ZENEGY

DATA PROCESSING AGREEMENT

Standard Contractual Clauses

pursuant to Article 28(3) of Regulation 2016/679 (the General Data Protection Regulation – "GDPR") for the purpose of the data processor's processing of personal data.

Between

Name
Cvr no
Address
ZIP code and city
Country

(hereinafter 'the data controller')

and

Zenegy Denmark ApS
CVR No: 38366041
Slotsmarken 16
2970 Hørsholm

(hereinafter 'the data processor')

each a 'party'; together 'the parties'

HAVE AGREED on the following 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.

ZENEGY

1. Table of Contents

2. Preamble

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. 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).

3. In the context of the provision of the services listed in Appendix E, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

5. Five appendices are attached to the Clauses and form an integral part of the Clauses.

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.

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.

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.

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

10. Appendix E provides an overview of the subscription-based services that the data controller purchases from the data processor.

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

12. These 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.

3. The rights and obligations of the data controller

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

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 these Clauses shall be understood as references to "EEA Member States".

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

4. The data processor acts according to instructions

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.

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.

5. Confidentiality

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.

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.

6. Security of processing

1. Article 32 of the 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.

2. According to Article 32 of the 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.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 of the 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 of the GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 of the 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 of the GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

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

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.

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 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.

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.

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.

6. If the sub-processor does not fulfil its 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 of the GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

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 of the GDPR.

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.

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 organisation

    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

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 of the GDPR on which they are based, shall be set out in Appendix C.6.

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

9. Assistance to the data controller

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 of the 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

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.4., 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, no later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority in the country where the controller is based 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 in the country where the controller is based, 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.

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.

10. Notification of personal data breach

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.

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 of the GDPR.

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.

4. The parties shall define in Appendix D 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.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so, cf. Appendix A.5, unless Union or Member State law requires the storage of the personal data.

12. Audit and inspection

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.

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.

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.

13. The parties' agreement on other terms

1. The parties may agree on 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.

14. Commencement and termination

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

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.

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.

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.

15. Signature

On behalf of the data controller

Name
Position
Telephone
Email
Signature

On behalf of the data processor

Name	Jes Tækker Stemann Brinch
Position	CEO
Telephone	+45 70 22 22 16
Email	jes@zenegy.com
Signature	

16. Data controller and data processor contacts/contact points

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

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

   With the data controller

   Name
   Position
   Telephone
   Email

   With the data processor

Name	Kristian Haagensen
Position	Product manager
Telephone	+45 70 22 22 16
Email	kristian@zenegy.com

ZENEGY

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 is:

On a subscription basis, the data processor makes available the cloud-based services ("Services") selected by the data controller according to Appendix E to the data controller and its employees. The Services can be accessed partly via the data processor's website, www.zenegy.com, and partly via the data processor's app.

The data controller's use of the data processor's cloud-based Services is done by the data controller's self-service via the data processor's website, and/or via the data processor's app. The data processor's employees can also access their own information, such as payslips, absence statements, holiday statements, and the documents that the employee or customer has entered, such as employment contracts. The use of both the data controller and its employees requires a user ID and a unique password.

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):

Storage and execution of payroll administration, HR administration, as well as bookkeeping/accounting, including administration of payroll, reimbursement of expenses, driving accounts, time registration, registration of holidays, absence registration and the like.

A.3. The processing includes the following types of personal data about data subjects:

The personal data processed by the data processor in connection with the data controller's use of the data processor's Services differ according to the category to which the data subject belongs, cf. the following overview:

CATEGORIES OF DATA SUBJECTS	**Personal data**
Customers	• Contacts of the data controller, including their contact information, such as telephone, email, title, department, address • Bank accounts for use by the Application • Member of any employers' association • Member of holiday arrangements
Current and former employees of the controller	• Name • Address • Civil registration number • Contact information, including telephone, email, position, department, address • Name and contact details of employees' relatives • Salary • Tax and tax credits • Labour market contributions • ATP contribution • Social contributions • Pension contributions • Absence (e.g. due to illness, maternity, military service, civic duty, periodic appointments, etc.) • Statement of holidays • Allowances (e.g. employee travel expenses, driving allowance, etc.)

