m^{IoT} Agreement

This ifm *mobile*^{IoT} Agreement (the **"Agreement"**) is concluded between ifm (**"ifm"** in the following) and the customer (in the following, **"Customer**", together **"Party"** or **"Parties"**).

ifm and the Customer agree to the terms of this Agreement specified in the following:

1. Definitions

"API" stands for Application Programming Interface.

"API Adjustments" has the meaning specified in section 5.1 of the Agreement.

"CUs (Communication Units)" refers to the on-board hardware devices sold to Customer by ifm and installed in the end customer machines which transmit machine data to and from the ifm platform via the ifm web portal.

"Derivations" refers to, without limitation, all derivations, modifications, error corrections, patches, bug fixes, configuration and calibration settings, software updates and upgrades, improvements, further developments and subsequent versions of the ifm software, independent of whether developed by ifm or a third party.

"Customer's Limited IP Rights" refers to (a) the resale rights defined in section 2.2, (b) the access and service configuration rights for machine data defined in section 2.2 (only if selected by Customer) and (c) the sublicensing rights defined in section 8.1.

"End Customer" refers to the Customer's customers: (a) whose machines use communication units bought by Customer in the frame of this Agreement or its enclosures, and/or (b) who subscribe to the ifm *mobile*^{IoT} Service bought by Customer in the frame of this Agreement or its enclosures.

"End User" refers to the End Customer's permanent or temporary employees authorised by End Customer to use the ifm *mobile*^{IoT} Service in End Customer's name pursuant to the terms of the ifm End User Agreement.

"End User Agreement (EUA)" refers to the end user licence agreement enclosed with this Agreement, which is binding for the End Customers and their End Users when accessing and using the ifm *mobile*^{IoT} Service .

"ifm' Intellectual Property " refers to the ifm software, ifm platform, ifm web portal, ifm specifications, ifm trade names, all patents, copyrights, author's personal rights, service marks, trade names, logos, designs, slogans, Internet domain names, protected information and other intellectual property of ifm's, independent of whether registered or not and created before or after this Agreement takes effect.

"Force Majeure" refers to all events outside of a party's reasonable control which have an effect on the fulfilment of the Agreement by the affected party, including all events of a prolonged interruption of transport, website access, Internet connection (ISP), mobile communication service (net provider), other telecommunication, or the power supply.

"ifm Firmware" or **"Firmware"** refers to the software and/or application programming interface embedded in the ifm communication unit (CU) connected with the machine, including any adjustments or other derivations thereof generated by ifm for the Customer (or independently of the Customer), which ensure that the CU is compatible with the communication log of the machine to allow for communication between CU and machine.

"ifm Communication Units" see **"CUs"** above.

"ifm *mobile*^{IoT} Service" or **"Service"** refers to the online service provided by the ifm software on the ifm platform and called up by End Customers and their End Users via the ifm web portal which presents machine data transmitted to and from the CUs installed in machines located within the territory.

"ifm Platform" or **"DataPlatform"** refers to the cloud-based platform which operates the ifm software as a service application (SaaS), such as DataPortal, Realtime Client, REST API or other IT systems, which give the Customers and their End Customers and their End Users online access to the ifm ***mobile***^{IoT} Service .

"ifm Software" or **"Software"** refers to the ifm software in object code format which executes the ifm *mobile*^{IoT} Service on the ifm data platform, including Web Portal, REST API and Realtime Client, software updates and upgrades, configuration and calibration settings and the required tools, as well as installation manuals and operating instructions and other appurtenant software documentation.

"ifm Web Portal" or **"DataPortal"** refers to the website, which on Customer's request can be configured to Customer's own trademark, through which End Customers and their End Users get online access to their machine data.

"Customer" refers to the company named in the preamble to this Agreement.

"Customer Brand" refers to the name, trademark, logo, address and other aspects of the Customer's trademark.

"Machine" refers to a vehicle, a machine or another asset bought or leased by End Customer for business purposes from the customer or a distributor for which machine data is transmitted via the ifm *mobile*^{IoT} service.

"Machine data" refers to: (a) the machine-readable raw data collected and transmitted to the platform by the ifm Communication Units, and (b) the usage data on an End Customer's machines procured from such raw data by the *mobile*^{IoT} service in form of single or overall data, such as status, geographic site, operating hours, and other vehicle and machine data transmitted between the ifm platform and the Communication Units.

"Mobile Communication Service" refers to all communication standards used by the CUs, such as LTE, 5G, or another communication service used for transmitting machine data to and from the CUs and the ifm platform.

"Party", "Parties" has the meaning assigned to the term in the preamble to this Agreement.

"Software Updates" refers to a version of the ifm software published at a later data which ifm uses at its own discretion for the use of the ifm *mobile*^{IoT} Services .

"**Affiliated Companies**" refers to any company, corporation or other legal person that: (1) is controlled by a party to this Agreement, or (2) controls a party to this Agreement or (3) is under joint control with a party to this Agreement for as long as such control continues. with "control" meaning that the controlling legal entity owns or controls, directly or indirectly, more than fifty percent (50%) of the participations or shares of the controlled legal entity, giving it the right to take decisions for such legal entity.

"Violation of intellectual property" has the meaning specified in section 8.1 of the Agreement.

2. Offer to conclude a contract

2.1 ifm Communication Units (CUs)

Once ordered by Customer, ifm shall sell its Communication Units to the Customer in compliance with this Agreement and the individual contracts.

2.2 Subscription to the ifm *mobile*^{IoT} Service

With the purchase of a Communication Unit, the Customer acquires an appurtenant Service Subscription which it can sell on directly (or via a third-party supplier) to its End Customers or their End Users in compliance with the regulations of this Agreement **(" Subscription Resale Rights"**). Furthermore, the Customer has the following additional options: (a) It can acquire licensed access to machine data for its own internal access, its own storage and assessment, and (b) the Customer can acquire services for configuring the Web Portal in such a way that the End Customer can access the ifm *mobile*^{IoT} Service via a portal configured for the Customer's trademark (Customized Front End) (**"Machine Data Access and Service Configuration Rights"**).

2.3 No other products, services or licenses ordered

ifm is not obliged to sell or otherwise provide any other products, services or licenses in the frame of this Agreement. This would require a separate agreement in writing.

3. Retention of Title

The delivery items (goods subject to retention of title) remain ifm's property until all claims ifm has against the Customer from the business relationship have been fulfilled. If the value of all security interests to which ifm is entitled exceeds the amount of all secured claims by more than 20%, ifm shall release a corresponding part of the security interests at the 'Customer's request; ifm may choose which of different security interests it wishes to release.

