Done at Brussels, 4 June 2021

C(2021) 3701 final

Annex

Annex

of

COMMISSION IMPLEMENTING DECISION (EU) 2021/915

of June 4 2021

on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (Text with EEA relevance)

ANNEX

Standard contractual clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with [choose relevant option: OPTION 1: Article 28(3) and (4) of Regulation (EU) 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)] / ~~[OPTION 2: Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC~~].

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. **Instructions**

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. **Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. **Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. **Security of processing**

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. **Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. **Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. **Use of sub-processors**

(a) ~~OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.~~

OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. **International transfers**

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies 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 controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in [OPTION 1] Article 32 of Regulation (EU) 2016/679/ [OPTION 2] Articles 33 and 36 to 38 of Regulation (EU) 2018/1725.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 **Data breach concerning data processed by the controller**

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to [OPTION 1] Article 33(3) of Regulation (EU) 2016/679/ [OPTION 2] Article 34(3) of Regulation (EU) 2018/1725, shall be stated in the controller's notification, and must at least include:

(1) 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;

(2) the likely consequences of the personal data breach;

(3) 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.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to [OPTION 1] Article 34 of Regulation (EU) 2016/679 / [OPTION 2] Article 35 of Regulation (EU) 2018/1725, with the obligation to communicate without undue delay 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.

9.2 **Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under [OPTION 1] Articles 33 and 34 of Regulation (EU) 2016/679 / [OPTION 2] Articles 34 and 35 of Regulation (EU) 2018/1725.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s): [*Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]*

1. Name:. . . . . .
Address: . . . . . .
Contact person's name, position and contact details: . . . . . .
Signature and accession date:. . . . . .

2.

. . . . . .

Processor(s): [*Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]*

1. Name: Hako GmbH

Address: Hamburger Straße 209-239
23843 Bad Oldesloe
Germany

Contact person's name, position and contact details: . . . . . .

Signature and accession date: . . . . . .

2.

. . . . . .

ANNEX II

Description of the processing

Categories of data subjects whose personal data is processed

- Users of Hako machines (e.g. operating personnel)
- Customers and their employees
- Service personnel and authorised partners

Categories of personal data processed

- Machine-related usage data with personal reference (e.g. I-button assignment to operating personnel by the client)
- Position data of the machine (GPS), insofar as this is personally identifiable in connection with user IDs or time stamps
- Personal master data/address data/contact data
- Communication and identification data (e.g. user ID, e-mail address if applicable)
- Contract master data (contractual relationship, product or contractual interest)
- Customer history
- Contract billing and payment data
- Planning and control data

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Access to location data or, if available, camera data only by authorised service technicians as part of a specific service call
- Logging of all location queries
- Access is exclusively via the Hako Fleet Portal with role-based assignment of rights
- Regular training of personnel
- Measures to anonymise image data for camera systems

Nature of the processing

- Collection, storage and analysis of machine data via IoT interfaces
- Transmission to the Hako fleet management portal (SaaS)
- Display and evaluation in the customer portal to optimise use, maintenance and service
- Anonymisation or pseudonymisation where possible, especially for machine position data
- Storage takes place within the EU or EEA (Hako server in Bad Oldesloe and Microsoft Azure cloud service in Europe)
- Transfers to third countries take place exclusively on the basis of suitable guarantees in accordance with Art. 46 GDPR (e.g. standard contractual clauses)

Purpose(s) for which the personal data is processed on behalf of the controller

- Provision of the Hako Fleet Management Portal
- Optimisation of machine availability, maintenance cycles and use of resources
- Traceability of machine utilisation (e.g. for accident prevention, training requirements)
- Fulfilment of contractual obligations towards customers
- Locating the machine by authorised service technicians if it cannot be found on site

Duration of the processing

- For the duration of the contractual relationship with the customer
- In addition, in accordance with statutory retention periods

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

- Storage of telematics data on Microsoft Azure cloud service in Europe
- For the duration of the contractual relationship with the customer
- In addition, in accordance with statutory retention periods

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

Contact details of the responsible body:	Hako GmbH Hamburger Straße 209-239 23843 Bad Oldesloe Germany
The Data Protection Officer of Hako GmbH is Contact details:	Astrid Bartel. Boschstraße 5 24118 Kiel Germany abartel@vater-gruppe.de
The responsible supervisory authority is:	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Holstenstraße 98 24103 Kiel Schleswig-Holstein Germany

Access control

Measures to ensure that only authorised persons have access to personal data:

Implemented/existing

- Written rules are in place that regulate who has access to which company areas.
- Employees wear visible badges.
- Visits are documented in a visitor book.
- Strict attention is paid to the separation of processing and public areas.
- The premises are monitored.
- There is a reception desk.
- Each key holder is included in a list.
- Acknowledgement takes place when keys are handed out.
- Alarm systems are in place.
- The entrances to the rooms are adequately secured (e.g. doors, light wells).
- A video surveillance system is in place.
- Appropriate arrangements have been made with the cleaning staff to prevent access to personal data.
- Attendance is monitored (e.g. time clocks, shift log).
- Sufficient security is ensured for remote workplaces.
- Absences are logged.
- An access control system is used.
- Appropriate arrangements have been made with IT service providers for maintenance work to prevent access to personal data.
- Access is blocked using chip cards/transponders.
- Security locks are used.
- Visitors are accompanied by employees.
- The security staff is selected with care.
- The cleaning staff are selected with care.
- Doors with knobs on the outside are used.
- A "Clean Desk" policy is in place.

Access control

Security measures to prevent unauthorised persons from accessing IT systems:

Implemented/existing

- There is a central firewall.
- Sufficiently secure passwords are used (e.g. no proper names and words from the dictionary, also use special characters, recommended length of ten characters, etc.).
- Incorrectly entered passwords are logged.
- Regular password changes are mandatory.
- There is a decentralised solution for employees who work from home.
- Each employee has their own user account.
- The encryption method used is state of the art.
- Access is blocked if more than three login failures occur. (varies depending on the application)
- Screens are automatically locked with password protection when breaks are taken.
- Two-factor authentication is used.
- Incorrect entry of the password leads to a time delay for a new attempt.
- The log entries are analysed if the password is entered incorrectly.
- Login with user name and password.
- There is a "secure password" policy.
- Intrusion detection systems are used.
- The following firewall and virus protection programmes are used: (Fortinet (firewall) Panda 360 (virus protection))

Access control

Measures applied to ensure that only personnel with the necessary authorisation to use the processing equipment have access to personal data and that the personal data used in processing is not read, copied, modified or deleted without authorisation:

Implemented/existing

- Protective measures are in place against unauthorised internal and external access (e.g. through encryption, firewalls).
- The authorisations for evaluations, access, modification and deletion are differentiated.
- The logs are analysed.
- The data carriers are inventoried. (Hard drives, notebooks, PCs (no USB sticks or external hard drives))
- The storage of data carriers is checked regularly.
- The receipt, issue and inventory of data carriers is recorded.
- Backup data carriers are stored externally.
- There are internal company guidelines for copying data records or the complete copying of data carriers.
- The devices of employees with remote workstations are serviced regularly.
- Obsolete data carriers are destroyed in a regulated manner.
- Data carriers are completely purged of existing data before being reused.
- Regular checks are carried out on the actual destruction of data carriers.
- Regular penetration tests are carried out against attacks by hackers.
- Procedures are used to recognise unwanted data outflows.
- The use of private data carriers is prohibited.
- Misprints are carefully disposed of.
- Access and access attempts are logged.
- The data on the data carriers is deleted before it is passed on, e.g. sold.
- There are rules for the use of mobile data carriers and devices.
- The concept fulfils the task-related and data protection requirements for both users and administrators.
- Shredders with a sufficient security level are used.
- File shredders are used.
- An external document shredder (e.g. in accordance with DIN 32757) is used.
- Authorisation concepts are used.
- Only the required number of administrators are authorised.
- The logs are kept for this period: (90 days)
- Data carriers are physically deleted.
- There is a "delete/destroy" policy.
- User rights are managed by administrators.

Transfer control

Measures to ensure that personal data cannot be read, copied, modified or removed without authorisation during transport, electronic transmission or storage on data carriers:

Implemented/existing

- The areas in which data carriers may be located before/after transport are defined. (Backup tapes are transported, other data carriers are not)
- The entry/exit of data carriers is recorded in writing.
- There is a specific group of people who are authorised to receive data carriers. (for backup tapes)
- There are binding regulations as to who may act as data recipients and who is authorised to pass on data.
- Only reliable couriers or transport companies are used.
- Electronic data transports are end-to-end encrypted.

Input control

Measures to ensure that it is subsequently possible to check and determine whether and by whom personal data has been entered, changed or removed from the processing system:

Implemented/existing

- The entry of new data is logged.
- As part of the logging process, it is recorded who has entered data.
- The logging process records when data was entered.
- The logging process records what data was entered.
- The logs of data changes are kept for the following period: (depending on the application)
- When documenting the input procedures, information about the person who made the changes is also recorded (not the name, but e.g. the job description)
- Logs are checked manually or automatically.
- There is an overview of which programmes can be used to enter, change or delete which data.
- Forms from which data has been transferred to automated processing are retained.
- Responsibilities for deletions are clearly allocated.