	• Deductions (including the data controller's expenses, union dues, unemployment insurance fund contributions, early retirement contributions, etc.) • Hour/time registrations • Registration of entities and accesses assigned to the employee • Overview of courses the employee has participated in • Bank accounts to use for payroll • Uploaded documents (e.g. employment contract, employee development interviews, criminal record, etc.)
Partners - Support	• Name • Address • CVR number • Contact information • Support contacts, including their contact information, such as telephone, email, position, department, address
Partners - Payroll Administrators	• Name • Address • CVR number • Contact information • Administrator contacts, including their contact information, such as telephone, email, position, department, address

A.4. Processing includes the following categories of data subject:

See the overview in section A.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 Processor's processing of personal data on behalf of the Data Controller continues as long as the Data Controller makes use of the Services provided by the Data Processor to which the Data Controller subscribes, cf. Appendix E.

At the termination of the subscription agreement, the data controller will have the choice between whether data should be deleted after 7 days or whether the data controller wants to store and access data for 6 months. If, before the end of a selected 7-day or 6-month period, the data controller continues to want data stored by the data processor, the data controller must reactivate the subscription.

If an employee's association with the data controller ends, the employee will continue to have access to her/his information until the data controller chooses to delete the information. Upon the data controller's decision to delete the information, the employee receives an offer for continued storage of the employee's own information under a separate data storage agreement.

Appendix B 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	ADDRESS	DESCRIPTION OF PROCESSING
Send in Blue	Registration number 498 019 298	Send in blue 55 rue d'Amsterdam, 75008 Paris, France	Newsletters Notifications Onboarding Reset of passwords
Dixa	CVR 36561009	Vimmelskaftet 41A, 1 Sal. 1161 Copenhagen Denmark	Customer support Ticket system
Upodi	CVR 38558862	Upodi ApS Åbogade 25, 8200 Aarhus N	Fakturering af Zenegy kunder
Microsoft Azure	IE8256796U	Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	Data hosting and data processing
MSA Dooel	[To be completed by Zenegy]	M.T. Gologanov 40 1000 Skopje Macedonia	Software development, system maintenance, and technical debugging
Zenegy ApS	37233994	Slotsmarken 16, 2970 Hørsholm	Operation, support, and development of the Application

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 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

See Clause 7.3.

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:

When the data controller uses the cloud-based **Zenegy Payroll** – whether such use is made by the data controller or a payroll administrator appointed by the data controller – the data processor processes personal data concerning the data controller's employees in connection with the data controller's payroll administration for own employees, including payroll run execution, holiday and absence, driving and time registration, reporting to SKAT and other public authorities.

When the data controller uses the cloud-based **Zenegy HR** – whether such use is made by the data controller or an administrator appointed by the data controller – the data processor processes personal data concerning the data controller's employees in connection with the data controller's HR administration for own employees, including administration of devices and access assigned to the individual employee, course administration, handling of the employee's expenses on behalf of the data controller, and storage of documents, such as employment contract.

When the data controller uses the cloud-based **Zenegy ERP** – whether such use is made by the data controller or an administrator designated by the data controller - the data processor processes personal data concerning the data controller's employees, customers and partners in connection with the data controller's accounting and bookkeeping activities.

When the data controller uses the cloud-based **Zenegy Expense** – whether such use is made by the data controller or an administrator designated by the data controller – the data processor processes personal data concerning the data controller's employees, customers and partners in connection with the data controller's expense management activities.

The data controller and/or its employees shall enter the information necessary for the use of the Services. Also, the data controller instructs Zenegy to obtain information continuously and automatically from relevant authorities to ensure that the information used about employees' conditions is up to date when the Services are used.

The Services are designed with an open API that enables others to develop and offer apps that can communicate with the Application, including sharing information across applications ("Third Party App(s)"). To the extent that the data controller chooses to install and make use of Third-Party Apps that can communicate with the Application, it is considered to be an instruction to Zenegy that there may be a transfer of the information entered into the Application and the information generated by the Application to such Third Party Apps.