During the existence of the retention of title, the Customer is prohibited from pledging or assigning the goods as security, and resale is only permitted to resellers in the normal course of business and only on condition that the reseller receives payment from his customer or makes the reservation that the title only passes to the customer when the customer has fulfilled his payment obligation.

If the Customer resells goods subject to retention of title, it hereby assigns its future claims from the resale against its customers with all ancillary rights – including any balance claims – to ifm by way of security without the need for further special declarations. If the goods subject to retention of title are resold together with other items without an individual price being agreed for such goods, the Customer assigns to ifm that part of the total price claim which corresponds to the price of the reserved goods invoiced by ifm.

4. Liability / Warranty

4.1 Passing of Risk

Also in case of freight-paid delivery, the risk passes to the Customer as follows:

a) if the delivery does not include assembly or erection, at the time when it is shipped or picked up by the carrier. At Customer`s request and costs, the supplier shall insure the delivery against the usual transport risks.

b) if the delivery includes assembly or erection, at the day of taking over in the Purchaser's own works or, if so agreed, after a successful trial run.

If the dispatch, delivery, start, execution of installation or mounting, the transfer into Customer’s own business or the test run is delayed for reasons attributable to Customer, or if the Customer is in default for other reasons, the risk shall pass to the Customer.

4.2 Liability / Warranty

The description of the product in Enclosure 2 is binding. ifm warrants the functionality of the products from its catalogue for a period of 60 months following delivery of the product, provided it is operated within the specification. The Customer shall inspect the product for possible defects immediately, but not later than within one month after delivery, and if applicable notify the defects in writing. In case of a complaint, the Customer must return the product together with a description of the defect, stating the ifm item number, to the responsible ifm branch office. ifm will examine the product and, at the Customer's request, send an examination report to the Customer. ifm must be given the opportunity for supplementary performance within a reasonable period. In case of a justified complaint, ifm shall free of charge, at its own discretion, rework, re-deliver or re-provide those parts or services, provided the reason for such complaint had already existed at the time the risk passed. If the Customer or a third party improperly modify or repair the delivery item, no claims can be based on these modifications or repairs and the resulting consequences.

In case of notifications of defect, the Customer has the right to retain payments to an extent which is reasonably proportionate to the material defects found. The Customer can only retain payments if a notification of defect has been made the justification of which is uncontested. The Customer has no right of retention if its claims for defects are statute-barred. If the notification of defects is unjustified, the Supplier shall be entitled to demand reimbursement from Customer of the expenses incurred.

Claims for damages by the Customer due to a material defect are excluded. This shall not apply to the extent that a Defect has been fraudulently concealed, the guaranteed characteristics are not complied with, in the case of loss of life, bodily injury or damage to health, and/or intentionally or grossly negligent

breach of contract on the part of the Supplier. A reversal of the burden of proof to the detriment of the Customer is not implied by the above provisions. Any further Customer's claims or claims different than specified in this section for material defects are excluded.

4.3 Limitation of liability

Except in cases of intent and gross negligence, both parties take liability only in case of the violation of significant contractual obligations (major obligations), and limited to the foreseeable damage typical for this type of contract.

The parties agree that the foreseeable damage typical for this type of contract is usually limited to an amount equivalent to the two months' subscription fees paid by the Customer to ifm from the day the claim occurred. The parties are free to prove that they suffered a higher damage.

The parties to this Agreement are not mutually liable for amounts constituting lost profits, lost business, accidental or indirect damage, consequential damage, or the other party's punitive damages, including for costs or damages in connection with downtime of the ifm *mobile*^{IoT} Service, service downtime of the mobile communication service, loss or falsification of machine or other data, downtime or defects of the CUs or services, work interruptions or work delay. The above-listed points do not limit the mutual obligations in the frame of the provision of damages, taking of defence measures, and indemnification specified in sections 8.1 and 8.2 of the Agreement. Also, the limitations or exclusions of liability are not applicable in case of culpable damage to life, limb or health, or of liability pursuant to the Product Liability Act.

4.4 Indemnification

The Customer must indemnify and hold harmless the Customer from third-party claims raised against ifm or ifm's Licensor and directly based on the allegation that third-party intellectual property rights or business secrets have been violated by (a) access to or use of customer data by means of the Services; or (b) the modification or use of the Services with the Customer's applications; and Customer must pay the damages or costs in connection with the resolution of the claim or finally imposed on ifm in the frame of such claim, comprising without limitation reasonably legal fees, provided that ifm (i) informs the Customer promptly of such claim; and (ii) grants the Customer extensive authority, information and support to defend itself against such claim; and (iii) allows the Customer sole control over the defence against such claim and all settlement negotiations regarding such claim. The Customer has the right without ifm's prior consent in writing to meet such claim or make a settlement, provided ifm will not incur any costs or significant disadvantages thereby.

4.5 No third-party rights

The warranty according to these Terms cannot be transferred. Neither the End Customers not their End Users can deduce rights or claims against ifm herefrom.

4.6 Limitation of liability

The liability provision in this Agreement is exclusive. No additional assurances or guarantees are given either in written or verbal form, either explicitly or implicitly. In particular, ifm excludes implicit assurances with regard to economic efficiency and suitability for a specific purpose. ifm is not liable either by contract or by law if the CU is modified by persons who are not employees of ifm or its affiliated companies.

4.7 Other damages

Unless specified otherwise in this Agreement, any claims for damages of the Customer's on any legal grounds whatsoever, in particular based on violation of duties from the contractual obligation and tort, are excluded. This does not apply if liability is based on:

a) According to the Product Liability Act
b) In case of intent
c) In case of gross negligence on the part of owners, legal representatives or executives
d) In case of malice
e) In case of non-observance of a warranty given
f) In case of culpable damage to life, limb or health, or
g) in case of culpable violation of major contractual obligations.

5. Provision of the ifm *mobile*^{IoT} Service

5.1 Achieving interoperability

ifm will work to its best knowledge and belief and with all economically reasonable efforts to achieve at the earliest possible date interoperability of the *mobile*^{IoT} Service with the machines, including the development of adjustments to the Customer-provided API (**"API Adjustments")** and the provision of other service configurations ifm considers necessary for reaching interoperability. The Customer assures and guarantees that is in possession of the full licence, right and authority to forward the machine API to ifm (without confidentiality obligations) to achieve interoperability of the *mobile*^{IoT} Service with the machine.

5.2 Configuration, activation support, technical support

The Customer acknowledges and confirms that it is liable and obligated both initially and continuously (a) to configure the representation of the machine data and other aspects of the *mobile*^{IoT} Service in a manner permissible according to the service documentation and otherwise in compliance with the wishes of Customer and its End Customers, and (b) to provide activation support and technical support to the End Customers and their End Users.