Order control

Measures required to process the data only for the purposes and to the extent necessary in accordance with the client's instructions:

Implemented/existing

- Careful selection of contractors takes place.
- There is a list of selection criteria.
- The contractor's subcontractors are carefully selected.
- There are detailed written regulations on the obligations of all parties to the contractual relationship (also with regard to subcontractors).
- There are clear rules on competences and responsibilities.
- A formalised order is placed.
- The work results of contractors are regularly checked (in terms of form and content).
- Necessary agreements on order processing or EU standard contractual clauses are concluded.
- Employees of the contractor are obliged to maintain data secrecy.
- The appointment of the data protection officer at the contractor is reviewed.
- Effective control rights vis-à-vis the contractor are agreed.
- The destruction of data after completion of an order is ensured.
- The contractor and its level of protection are regularly reviewed.

Availability control

Measures that increase availability:

Implemented/existing

- There are fire extinguishers, smoke and fire detectors.
- Backup data carriers are stored separately.
- An uninterruptible power supply (UPS) has been established.

- Data is stored on backup media.
- Storage units are designed redundantly.
- The data backups are encrypted.
- Appropriate precautions have been taken in the event of a disaster (e.g. internal/external attacks, damage caused by fire).
- Effective water protection systems are in place.
- Temperature and humidity are monitored in the server room.
- Fire extinguishers are installed in the server room.
- Sensitive data is stored in a data protection safe (e.g. S60DIS).
- RAID systems are used.
- Operating systems and data are stored on separate partitions.
- Backup processes are monitored.
- Regular data recovery tests are carried out and the results are logged.
- Backup media is stored in a secure location outside the server room.
- The server room is air-conditioned.
- Protective sockets are used in the server room.
- The server room has its own access control system with alarm system/alarm signalling.
- There are no sanitary connections in or above the server room.

Separation control

Measures to ensure that personal data collected for different purposes can be processed separately:
Implemented/existing

- There is at least one set of separate backups of all data under our responsibility.
- Production and test environments are always separated from each other.
- Personal data for development purposes is pseudonymised/anonymised.
- Data with high protection requirements is handled with particular care.
- There is a concept for client separation.
- There is a system for the modification, deletion and transmission of data with different contractual purposes.
- Systems are used that enable internal client separation (purpose limitation).

Organisational control

Internal measures to ensure an appropriate level of data protection:
Implemented/existing

- Backups of the database are carried out according to a defined scheme.
- Logging and log files are analysed.
- Established high standards for IT security and the handling of IT projects are utilised.
- A replacement is provided in the event of holiday or illness.
- There are regular reminders and warnings to promote awareness of the problem.
- Employees receive appropriate training on the secure handling of data.
- Separation of functions is practised.
- There are written regulations on the course of data processing and on the various data security measures.

Pseudonymisation

The following measures have been implemented so that data can no longer be assigned to a person:
Implemented/existing

- In the case of pseudonymisation, allocation data and personal data are stored in a separate and secure system (encrypted if possible).
- There are internal instructions to anonymise / pseudonymise personal data as far as possible in the event of disclosure or after the statutory deletion period has expired. (HR Scramble)

Data protection management

Measures used to regulate, document and review the processing of personal data:
Implemented/existing

- Employees are trained and obliged to maintain confidentiality.
- Employees are regularly (at least annually) sensitised.
- The organisation complies with information obligations.
- There is central documentation of all procedures and regulations on data protection with access for employees as required/authorised.
- The effectiveness of the technical protective measures is reviewed at least once a year.
- Software solutions for data protection management are used (e.g. ECOMPLY).
- There is central documentation of all procedures and regulations on data protection with access for employees as required / authorised (e.g. wiki, intranet).
- The following components of the company are certified (e.g. ISO 27001, BSI IT-Grundschutz or ISIS12): (ISO 27001 for SAP and Azure Cloud)
- The data protection impact assessment (DPIA) is carried out as required.

Privacy by Design

These default settings are intended to ensure that only personal data that is required for the respective purpose is processed:

Implemented/existing

- No more personal data is collected than is necessary for the respective purpose.
- Simple exercise of the data subject's right of cancellation by technical measures is possible.

Incident response management

The following measures have been implemented for security incidents:

Implemented/existing

- There is a documented process for recognising and reporting security incidents / data breaches (also with regard to the bligation to report to the supervisory authority).
- There is a documented procedure for dealing with security incidents.
- The DPO is involved in security incidents and data breaches.
- Security incidents and data breaches are documented in ECOMPLY.

ANNEX IV

List of sub-proces-

sors

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: One Microsoft Place

Address: South County Business Park
Leopardstown
Dublin 18
D18 P521
Irland

Contact person's name, position and contact details: EU Data Protection Officer of Microsoft

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

- Storage of telematics data on Microsoft Azure cloud service in Europe
- Storage for the duration of the contractual relationship with the customer
- Data is made available in the Hako Fleet Management Portal

2.

. . . . . .