Furthermore, the data controller accepts that its Employees have the ability to install and make use of Third-Party Apps that can communicate and exchange each employee's information with the Application, and that such data processing is subject to the instruction under this agreement.

The data controller gives similar instructions that the data controller's employees can also choose to install and make use of Third Party apps that can communicate with the Application and instruct Zenegy that in such case the information entered/loaded in the Application and generated by the Application to which the employee has access to, may be transferred to such Third Party Apps.

Zenegy is entitled to process the personal data specified in Appendix A.3 for its own purposes as an independent data controller upon the termination of the subscription agreement with the data controller.

Zenegy is also entitled to store the personal data specified in Appendix A.3 for the purpose of being able to send out newsletters and notify of new circumstances at Zenegy, if the person concerned has consented to this; anonymise the information for statistical purposes, and process the information as required by law, including in connection with a legal decision, regulatory requirements, the bankruptcy of the data controller, death or the like.

Please also refer to the agreed terms of Zenegy's subscription terms.

C.2. Security of processing
The level of security shall take into account:

The processing of data includes personal data covered by Article 9 of the General Data Protection Regulation on specific categories of personal data, which is why a high level of security has been established.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

However, the data processor shall – in any event, and at a minimum – implement the following measures that have been agreed with the data controller:

Service and database location

Zenegy has physically separated its production (Zenegy Production) and testing (Zenegy Beta) databases.

Zenegy Beta is located in North Europe - Dublin - Ireland

Zenegy Production is located in West Europe - Amsterdam - Netherlands

More information about Azure locations can be found here: https://azure.microsoft.com/da-dk/global-infrastructure/regions/.

Data encryption

Data is encrypted both during transport and "at rest".

Database availability

Data is stored in Azure. IP must be manually added to Azure to access and expires after two hours.

Access is limited to very few users.

Passwords

Passwords are SHA256 encrypted with a unique salt.

Backup

Zenegy uses Azure to host its application and API. The backup policy is set to preserve 5 previous versions.

Zenegy uses Azure to host its database. The backup policy is set to take a full backup every week.

Also, the "Point-in-time" backup function is set up so that the database can be restored at any time 35 days back in time.

More information about Azure continuity can be found here: https://azure.microsoft.com/en-us/updates/point-in-time-restore-retention-for-standard-edition-extended-to-35-days/.

Third-party and supplier risk assessment

Zenegy provides annual reviews of its suppliers and third parties.

This is done specifically by reviewing data processor agreements for individual suppliers, a risk assessment, and a scope assessment.

Risk and scope are divided into three categories:

Risk

Low risk

- 5 people or fewer have access to the resource
- Complex passwords are required to access the resource
- Two factor authentication and/or certificate-based access is required to access the resource

Medium risk

- More than 5 people have access to the resource
- Data may originate from multiple sources
- Zenegy does not have full control over data
- Complex passwords and/or two factor-authentication are required to access the resource

High risk

- More than 5 people have access to the resource
- Simple access codes are required to access the resource

Extent

Low scope

- The extent of a data leak is low
- Example: Unidentifiable information, not sensitive information

Medium scope

- The extent of a data leak is medium
- Example: Identifiable information, such as names, addresses, and emails.

High scope

- The extent of a data leak is great
- Example: Usernames and passwords, health information, civil registration numbers, religious and union affiliations.

User's access to data via browser

Accessible over the Internet via a web browser that supports HTTPS.

Zenegy has implemented an option for owners of a Zenegy account to maintain passwords that comply with ISO 27001.

Zenegy has implemented an option for owners of a Zenegy account to implement two factor authentication.

All of Zenegy's internal users access Zenegy with all security features turned on.

User access to data through API

Zenegy makes available a REST API.

Access is managed on several levels.

- A user of the API cannot access more than the role that the user has in Zenegy.
- Zenegy uses the industry-standard OAuth 2.0.
- Apps are limited by the uri that is added when created.
- Apps can only access Zenegy data via HTTPS.
- Apps may have additional limitations in the form of Scopes created when the App is created.

More information about OAuth 2.0 can be found here: https://aaronparecki.com/oauth-2-simplified/

Physical access to Zenegy facilities

Zenegy is operated as a closed facility, although no information is processed physically.