5.3 No provision of other services for End Customers

With the exception of providing the *mobile*^{IoT} Service, ifm is under no obligation whatsoever of providing activation support, technical support, training or other services for End Customers or their End Users. Responsibility for the provision of such services to End Customers and End Users lies solely with the Customer.

6. Customer's obligations

6.1 Control over the use of ifm's *mobile*^{IoT} services and machine data

In addition to the obligations specified in sections 4.5, 5.1, 5.2, 5.3 and 9.3, the Customer is liable and responsible at all times for:

a) the legal or illegal use of the *mobile*^{IoT} Service by End Customers, their End Users and others the Customer may have granted access in violation of the regulations of this Agreement;

b) the lawfulness of all machine data, including but not limited to its lawful procurement and use, as well as any obligation to determine the ownership in the data or to observe the intellectual property rights contained in such data;

c) any message, entry or other effect introduced via the CUs into the machine control, software or system architecture in consequence of Customer's use of the *mobile*^{IoT} Service , irrespective of whether ifm alerted the Customer to the probability of the risk occurring and the potential consequences; as well as

d) the up-to-dateness of the firmware: To ensure the functionality of the CUs, the Customer must ensure that the firmware updates and security patches provided by ifm are duly executed.

6.2 Cooperation and granting of access

If ifm considers it necessary to provide activation support and technical support to achieve interoperability pursuant to section 6.1 or to configure the DataPortal for the customer trademark, the Customer undertakes to use its best efforts to help ifm in this process, including but not limited to (a) granting ifm unrestricted access to the machines and CUs and (b) providing an output log, the machine data, and all other data ifm may reasonably require to reproduce the problem.

6.3 Investigation of third-party breaches

The Customer shall cooperate with ifm to its best knowledge and belief and offer ifm adequate support if ifm initiates investigations or brings charge against a third party suspected of using or having used ifm's *mobile*^{IoT} Service in direct or indirect connection the use of the Service by the Customer, his End Customers or their End Users in the frame of this Agreement if ifm finds that the third party may have breached ifm's intellectual property rights.

7. Intellectual property

7.1 Intellectual property rights

In compliance with the Customer's right to resell subscriptions pursuant to section 2.2 of this Agreement, ifm herewith grants the Customer (and its third-party providers) a corresponding limited, terminable, personal, non-exclusive and non-transferable license for granting service sublicenses to the Customer's End Customers and their End Users who are subscribers; such sublicenses shall be used in compliance with the requirements of this Agreement (**"Sublicensing Rights"**). Under none of the Customer's limited IP rights, claims or property rights in the CU firmware, the API Adjustments, the ifm software, other intellectual property of ifm's or any other aspect of the *mobile*^{IoT} Service are assigned, and such limited IP rights must not be considered as a sale of rights. Subject to Customer's limited IP rights, ifm shall remain the owner of all rights, claims and contents of all intellectual property, including the CU firmware, API Adjustments, ifm software, all contents of the DataPlatform and DataPortal which are not the Customer's trademark and all derivations, improvements, customer-specific adaptations to the above-mentioned contents, irrespective of whether they were created or developed by ifm alone or together with the Customer and irrespective of whether they were developed as part of the work in accordance with section 5.1 or as part of the provision of activation support or technical support.

The Customer has no right to won copies of the ifm software, unless there are legal reasons justifying the storage of a backup copy for archiving. Beyond this, the regulations of this Agreement do not grant the Customer any right in the source code of the ifm software. The Customer is not allowed to do the following, or permit a licensed user or other parties to do the following:

a) reverse-develop, decompile, translate, or disassemble the source code, or attempt to identify the source code or the ideas or algorithms on which ifm's intellectual property is based, or use ifm's intellectual property or other aspects of ifm's *mobile*^{IoT} Service in any other manner than permitted pursuant to this Agreement,

b) transfer ifm's intellectual property or other aspects of the *mobile*^{IoT} Service or sell, rent, loan, disclose, or use it for time sharing or outsourcing purposes;

c) use ifm's intellectual property or other aspects of ifm's *mobile*^{IoT} Service to the benefit of a third party, make it available to a third party or permit its use by third parties,

d) attempt to reset or deactivate ifm's intellectual property or other aspects of ifm's *mobile*^{IoT} service , except in the manner permitted pursuant to this Agreement, or

e) attempt to disguise or remove copyrights, trademarks and other information appearing on ifm's intellectual property or other aspects of the *mobile*^{IoT} Service .

7.2 License verification

At ifm's request, announced to the Customer via notification but not more frequently than once within every twelve (12) months, ifm has the right to check via audit (on site or remotely) the use of the CU firmware, the API Adjustments and the ifm Service by the Customer, its affiliates, its End Customers and End Users and by third parties whom the Customer may have granted access to the Services.

Such audit must be carried out in consultation with the Customer during the regular business hours without unreasonably interfering with the business activities.

7.3 Use of the machine data

Subject to the limited licenses and rights granted to the Customer under section 7.1, ifm has the right to use the collected and anonymised machine data for marketing purposes and to improve its products and services. This section 7.3 shall prevail after termination of this Agreement.

8. Indemnity

8.1 Indemnification of the Customer

ifm shall indemnify and defend the Customer and its affiliates and hold them harmless in respect of all costs and damage finally imposed on the Customer for direct breach of third-party intellectual property specifically during use of the ifm Service **("Breach of Intellectual Property"),** under the condition that (a) the Customer informs ifm immediately in writing of the asserted Breach of Intellectual Property, (b) the Customer allows ifm to pursue an adequate defence strategy at ifm's own discretion and to conduct all associated negotiations to settle the issue, and (c) the Customer cooperates with ifm in taking the necessary defence measures (including but not limited to the provision to ifm of all documents and information in the possession or under control of Customer which are relevant for defending against the asserted Breach of Intellectual Property, and the Customer arranging for its personnel to give witness statements, or the Customer consulting with ifm or ifm's lawyers in connection with such defence).

However, ifm is not liable for Breaches of Intellectual Property attributable to (a) modifications to the CUs carried out by persons other than ifm or ifm's affiliates, (b) use of ifm's *mobile*^{IoT} Service outside of the scope of the limited licenses and rights, (c) use of the applications, technologies or assets of ifm's *mobile*^{IoT} Service by the Customer in a manner which uses non-authorised rights to third-party intellectual property, and (d) claims based on a violation of Customer's assurances and warranties listed in

section 5.1 or of other aspects under Customer's responsibility pursuant to sections 4.5, 5.2, 5.3, 6.1 and/or 9.3 ("**Customer's Responsibilities**").

