-work or partial sick leave arrangements	+	+	+	+	+	+	-	-	+	+	+	+	+	+	+	+	+	+	-	-	-	-
Salary supplements, including travel expenses, mileage reimbursement, etc.	+	+	+	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	-	-	-	-
Salary deductions, including canteen expenses, employee purchases, unemployment insurance contributions, etc.	+	+	+	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	-	-	-	-
Project registrations	+	+	+	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	-	-	+	+
Vehicle registration number associated with the employee	+	+	+	+	+	-	-	-	+	+	+	+	+	+	+	-	+	+	-	-	+	+
Driven kilometres, including route (GPS data)	+	+	+	+	+	-	-	-	+	+	+	+	+	-	-	-	+	+	-	-	+	+
Electronic expense claims/travel reimbursements	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	-	-	-	-	-	+	+
Devices and access rights assigned to the employee	+	+	+	-	-	-	-	-	+	+	+	+	+	+	-	-	+	+	-	-	-	-
Courses attended by the employee and other competencies	+	+	+	-	-	-	-	-	-	-	-	-	-	+	-	-	+	+	+	-	-	-
Contracts and other employment-related documents (e.g., notes from probationary interviews, warnings, terminations, etc.)	-	-	+	-	-	-	-	-	+	+	+	+	+	+	-	-	-	-	+	-	-	-+
Performance and development review action plans	-	-	+	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-

	Payroll Processing on the application Epos Payroll	Payroll Processing on the application Azets Epos Payroll	Payroll Processing on the application Perspektiv	Payroll Processing on the application Azets Simplify	Payroll Processing on The Data Controller' s Payroll System	Reimbursement Application	Pension Management	eKapital Reporting Employee Share Scheme	Finance Administration on the application Azets Simplify	Finance Administration on the application Visma Business	Finance Administration on the application e-conomic	Finance Administration on the Data Controllers ERP-system	Property management, including chairman assistance and related services	HR assistance	Digital monitoring and emptying of digital mailbox	SaaS application Azets Cozone Employee (exchange of data)	SaaS application EPOS Payroll	SaaS Application Azets EPOS Payroll	SaaS Applications EPOS Løn, HR, Recruitment, and Management	SaaS Application Workcyclus (Workplace Assessment)	SaaS Application Azets Expense	SaaS Application zExpense
Files uploaded by the data controller's candidates containing personal data, including applications, CVs, diplomas and course certificates, expected salary requirements, etc.	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-
Payment information	-	-	-	-	-	-	-	-	+	+	+	+	+	+	+	-	-	-	-	-	+	+
Images as well as IP and cookie information uploaded by the data controller	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-	-
Passport information, health insurance card information, and similar identification documents	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	-	-	-	-	-
Debt collection information, including RKI registration	-	-	-	-	-	-	-	-	+	+	+	+	+	-	+	-	-	-	-	-	-	-
Information otherwise included in communications with potential or existing shareholders, tenants, subtenants, residents, and owners, etc.	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-
Other membership data in housing associations/rental properties, including household size, tenancy history, waiting list registrations, consumption data (such as water, heating, and electricity), etc.	-	-	-	-	-	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-
Sensitive personal data, including but not limited to:																						
Absence information containing health data, including information about maternity/paternity leave periods	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-
Health information in the form of electronic attachments	-	-	-	+	-	-	-	-	+	+	+	+	+	+	+	-	-	-	-	-	+	+
Information on physical and mental work environment, including social capital	-	-	+	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	-	+	-	-
Documentation of the mandatory workplace health and safety discussion	-	-	+	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-
Action plans at all organizational levels	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-
Information about private matters, such as financial and social circumstances	+	+	+	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	+	+	-	-
Trade union affiliation, including salary deductions for union membership fees	+	+	+	+	+	-	-	-	+	+	+	+	+	+	+	-	+	+	+	-	-	-
Criminal matters	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	+	-	-	-
Confidential personal data:																						
CPR number	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	+	+

Appendix D.3: Connection between Services and categories of data subjects

The following connection exists between the contracted Services and the categories of data subjects specified in Appendix A.4:

	Payroll Processing on the application Epos Payroll	Payroll Processing on the application Azets Epos Payroll	Payroll Processing on the application Perspektiv	Payroll Processing on the application Azets Simplify	Payroll Processing on The Data Controller' s Payroll System	Reimbursement Application	Pension Management	eKapital Reporting Employee Share Scheme	Finance Administration on the application Azets Simplify	Finance Administration on the application Visma Business	Finance Administration on the application e-conomic	Finance Administration on the Data Controllers ERP-system	Property management, including chairman assistance and related services	HR assistance	Digital monitoring and emptying of digital mailbox	SaaS application Azets Cozone Employee (exchange of data)	SaaS application EPOS Payroll	SaaS Application Azets EPOS Payroll	SaaS Applications EPOS Løn, HR, Recruitment, and Management	SaaS Application Workcyclus (Workplace Assessment)	SaaS Application Azets Expense	SaaS Application zExpense
Current and former employees	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Fee recipients	-	-	+	-	-	-	-	-	-	-	-	-	-	+	+	+	-	-	-	-	-	-
Prospective employees	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	+	-	-	-
Customers, suppliers, and other business partners	-	-	-	-	-	-	-	-	+	+	+	+	+	+	+	-	-	-	-	-	+	+
Members of housing associations (cooperative housing associations, owners' associations, homeowners' associations, and similar), as well as housing association's employees, board members, tenants/residents/subtenants, suppliers, and other business partners	-	-	-	+	-	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-
Owners of rental properties/tenancies and their employees, board members, tenants/residents/subtenants, suppliers, and other business partners	-	-	-	+	-	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-

Appendix D.4: Connection between Services and approved sub-processors

The following connection exists between the contracted Services and the approved sub-processors listed in Appendix B.1:

	Payroll Processing on the application Epos Payroll	Payroll Processing on the application Azets Epos Payroll	Payroll Processing on the application Perspektiv	Payroll Processing on the application Azets Simplify	Payroll Processing on The Data Controller' s Payroll System	Reimbursement Application	Pension Management	eKapital Reporting Employee Share Scheme	Finance Administration on the application Azets Simplify	Finance Administration on the application Visma Business	Finance Administration on the application e-conomic	Finance Administration on the Data Controllers ERP-system	Property management, including chairman assistance and related services	HR assistance	Digital monitoring and emptying of digital mailbox	SaaS application Azets Cozone Employee (exchange of data)	SaaS application EPOS Payroll	SaaS Application Azets EPOS Payroll	SaaS Applications EPOS Løn, HR, Recruitment, and Management	SaaS Application Workcyclus (Workplace Assessment)	SaaS Application Azets Expense	SaaS Application zExpense
Azets Insight SRL	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-
Azets Insight AB	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Azets Insight AS: Azets Invoice/Reporting	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-
Azets Insight AS: Visma Business	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-
Azets Labs A/S: Azets EPOS Payroll	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-
Azets Labs A/S: Workcyclus APV products	-	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	+	-	-
Azets Perspektiv A/S	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Azets Software AB	+	+	-	+	+	+	+	+	+	+	+	+	+	-	-	+	-	-	-	-	-	-
e-Boks A/S	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-
EG Danmark A/S: EG Bolig	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-
Findity AB	+	+	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-	-	+	-
Freshworks Inc.	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
PostNord Strålfors A/S: Digital distribution of payslips	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-
PostNord Strålfors A/S: e-Distribution solution	-	-	-	+	+	-	-	-	+	+	+	+	+	-	+	-	-	-	-	-	-	-
Twoday Danmark A/S	-	-	-	-	-	-	-	-	+	+	+	+	+	+	-	-	-	-	-	-	-	-
Unik System Design A/S	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-
Visma e-conomic A/S	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-
Visma IMS A/S	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-
Wolters Kluwer Danmark A/S	-	-	-	-	-	-	-	-	+	+	+	+	+	-	-	-	-	-	-	-	-	-
Zebon ApS	+	+	-	-	-	-	-	-	-	+	-	+	-	-	-	-	-	-	-	-	-	+
Zenegy Danmark ApS	-	-	-	+	-	-	-	-	+	-	-	-	+	-	-	-	-	-	-	-	-	-

Appendix E Change Log

Version	Change
1.2 Amended by The Danish Data Protection Agency	Amendments to Clause 7.6 *(The clause has been made optional, and the wording has been modified).*
2.0 Amended by Azets Insight 1st May 2025	• Changed placement of background and purpose • 7.2: Selection of option 2 • 7.3: Selection of option 2 and a minimum of two (2) weeks • 7.6: Deselection of optional Clause • 9.2: Selection of supervisory authority (Danish Data Protection Agency) • 10.2: Selection of 48 hours, if possible • 11.1: Selection of option 2 • 11.2: Addition of the Danish Bookkeeping Act • Appendix A–C adjusted according to the processing activities • Appendix B: Deselection of optional section B.2 • Appendix D: Adjusted specifically for the data processor • Appendix E: Version history added