

## **wehowsky.com standard Data Protection Agreement**

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

IT Relation A/S  
CVR 27001092  
Dalgas Plads 7B, 1. 2.  
7400 Herning  
Denmark

(the data controller)

and

wehowsky.com ApS  
CVR 37783110  
Saantesvej 13  
2820 Gentofte  
Denmark

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

**1. Table of Contents**

2. Preamble..... 3

3. The rights and obligations of the data controller ..... 3

4. The data processor acts according to instructions..... 4

5. Confidentiality ..... 4

6. Security of processing..... 4

7. Use of sub-processors ..... 5

8. Transfer of data to third countries or international organisations ..... 6

9. Assistance to the data controller ..... 7

10. Notification of personal data breach ..... 8

11. Erasure and return of data ..... 8

12. Audit and inspection..... 8

13. The parties' agreement on other terms ..... 9

14. Commencement and termination ..... 9

15. Data controller and data processor contacts/contact points ..... 10

Appendix A Information about the processing ..... 11

Appendix B Authorised sub-processors ..... 12

Appendix C Instruction pertaining to the use of personal data ..... 12

Appendix D The parties' terms of agreement on other subjects ..... 16

## 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 *Wehowsky Partner Contract Agreement and Customer Contract*, 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. Four 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. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
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.

## 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 GDPR), the applicable EU or Member State<sup>1</sup> data protection provisions and the Clauses.

---

<sup>1</sup> References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

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

#### **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 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 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 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.

## 7. Use of sub-processors

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).
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 3 months in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The data controller must notify the data processor within 7 days of receiving the notice. 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. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.
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.

## 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 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 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
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.

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.

## 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 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 6.3., 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, Datatilsynet (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, Datatilsynet (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.

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 24 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.
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 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.

## 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 unless Union or Member State law requires 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.

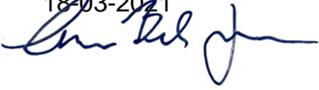
### 13. The parties' agreement on other terms

1. The parties may agree 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.
5. Signature

On behalf of the data controller

Name Frank Beck Jensen  
Position Head of Compliance and Security  
Date 18-03-2021  
Signature 

On behalf of the data processor

Name Andreas Wehowsky

Position	CEO
Date	18/3-2021
Signature	<i>Andreas Wehowsky</i>

## 15. 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.

Name	Frank Beck Jensen
Position	Head of Compliance and Security
Telephone	40906035
E-mail	frbec@itrelation.dk

Name	Emil Lynge
Position	DPO
Telephone	+45 21 24 24 87
E-mail	info@wehowsky.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 is:**

That the data controller as well as the data processor can monitor notifications from MUNINN via wehowsky.com (the data processor's) cloud platform and do incident response and reporting. Monitoring requires collection and processing of information, including data that could be related to a person (for example an IP address).

### **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):**

That the data processor is able to do incident response and investigation in response to sign of hacker attacks or the like in the data controller's own IT systems.

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

IP addresses, MAC-addresses and hostnames of computer in the data controller's own computer network.

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

Selected employees with the data processor and other persons who have access to the data controller's computer network.

### **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 processing is solely active in relation to monitoring of and incident response to concrete and critical notifications from MUNINN and lasts until the agreement is terminated or cancelled by one of the parties.

**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	ADDRESS	DESCRIPTION OF PROCESSING
Amazon AWS		Ireland	Amazon solely provides servers and network to ensure the operation of the Wehowsky.com Cloud Platform and cannot access the data of the data controller.

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.

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

As noted in section 7.3, the data processor must notify the data controller of changes to sub-processors in order to enable the data controller to object to such changes. Such a notification must be received by the data controller at least 3 months before the use or change of sub-processors is due to take effect. If the data controller has objections to the changes, the data processor must be informed within 7 days of receipt of the notification. The data controller may only object if the data controller has reasonable, concrete reasons for this.