Beyond this, ifm may, at its own discretion and costs, take one of the following measures to mitigate and/or settle claims for Breach of Intellectual Property: (a) Replacement or modification of aspect of ifm's *mobile*^{IoT} Service in such a manner that the Service is no longer in breach, (b) procurement of a licence for the Customer to use the rights which were allegedly breached, or (c) cessation of the *mobile*^{IoT} Service with simultaneous refund of already paid fees. The above-listed measures are the only legal remedies the Customer is entitled to, and the only obligations and liabilities ifm must assume in case of a Breach of Intellectual Property.

8.2 Indemnification of ifm

The Customer shall hold ifm and its affiliates harmless of all damage, costs, lost, disclosed, or damaged machine data and other data, lost profits, reasonable legal fees and liabilities, including all claims ifm employees or other third parties may assert by reason of death, injury or damage to tangible or intangible assets attributable to the use or operation of the ifm *mobile*^{IoT} Service, provided such damage results from or is attributable to:

a) breach of Intellectual Property by the Customer;

b) violation of the regulations in section 7.1 or 9 of this Agreement or the End User Agreement by the Customer, its End Customers and/or their End Users;

c) areas within the Customer's scope of responsibilities pursuant to section 5.1;

d) use of the ifm *mobile*^{IoT} Service by non-licensed users who have gained access to the ifm *mobile*^{IoT} Service via the access code supplied to Customer by ifm, except in the form detailed in section 2.2; or

e) all claims asserted by End Customers or their End Users against ifm, including claims for any down-time or failure of the Service, CU or machine.

9. Confidentiality/data protection

9.1 Confidentiality

Both parties shall use their best efforts to ensure that no business secrets and confidential information of the other party are disclosed to others during the term of this Agreement and for a period of five (5) years thereafter. Except for the trademark ifm, the total intellectual property of ifm which ifm makes available to the Customer is considered confidential information and must not be disclosed to third parties in whole or in part, unless expressly permitted under this Agreement.

Neither party is obligated to keep confidential any information that is or becomes publicly known without any error or omission on the part of that party, or that was already known to that party, that was independently developed by a third party, or that was disclosed in the course of a lawful judicial or administrative proceeding.

9.2 Privacy statement

Use and protection of the personal data of the Customer and its End Customers and their End Users by ifm is subject to the Data Processing Agreement (DPA) annexed as Enclosure 5.

9.3 Compliance with the data protection regulations

Customer understands and agrees that it is Customer's obligation to comply with all privacy laws and regulations that apply to Customer's transactions and other actions taken under this Agreement, including those relating to End Customers and their End Users.

10. Applicable ifm directives

ifm's Code of Conduct

The Customer is obliged to comply with ifm's Code of Conduct annexed as Enclosure 3 and to have its affiliates, authorized sales partners, End Customers and their End Users comply with the regulations of the Code of Conduct.

11. Termination

11.1 Duration

Unless terminated prematurely pursuant to these terms, this Agreement shall start on the Effective Date and initially run for two (2) years ("**Initial Duration**"). Then, it shall automatically extend for another year ("**Extension Period**", both durations are summarily referred to as "Duration"), unless one party informs the other party at least three (3) months before the end of the duration of its intention not to extend the Agreement.

11.2 Termination in case of major breaches

Either party may terminate this Agreement and the Enclosures in the event of a major breach by the other party of the terms and limitations of this Agreement or its Enclosures thirty (30) days after written notice of a major breach and imminent termination is served on the other party, specifying the nature of the breach. If such major breach is remedied within thirty (30) days of receipt of notice of the breach and of impending termination, this Agreement and all Enclosures shall not be terminated and shall remain in full force and effect.

A "material breach" referred to herein includes, without limitation, the following:

a) Customer's failure to pay an invoice by ifm in keeping with the terms of payment;

b) any breach of section 8.1 of this Agreement by the Customer, its End Customers or their End Users;

c) any breach by either party of its obligation of secrecy specified in section 10 of this Agreement;

d) any failure by Customer to legally indemnify ifm at ifm's request pursuant to section 9.2 of the Agreement.

11.3 Termination by ifm

Furthermore, ifm has the right to terminate this Agreement and the Enclosures at any time by written notice of immediate termination to the Customer:

a) if the Customer has filed an application for the opening of insolvency proceedings or comparable proceedings due to insolvency or overindebtedness;

b) if a decision has been passed that the Customer is overindebted, insolvent or bankrupt;

c) if the Customer has initiated legal proceedings or submitted documents that contain an agreement concerning the Customer's restructuring, reorganisation or any other agreement relating to the Customer's business with regard to insolvency or overindebtedness;

d) the appointment of a receiver or a comparable administrator under applicable law for all or material assets of the Customer's;

e) the assignment of the Customer in favour of creditors;

f) the initiation of proceedings for the liquidation or dissolution of the Customer or for the termination of its partnership or corporate agreements;

g) when all or a substantial part of the assets of the Customer are transferred to a third party.

11.4 Legal consequences of termination

In case of termination of this Agreement for any cause whatsoever, the following applies:

a) Except for the situation regulated in section 11.4(f) below, all Enclosures to this Agreement, all outstanding subscriptions and all licenses or rights granted on the basis of this Agreement are terminated automatically and simultaneously without further notification;

b) Except for the situation regulated in section 11.4(f) below, the Customer, its End Customers and their End Users are obliged to immediately stop using ifm's intellectual property, all other aspects of ifm's *mobile*^{IoT} Service and all other confidential information of ifm's, return to ifm all copies of such intellectual property which are in their possession or otherwise submit adequate proof to ifm in the form of an affidavit confirming the destruction of such data.

c) Except for the situation regulated in section 11.4(f) below, the Customer, its End Customers and their End Users are obliged to immediately stop using the CU firmware and API adaptations and the SIM cards provided by ifm;

d) For each termination of this Agreement according to sections 11.2 or 11.3, unless the termination was caused by a "material breach of the Agreement" by ifm, the Customer shall pay to ifm a cancellation fee corresponding to the amount of subscription fees for (i) twelve (12) months or (ii) the remainder of the term, whichever is shorter; and

e) all unpaid costs, additional costs and costs for early cancellation resulting from the termination of the mobile communication service become due immediately and must be paid to ifm by the Customer.

f) If this Agreement is terminated for any reason other than by ifm according to section 11.2 or 11.3 and the Customer has paid all charges according to section 11.4(d) and (e) (including the fees for outstanding subscriptions), all outstanding End Customer subscriptions will continue after termination of the Agreement until the end of the then current term, and at the end of the term (i) each End Customer subscription will automatically and irrevocably expire without renewal, (ii) the corresponding SIM card will automatically and irrevocably be deactivated and (iii) all corresponding machine data for that End Customer will be deleted after thirty (30) days without prior notice.