All visitors are logged.

All keys are system keys that cannot be copied.

Keys are regularly accounted for in connection with termination and appointments with annual checks where employees must physically present their keys.

Work from home

Employees have the opportunity to work from home.

All computers are encrypted and protected by access codes.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing such technical and organisational measures, which 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

Data is stored for as long as the data controller finds that it fulfils the purpose of the data controller.

Zenegy makes features available to the data controller so that the data controller can live up to those purposes.

If the data controller terminates its agreement with Zenegy, Zenegy has built functionality that enables the export and deletion of data in two ways – the chosen way depends on the data controller's detailed instructions:

- ☐ Export all data and delete data within 7 days
- ☐ Export all data and delete data within 6 months

Zenegy packages all data digitally so that the data controller has the opportunity to download and transfer data to another system.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

See C.2. Security of processing - Service and database location

C.6. Instruction on the transfer of personal data to third countries

The data controller is aware of – and is obligated to make its employees aware – that the data processor's Services are made available through a cloud-based solution where the data processor makes use of software and IT systems, among other things, including servers provided by third parties.

To the extent that the data processor's Services make use of or are based on services provided by sub-processors in third countries, the data controller hereby instructs and authorises the data processor to transfer personal data to the data processor's sub-processors in such third countries for the purpose of the data processor's provision of the Services to which the data controller subscribes to from the data processor, in accordance with Appendix E.

The use of sub-processors in third countries must be subject to similar provisions to the provisions agreed between the data controller and the data processor, and the data processor is obliged to ensure that the transfer and data processing is carried out in accordance with applicable EU standard clauses for the transfer of personal data (EU standard contractual clauses).

In its agreement with sub-processors, the data processor shall include the data controller as a third-party beneficiary in the event of the data processor's bankruptcy, so that the data controller can enter into the data processor's rights and assert them against sub-processors, cf. Clause 7.6.

The transfer to third countries is carried out in accordance with the European Commission's standard contractual clauses on data protection. The data controller hereby authorises the data processor to enter into a relationship with the sub-processors of data in the third countries concerned on behalf of the data controller, based on the EU Commission's standard contractual clauses on the transfer between a data controller in the EU to a data processor outside the EU.

If the data controller not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

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 processor shall from February to June at the data processor's expense obtain an auditor's report] from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and these Clauses.

The parties have agreed that the following types of auditor's report] may be used in compliance with these Clauses:

- ISAE 3402

The auditor's report shall without undue delay be made publicly available on the data processor's website, www.zengy.com, to the data controller for information.

The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology at its own expense and risk.

Based on the results of such an audit, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor shall give the data controller or a representative of the data controller access to carry out an annual inspection, including physical inspection, of the sites from which the data processor processes personal data, including physical sites and systems used for or in connection with the processing. Such an inspection is carried out annually when the data controller convenes for the possibility of inspection, typically on a date in September or October.

The data controller's and the data processor's costs, if applicable, relating to an inspection shall be borne by the data controller, cf. Appendix D.

Clause 12.1. The data processor shall be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor or the data processor's representative shall have access to an annual physical inspection of the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing to ascertain the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data processor may perform an inspection of the sub-processor when the data processor deems it required.

Documentation for such inspections shall without undue delay be submitted to the data controller for information.

The data controller may contest the scope and/or methodology of the report and may in such cases at its own expense and risk request a new inspection under a revised scope and/or different methodology.

Based on the results of such an inspection, the data controller may its own expense and risk request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller may at its own expense and risk elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor's and the sub-processor's costs related to a physical inspection at the sub-processor's facilities shall not concern the data controller unless the inspection is initiated by the data controller, cf. Clause 12.1 of Appendix D.

Appendix D The Parties' agreement on other matters

The Parties have agreed on the following supplements for the Clauses:

For Clause 4.2

Notwithstanding Clause 4.2, the data processor is not obliged to actively verify or examine the legality of the data controller's instructions.