**Appendix C Instruction pertaining to the use of personal data**

**C.1. The subject of/instruction for the processing**

Processing of personal information derives from a normal procedure for incident response. 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:

- The data processor looks at a notification from MUNINN and follows an established procedure for incident response. In order to investigate a hacker attack, the data processor can fetch log events and recorded network data from a MUNINN sensor and process it using the cloud platform. When collected and processed network data at the data controller algorithmically by the data processor's software is deemed relevant to the security level of the data controller's network, a high-level description of the event is automatically sent to the data processor for storage.
- When the data controller in using the data processor's cloud platform wishes to further analyse events, network data is sent for storage with the data processor.
- When preparing a network analysis on the data controller's request, network data is sent for analysis on the data processor's cloud platform. The analysis implies:
  - Linkage of IP-addresses, MAC-addresses and hostnames for electronic equipment on the data controller's network. From now on jointly referred to as "machines"
  - Linkage of events to machines
  - Linkage of used software with machines

## C.2. Security of processing

The level of security shall take into account:

- That data collection on hardware with the data controller does not discriminate between sensitive and non-sensitive data, and that it is not known what kind of data is collected. Thus, **all** data collected this way be considered highly sensitive, until it has been confirmed this is not the case. This results in the highest level of security for all processes at the data processor touching upon this type of data.
- That event data sent to storage with the data processor contains IP addresses which is potentially linked to visited domains and timestamps. As IP addresses are considered relatable to personal data, the security level for transmission, storage and access to events must reflect this fact.

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.

The data processor's cloud platform can only be accessed by users which have been approved by the data controller. The MUNINN sensor cannot be accessed from the internet, as it runs within the data controller's firewall, unless the data controller has arranged other installation.

If the data controller wishes to access MUNINN from the internet, it is ensured that:

- MUNINN can only be accessed if the user has access to one of the certificates issued by the data processor and linked specifically to the sensor in question.
- That the access is always time limited in order to decrease the attack surface.

- That all traffic between the user and MUNINN is encrypted in every link.
- That all use of this service is recorded in an access log which can be handed over on the data controller's request.

All data is transmitted encrypted and using two-way certificate exchange in order to ensure mutual trust between MUNINN sensors, the cloud platform, users of the cloud platform and internally between services in the cloud platform.

Data is protected on the cloud platform using multiple layers of protection and with strict procedures for access control.

Physical locations are protected with access control and access to rack servers in server rooms.

Home workplaces are not used for the purpose of processing data controller's data.

All user access and system access to the data processor's cloud platform and MUNINN sensors, as well as the internal IT systems of wehowsky.com are audit logged.

### **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 the following technical and organisational measures:

- Full audit logs and documentation of 1) procedures and 2) processing of data in concrete cases

### **C.4. Storage period/erasure procedures**

Raw network data, which in accordance with C.2 is considered highly sensitive data, is stored only on premise on the MUNINN sensor unless actively requested by the data controller. Sensitive data is stored until the sensor's capacity for raw data is full, after which the oldest data is deleted. This time window does not have a limit, but data is deleted after at most 30 days. The time period for which raw network data currently exists can be monitored from the MUNINN sensor status window.

Data sent to the data processor's cloud platform is stored for 14 days at most.

Regarding the high-level descriptions of events, they are stored on the data processor's cloud platform until the cooperation with the data controller is stops.

Regarding data processed in relation to incident response, they are stored until the data controller considers the incident handled. Furthermore, all open cases of this type are reviewed every 14 days in order to re-evaluate the need for storing data.

The data controller is responsible for the security and storage policy for all data downloaded from the data processor's cloud platform and/or the MUNINN sensor.

### **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:

- On hardware under the physical control of the data controller.
- On EC2 servers in the region EU-West-1 under the control of Amazon Web Services.
- ( In the data processor's offices protected as stated in C.2 )

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

- Under normal operations, data will not be transferred to a third country as data is not stored on servers outside the EU. Since the sub-processor could choose to transfer data under some circumstances, the data controller hereby gives the data processor an explicit instruction to transfer personal data to third countries, namely on Amazon EC2 servers in the region EU-West-1 under the control of Amazon Web Services. See section A.3. on the types of personal data that could be transferred.

The data controller has by signing the Clauses approved the use of Amazon Web Services and instructed the data processor to transfer personal data to third countries by using Amazon Web Services for the delivery of the Services.

The legal basis for transferring personal data to third countries is the EU Commission's Standard Contractual Clauses in force (SCC). The data processor and the approved sub-processor(s) are authorized to enter into the SCC on the behalf of the data controller. The data controller will be considered as the Data Exporter as stated in the SCC. When personal data is transferred to the approved sub-processor(s), The data controller agrees to be obligated by the obligations for the data exporters in accordance with the SCC.

### **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 may perform inspection, including physical inspection, at the data processor, when a need arises based on the data controller's assessment.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, 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**

Refer to the Amazon Web Services terms and conditions.

## **Appendix D The parties' terms of agreement on other subjects**

### **D.1. Compensation**

All support provided to the data controller by the data processor is settled as consultant hours, cf. the price sheet of wehowsky.com.