11.5 Surviving clauses

Sections 4.5, 4.6, 5.3, 6-10, 11.4, 11.5 and 12.3 of the Agreements survive the termination of this Agreement and the termination of a license or law granted in the frame of this Agreement.

12. Settlement of disputes

12.1 Support

The support services of ifm and the Customer shall endeavour to settle any disputes. If the support cannot settle the dispute, it shall be escalated and settled internally according to section 12.2.

12.2 Internal settlement of disputes

Neither party may bring any action against the other party with respect to any matter relating to this Agreement or its Enclosures until the parties have exhausted the following procedures:

a) If either party believes that a dispute exists under this Agreement or its Enclosures, it may notify the other party of the dispute. The notification shall specify the nature of the dispute;

b) Within ten (10) days of receipt of a notice of a dispute, a General Manager / Head of Department of each party shall meet and attempt in good faith to settle the dispute.

c) If the dispute cannot be settled in the meeting specified in section 12.2(b) and after expiry of ten (10) days after notification of the dispute, the Managing Directors of each party shall meet within thirty (30) days and attempt in good faith to settle the dispute.

d) All negotiations pursuant to this clause are confidential and are treated as compromise and settlement negotiations.

Internal settlement of disputes should only be used if both parties feel this is necessary and reasonable. This must be evaluated in each individual case.

12.3 External settlement of disputes

If the dispute has not been internally settled within forty (40) days after notification of the dispute according to section 12.2, either party may request a court decision. All disputes arising out of or in connection with this Agreement or its Enclosures shall be brought exclusively before the Regional Court where ifm has its registered office.

12.4 Applicable law

This Agreement shall be subject to the law of the country where ifm has its registered office. The application of the United Nations Convention on Contracts for the International Sale of Goods of 11.04.1980 is excluded.

13. General

13.1 Subcontractors

To meet its obligations from this Agreement in whole or in part, ifm may assign one or several subcontractors.

13.2 No joint venture

The provisions in this Agreement or its Enclosures must not be interpreted to establish a joint venture, partnership, or employment relation between the parties; likewise, no party has the right, authority or permission to expressly or implicitly assume obligations in the name of the other party.

13.3 No assignment

Without procuring the previous consent in writing from the other party, the parties must not assign rights from this Agreement and its Enclosures or to delegate obligations assumed in the frame of this Agreement; this, however, under the condition that ifm may transfer this Agreement and its enclosures without any such consent to a third party which acquires ifm's intellectual property or essentially ifm's total assets. Assignment or delegation of obligations in breach of section 13.3 of this Agreement is void.

13.4 Force majeure

None of the parties is liable for non-fulfilment of its obligations in consequence of an event of force majeure.

13.5 Communication

All notifications, inquiries, claims, demands or other messages required in the frame of this Agreement must be in writing and shall be sent either per mail or registered letter to the respective party's business address, or by email to info.mobileiot@ifm.com.

13.6 Waiver

A party's omission to assert rights from this Agreement or its Enclosures shall be not construed as a waiver of such rights.

13.7 Severability clause

Should individual terms or regulations of this Agreement prove to be illegal or unenforceable, the validity or enforceability of the remaining Agreement remains unaffected.

13.8 Final regulations

This Agreement and its Enclosures constitute the entire agreement between ifm and the Customer and supersede (except for an NDA already effectively concluded) all prior or contemporaneous communications, statements or agreements between the parties, whether oral or written, including but not limited to any offers, proposals, emails, brochures or information on Internet sites relating to the subject matter of this Agreement or its Enclosures. The Customer's terms and conditions (including those which appear on the reverse side of an order or an attachment to an order, whether in relation to payment or otherwise) shall not apply. In the event of any conflict between the terms of this Agreement and its Enclosures, the terms of the following documents shall prevail in the order in which they appear:

(a) this Agreement, (b) the ifm directives mentioned in section 10, and (c) special offers beyond this Agreement. Any modification to this Agreement and all its Enclosures must be by a change note in writing signed by an authorised representative of each party.

Annexes

Enclosure 1 – **Additional Terms and Conditions regarding SIM Cards**

Enclosure 2 – **Product Description**

Enclosure 3 – **ifm Code of Conduct**

Enclosure 4 – **End User Agreement (EUA)**

Enclosure 5 – **Data Processing Agreement (DPA)**

Annex 1

"Additional Terms and Conditions regarding SIM Cards"

These Additional Terms and Conditions (ATCs) supplement the mIoT Agreement. They apply to the mobile communication services for machine-to-machine (M2M) applications and mobile Internet of Things (*mobile*^{IoT}) applications and the further appurtenant services (in the following collectively, the "Services") which the Customer ordered from ifm electronic gmbh (ifm in the following).

1. Definitions

"Group Companies" refers to any group company of the Customer's.

"Connected Networks" refers to third-party mobile communication networks in which M2M services are used.

"Post-installation services" refers to the M2M services by ifm.

"End user" refers to non-reseller users who use a SIM for their own purposes.

"Devices" refers to all devices in which SIMs are used which have been provided by ifm pursuant to these Terms.

"Force majeure event" refers to an event which is outside of the range of influence of a contractual party (or of a person acting in such party's name) and which by its nature could not have been foreseen or prevented by such party or person; the term includes but is not limited to: acts of God, storms, floods, riots, fire, sabotage, civil uprising or unrest, intervention of civil or military authorities, acts of war (whether declared or not) or armed conflicts, terrorist attacks, or failure of energy supply.

"BNetzA" refers to the Bundesagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (German Federal Network Agency).

"Platform " refers to the global M2M data service platform.

"SIM" refers to a Global M2M SIM provided to the Customer in the frame of this Enclosure.

"Territory" refers to the territory in Germany, as well as other countries with roaming partners, if agreed upon.

"ifm group (company)" refers to all group companies of ifm Stiftung & Co. KG.

2. Services

ifm provides the following services:

- provision of a mobile communication connection for M2M/mIoT applications bound to the corresponding hardware which allows the Customer to use mobile data communication connections and other net and network services. This is effected by the provision of the SIM coded in the hardware. The SIM is permanently installed in the hardware; use of the mobile communication connection and the net and network service is permitted to the Customer in connection with the hardware only.
- All services in the sense of these ATCs are provided under the condition that the Customer may only use them in combination with the hardware.
- ifm shall provide the services in the sense of these ATCs in the frame of its technical and operational possibilities. The above-named mobile communication connection is made on the basis of the advance services provided by licensed mobile network operators.