To the extent that the data controller gives instructions to the data processor, which subsequently proves to be unlawful, the data controller shall be obliged to indemnify the data processor from any loss resulting therefrom, including indemnifying the data processor of any claim against the data processor resulting therefrom, including any penalty or other sanctions imposed by relevant authorities, as well as claims from other third parties, including the data subjects concerned, sub-processors, and the data processor's other partners.

For Clause 7.3

The data controller acknowledges that the data processor's Services are standardised, cloud-based subscription services made available to a large number of customers and that the data processor is therefore not able to design the systems offered in such a way that each customer may require the data processor not to make use of specific sub-processors approved by the data processor.

Thus, the data controller acknowledges that if the data controller objects to the data processor's change or choice of new sub-processors and the data processor does not accommodate such an objection, the data controller's sole remedy is to terminate the subscription agreement with the data processor. The termination may take place with immediate effect, and neither party shall have any claim against each other in this connection.

For Clause 9.2

To the extent that the data controller wishes the data processor assistance to the services described in Clauses 9.2, (c) and (d), the data controller is obliged to remunerate the data processor for the time spent with the hourly rates used by the data processor at all times, as shown on the data processor's website.

For Clause 12.1

The data processor is obliged to allocate the resources necessary for the data controller or its adviser/representative to carry out its inspection and/or audit by the data processor or its sub-processors. "The costs incurred by the data processor in connection with a physical inspection and/or an audit carried out by the data processor or its sub-processors shall be borne by the data controller. The time of the data processor and/or its sub-processors shall be reimbursed with the hourly rates used by the data processor at all times, as shown on the data processor's website."

For Clause 13.1

The data processor's liability to the data controller is limited to what is set out in the subscription terms just as the other provisions of the subscription terms shall apply between the data controller and the data processor, except to the extent that they impair the fundamental rights and freedoms of the data subject under the General Data Protection Regulation.

Appendix E Overview of the services offered by the Data Processor to which the Data controller subscribes.

A description of each Service is listed on the Data Processor's website, www.zenegy.com.

Service	Description
Zenegy Payroll	Zenegy provides cloud-based payroll services to companies of all sizes. The service assists and automates many complicated payroll administration processes by keeping track of absence, hourly, driving, and supplementary and deduction registrations, including approval flow for the registrations as mentioned earlier as well as the payroll run execution. Zenegy provides an overview of employees, departments, relatives, pension agreements, payments, and reporting to Skat. Utilising a role system, Zenegy ensures role separation for the different user types. Zenegy logs all user actions in the system so that digital audits can be performed. Through a reporting module, Zenegy allows users to pull relevant reports on the various functions.
Zenegy HR	Zenegy provides certain cloud-based HR-solutions for companies of all sizes. The solution is a collection of several different products, that support the company's processes, including a device and access module, that helps the company manage the release and return of material and tools, and create access and delete them. Also, the solution includes a module for managing and signing up for both physical and virtual courses and events. The solution also includes a template- and document module. The template module helps your organisation maintain and create documents in the form of contracts or agreements. The document module allows you to upload documents on to each employee, such as employment contracts or employee development interviews. Users with the permitted access rights can also share documents with all employees in a company, for example, employee handbooks or workplace assessments.
Zenegy ERP	Zenegy provides cloud-based accounting solutions for companies of all sizes. The solution is an accounting system for invoicing customers, posting expenses and revenue. The solution contains several modules in the form of product, customer and supplier files, chart of accounts, diaries, VAT handling, dimensions, unit system, payment overviews, currency handling and exchange rates as well as income year.
Zenegy Expense	Zenegy provides cloud-based expense solutions for companies of all sizes. The solution enables the handling of employee credit/debit cards as well as the handling of supplier expenses. Also, the solution includes setting up approval flow as well as a posting solution for posting and categorising expenses.
Zenegy Storage	Zenegy offers a cloud bases opportunity for employees of the data controller to store their data in the Application after the end of the subscription agreement or after an employee's association with the data controller has ended.

17. Version

VERSION	ÆNDRINGER
1.2 – 05.03.2021	Updated: - Version added - Footer updated - Better layout to umprove readability - Bilag B – Subprocessors updated - Bilag C, C1 - Formål præciseret
2021-6-1.0	Updated - Subproccesors updated