Insofar, ifm is free at any time without Customer's prior consent to use third-party services to fulfil the contract.

3. Customer's use of the services

3.1 Customer shall use the services exclusively for the contractual purpose within the contractual area in compliance with these Terms. It shall analogously provide for compliance with the contractual regulations on the side of its end customers if the contractual purpose comprises a transmission of the services to its end customers.

3.2 Customer shall use the services exclusively for the contractual purpose within the contractual area in compliance with these Terms. It shall analogously provide for compliance with the contractual regulations on the side of its end customers if the contractual purpose comprises a transmission of the services to its end customers.

3.3 Customer shall ensure that the services provided under these Terms shall be used by Customer and its end users for the contractual purpose only and not in any manner that:

a) involves the provision of services via the connection services that enable an end user – also via a proxy server, gateway or router – to access a publicly accessible destination (i.e. a public IP address), unless the use of the public IP address is for the purposes of configuration and efficient use of the M2M services in accordance with these Terms;

b) would result in a violation of copyrights, trade marks, business secrets or other third-party intellectual property rights;

c) would interfere with the use of a network by other users or bypass security measures, irrespective of whether such unauthorised access results in loss or falsification of data;

d) could result in a hazard for life, limb and health of other persons or in environmental damage.

e) Irrespective of clause 3.4 (e), the Customer has the right to sell its own products comprising the SIMs to end users if agreed to between the parties as a contractual purpose.

3.4 The Customer shall refrain from and oblige its end users to refrain from:

a) modifying, adjusting, amending, or translating the services or SIMs, or creating derivative works therefrom;
b) combining the SIMs using them together with other hardware, software, products or services that are not in accordance with the purpose of these Terms or have not been expressly approved by ifm;
c) sub-licensing, leasing, renting, loaning, or otherwise transferring the SIMs to third parties, except to end users;
d) reverse engineering, decompiling, disassembling or otherwise attempting to discover the source code or object code of the SIMs or software running on the SIMs;
e) reselling or using the services to provide services to third parties or allow third parties to remotely access the services, or to use the SIMs (or permit such use) to develop product lines similar to the SIMs, unless this is in accordance with the contractual purpose and has been agreed to between the parties;
f) using the SIMs for other purposes than for the services related to the purpose of these Terms and the applications expressly agreed in writing with ifm.

3.5 The Customer shall procure all authorisations required for customer-side use of the Services (including registration with the BNetzA, if applicable).

4. Dynamic updates of the SIMs

ifm reserves the right to carry out updates or upgrades in any manner whatsoever. Such updates or upgrades shall not significantly deteriorate the functionality of the SIMs.

5. Connection services

5.1 ifm ensures that M2M services will be available to the Customer for use in the connected networks in each of the territories.

5.2 ifm reserves the right to modify the list of connected networks in keeping with changes to the economic and legal framework conditions. In doing so, ifm shall take the Customer's interests in consideration to exclude as far as possible any modification to the range of services for national roaming for the duration of the contractual agreement. At the same time, the Customer is aware that a) the supply of certain network technologies for providing the connection services may end before the termination of the Terms, or b) existing network technologies may be replaced by other network technologies in the course of network refurbishment. Accordingly, the Customer will ensure that its hardware will be compatible with the network technologies used.

5.3 At ifm's disposition, the Customer shall pause the enabling of a SIM if it has been manipulated to make settlement information inaccurate.

5.4 To avoid interruptions of M2M applications abroad, no data roaming maximum limits pursuant to EC Directive 544/2009 will be specified for the M2M cards which are the subject of this Agreement. The Customers does not want any automatic information regarding charges or data volume used.

6. Intellectual property

"Intellectual property rights" refers to patents, registered and non-registered trade and service marks, registered designs and design rights, copyrights (including such rights in computer software and databases) and database rights.

6.1 The Customer acknowledges that all property rights to the Services and to all documents, data and specifications contained therein shall remain the exclusive property of ifm (and/or its licensees) and that the Customer shall not be entitled to any rights in this respect other than those stipulated in these Terms. Should the Customer (now or in future) acquire intellectual property rights in or in respect of the Services, the Customer shall assign all such intellectual property rights to ifm.

6.2 The Customer confirms that the SIM will not be used in combination with another product not provided by ifm where the combination of the SIM and the product would violate third-party intellectual property rights.

6.3 For the duration of the mIoT Agreement or until the expiry of the individual agreement ending last, ifm grants the Customer the free-of-charge non-exclusive right of using the intellectual property rights for the contractual purpose.

6.4 The customer acknowledges that it is not authorised to apply for industrial property rights in intellectual property rights pursuant to 6.1.

7. Data protection

7.1 The parties confirm that the Customer is the controller in respect of the contents of any communication via the connection services and of all saved personal data of the Customer's or end user's ("Customer's personal data"). Regarding all personal data it processes for the Customer, ifm shall take reasonable and sufficient operational and technical security measures to protect Customer's personal data from accidental or illegal erasure or from accidental loss, damage, modification, as well as unauthorised disclosure or access.

7.2 Customer confirms that ifm may receive legally binding requests from authorities to disclose Customer's personal data, or may be obligated by law or by a court order to disclose Customer's personal data to other persons than the Customer. ifm shall inform the Customer about any such demand in good time, unless ifm is subject to other binding prohibitions, for example under criminal law, forcing ifm to maintain confidentiality in the course of preliminary proceedings.

7.3 The Customer assures that:

a) in its role as a controller of the Customer's personal data, it shall observe all applicable data protection laws; and
b) if obligated to do so in the frame of the applicable data protection law, it shall inform all end users or, if necessary, procure end users' informed consent that ifm (or a processor made liable) will process the Customer's personal data for the purpose of providing the services.

7.4 If end user's or Customer's consent is required pursuant to applicable data protection law and if such consent is refused and/or revoked, and if the Customer cannot otherwise prove for one or several end users that the disclosure or processing of personal data pursuant to clause 7.4 is in compliance with the applicable data protection law, the Customer shall immediately call ifm's attention to this circumstance. The Customer acknowledges that in this case ifm will not be obliged to continue to provide the services for the respective end users, irrespective of any other regulations of this Agreement.

8. Confidentiality

8.1 These Terms are confidential and must be disclosed to third parties without the other party's prior consent in writing. Each party is aware that in consequence of this Agreement, it may become aware of information not in the public domain about the other party, its employees, suppliers or other subcontractors, including but not limited to information regarding prices, processes, finances, statistics, future and current products, current services, or appurtenant information (Confidential Information). Without the disclosing party's prior consent in writing, the receiving party must not disclose Confidential Information (except to the extent required for the contractual purpose) to other persons, firms or companies, use it for its own purposes, copy or modify it or reproduce it in any other manner.

8.2 Clause 8.1 shall not be applied on Confidential Information which

a) has been made publicly available by other means than by a violation of clause 10.1;
b) has been made available by a third party that acquired such information lawfully and is not subject to confidentiality;
c) is the result of an independent development by the receiving party or one of its group companies;
d) has to be disclosed on a legal basis to a state regulatory authority or on the basis of the applicable stock exchange law.

9. Export control

In connection with the execution of the Agreement, each party agrees

a) to comply with all applicable laws in respect of export controls and with the financial and economic sanctions of the European Union, the United States of America, and other countries which are significant for the parties' contractual relationship;

b) not to deliberately take actions causing the other party or a member of such party to violate the respective regulations.

10. Miscellaneous

10.1 Any modifications of the Terms must be in writing. This is also true for the waiver of the requirement of written form.

10.2 Without the other party's prior consent in writing (which must not be unreasonably withheld or delayed), no party to the Agreement is allowed to assign its rights and obligations under these Terms, but ifm is allowed to assign its rights and to assign, transfer or subcontract its obligations under these Terms to another member of the ifm group, and ifm is allowed to subcontract the provision of the services in the regular course of business with the proviso that the commissioning of a subcontractor does not release ifm from any liability under these Terms.

10.3 Should one of the above clauses be invalid in whole or in part, the validity of the remaining clauses shall not be affected. The parties shall promptly agree on a clause which comes as close as possible to the original invalid clause.

Annex 2

Product description ifm *mobile*^{IoT} Platform

The ifm *mobile*^{IoT} platform is the integration of multiple services that will allow machines to get connected into the platform as well as the environment and front-end to manage these entities. The various services as part of the Platform are described in this document.

ifm mobile^{IoT} M2M services - Connectivity and mobile telecommunication

The connectivity service contains the remote and/or mobile telecommunication connection from the machine into the ifm *mobile*^{IoT} Platform. By using the ifm *mobile*^{IoT} hardware, with embedded SIM card installed, the customer may use the telecommunication and network infrastructure provided by ifm. The infrastructure is constructed such that the telecommunication channel between the ifm *mobile*^{IoT} hardware and the ifm *mobile*^{IoT} Platform is secured to the latest technology standards. Using hardware without the ifm *mobile*^{IoT} embedded SIM, this security could not be guaranteed.

Once the connectivity service was activated through a contract, the hardware may connect to the hosting services of the ifm *mobile*^{IoT} Platform. The activation of the contract will take place in the ifm *mobile*^{IoT} Suite front-end. The connection using the mobile telecommunication services is allowed and granted in the attached **country and network partner list**.

ifm mobile^{IoT} Real-time services – Remote connection, diagnostics and debugging

With the Real-time services, the customer may create a point-to-point real-time channel, whether or not using the mobile telecommunication services, between a workstation (like laptop or pc) and the machine. This channel, depending on the type of channel chosen, gives either direct access to the machines CAN bus(ses), Ethernet network(s) and therefore all components connected to either of these interfaces. Creating such a channel and connection to the components on the machine, diagnostics and debugging could be made remotely in real-time. None of the traffic generated during the use of Real-time services will be stored or retained. When using the telecommunication services, the time connected with the real-time services will be counted and is either part of the contract agreed on or could be separately being invoiced by ifm.

ifm mobile^{IoT} DataHosting services – Data and cloud hosting

Processing, storing or giving context to machine data is part of the data hosting services of the ifm *mobile*^{IoT} Platform. This could be either the data that has been collected during machine runtime, therefore data being sent from the machine to the platform, or files like configuration, software or firmware or any other kind. The retained data is either accessible through the ifm *mobile*^{IoT} DataPortal or the provided APIs for all users and accounts with the according permissions to that data. All other kind of data will be stored as long as either the machine contract is valid, or the cooperation between customer and ifm comes to an end. This kind of data is being stored within the ifm *mobile*^{IoT} Suite and therefore available for the users with corresponding permissions.

All types of files and data is being stored to the customers domain, therefore only having the corresponding permissions the data is accessible.

ifm mobile^{IoT} Suite – Management Portal

The ifm *mobile*^{IoT} Suite is the cloud-based Management Portal where the customer can do the management of the ifm *mobile*^{IoT} Platform with main focus the customer machine fleet. The ifm *mobile*^{IoT} Suite consists of two main functions, being Asset management and Tooling.

The asset management section allows the management of:

- Accounts and users allowed in, different parts of, the ifm *mobile*^{IoT} Platform
- Organizational hierarchy
- The machines, its underlying components and their configurations
- Machine or platform contracts can be pre-Activated, activated and terminated

Within the Tooling section, the user or developer of the machines is given tools to easily create configurations for the machine or even configure the machine over the air, using the ifm *mobile*^{IoT} M2M services.

The ifm *mobile*^{IoT} Suite is built for management and configuration of the ifm *mobile*^{IoT} Platform and it's components. Therefore the front-end, the look-and-feel is set to ifm styling and not adjustable.

ifm mobile^{IoT} DataPortal – Data visualization Portal

The ifm *mobile*^{IoT} DataPortal is the data visualization section of the Platform, which can be configured, adjusted and customized to the customer wishes and look-and-feel, within the limits given by the DataPortal UI possibilities.

The front-end may be customized using the layout canvas and placing available widgets, configuring it to the information that has been collected by the machines that has to be visualized. Besides that, the theming of the DataPortal is adjustable and can be styled to the customer cooperate identity, using coloring and branding with logos.

The DataPortal can also be branded and customized by the customer for their customer(s), by using the hierarchal structure and assign the customized layout and themes to a specific organization in the hierarchy.

Besides the front-end customization, the DataPortal is also the place to create reports, plots, map traces, etc.

Urls:

Machine management Suite: https://suite.miot.ifm

DataPortal: https://portal.miot.ifm

COUNTRY AND NETWORK PARTNER LIST

Argentina	Claro
Argentina	Telecom Personal
Australia	Optus
Australia	Vodafone
Austria	Orange
Austria	T-Mobile
Austria	Mobilkom
Belgium	Base
Belgium	Proximus
Bulgaria	M-Tel
Bulgaria	Globul
Bulgaria	Vivacom
Cambodia	Cellcard
Cambodia	Hello
Canada	Bell Mobility
Canada	Telus
Canada	Videotron
Chile	Entel
Chile	Claro
Colombia	Claro
Colombia	Tigo
Croatia	Croatian Telecom
Croatia	Tele2
Croatia	VIPnet
Cyprus	Cytamobile-Vodafone
Cyprus	MTN
Czech Republic	Vodafone
Czech Republic	T-Mobile
Denmark	Telenor
Denmark	TDC
Egypt	MobiNil
Egypt	Etisalat
Egypt	Vodafone
Estonia	EMT
Estonia	Tele2
Estonia	Elisa
Finland	DNA
Finland	Alands Mobiltelefon
Finland	Elisa
France	Orange
France	SFR
France	Bouygues
Germany	T-Mobile
Germany	Vodafone
Germany	E-plus
Germany	O2
Greece	Cosmote
Greece	Vodafone
Guatemala	Tigo
Guatemala	Claro
Hongkong	3
Hongkong	Hutchison
Hongkong	SmarTone
Hungary	Telenor
Hungary	T-Mobile
Hungary	Vodafone
India	Idea
India	AirTel
India	Vodafone
Indonesia	3
Indonesia	Indosat
Ireland	Vodafone
Italy	Vodafone
Italy	TIM
Italy	Wind
Jordan	Zain
Jordan	Umniah
Kazakhstan	Tele2
Kazakhstan	KCell
Kenya	Airtel
Kenya	Safaricom
Korea	KT
Korea	SK Telecom
Kuwait	Zain
Kuwait	Oreedo
Latvia	Tele2
Latvia	Bite Latvija
Latvia	LMT
Lithuania	Tele2

Lithuania	Bite GSM
Luxembourg	LUXGSM
Luxembourg	Tango
Luxembourg	Orange
Malta	Vodafone
Mexico	IUSACell
Mexico	Telcel
Netherlands	Vodafone
Netherlands	T-Mobile
Netherlands	KPN
Norway	Telia
Norway	Telenor
Panama	Claro
Panama	Cable & Wireless
Panama	Digicel
Paraguay	Claro
Paraguay	Airtel
Peru	Nextel
Peru	Claro
Philippines	Globe
Philippines	SMART Gold
Poland	Era
Poland	Plus
Poland	Play
Portugal	Optimus
Portugal	Vodafone
Portugal	TMN
Qatar	Vodafone
Qatar	Q-Tel
Romania	Vodafone
Romania	Orange
Russian Federation	MTS
Russian Federation	NCC
Russian Federation	Rostelecom
Russian Federation	Rostelecom
Saudi Arabia	STC Al Jawal
Saudi Arabia	Zain
Serbia	VIP
Serbia	Telenor
Serbia	mt:s
Singapore	M1
Singapore	StarHub
Singapore	SingTel
Slovakia	T-Mobile
Slovakia	Orange
Slovenia	Mobitel
Slovenia	SI Mobil
South Africa	Vodacom
Spain	Vodafone
Spain	Orange
Sweden	Telenor
Sweden	Tele 2
Switzerland	Swisscom
Switzerland	Sunrise
Taiwan	Far EasTone
Taiwan	Taiwan Mobile
Thailand	Real Future
Thailand	True Move
Turkey	AVEA
Turkey	Vodafone
United Kingdom	Vodafone
United States	AT&T
United States	Viaero
United States	Commnet Wireless
United States	Immix
United States	AWN
United States	Union Telephone Company
United States	T-Mobile
Vietnam	Vinaphone
Vietnam	VietnaMobile
Vietnam	Viettel

Annex 3
Code of conduct for ifm business partners

In accordance with the ifm code of conduct we tolerate no corruption, bribe and child labour. We expect the same ethical standards from our partners. This code of conduct defines the principles and requirements for our business partners regarding their responsibility for people and the environment.

1. Compliance with laws and standards

The business partner complies with the applicable laws, guidelines and standards.

2. Prohibition of corruption and bribery

The business partner condemns any form of corruption and bribery. This includes that the business partner does not grant payments or other advantages (e.g. kick-back payments, gifts, entertainment) to any individual, company or office bearer with the aim to influence decision making processes.

3. Confidential information and data privacy

The business partner complies with all applicable data protection laws. The business partner ensures that strict secrecy is kept about confidential information or trade secrets he becomes aware of in the context of the business relationship with ifm and that this information is not used unlawfully or disclosed to a third party.

4. Discrimination

The business partner does not discriminate against anyone because of their age, gender, religion, ethnicity or any other reasons.

5. Prohibition of child and forced labour

The business partner does not employ workers who cannot produce any evidence of their minimum age of 15. In those countries subject to the developing country exceptions of the ILO convention 138, the minimum age may be reduced to 14.
The business partner refuses to employ anyone or make anyone work against their own free will.

6. Anti-trust law

The business partner is committed to fair competition, complies with the applicable antitrust laws and will not engage in price agreements, the sharing of markets or customers, market sharing agreements or bid-rigging.

7. Freedom of association and collective bargaining September

Workers, without distinction, have the right to join or form trade unions of their own choosing and to bargain collectively. The business partner adopts an open attitude towards the activities of trade unions and their organisational activities. Workers representatives are not discriminated against and have access to carry out their representative functions in the workplace. Where the right to freedom of association and collective bargaining is restricted under law, the employer facilitates, and does not hinder, the development of parallel means for independent and free association and bargaining.

8. Environmental protection and occupational safety

The business partner undertakes to adhere to the applicable environmentally-relevant legal provisions and official regulations of authorities and to continuously improve environmental protection on an economically justifiable scale.

The business partner adheres to the legal provisions for assuring health and safety at work.

9. No ifm products for military applications

In accordance with ifm's corporate philosophy, ifm will in principle not develop, produce or sell products which directly serve military purposes. Therefore, the business partner will not use or deliver ifm products to customers who want to use ifm products for military applications or install them in military applications.

Annex 4
Template of an end user agreement for the Customer Web Portal
(Customized or White Label Front End)

IMPORTANT: Carefully read the following before using *mobile*^{IoT} services: This End User Agreement ("EUA") is a legally binding agreement between you as an end customer or end user (both defined in the following) and _____ ("OEM") for your licensed use of *mobile*^{IoT} services, the licensor of the OEM (defined in the following) being a third-party beneficiary under this EUA. With the acceptance of this EUA or the activation of, access to, or other use of the *mobile*^{IoT} services, you consent to being and becoming bound to the conditions of this EUA as a precondition for your license and the use of the *mobile*^{IoT} services. Please check the terms of this EUA and then accept or refuse them. If you do not agree to the terms of this EUA, you are not allowed to use it or to enable or access the *mobile*^{IoT} service or to use it in any other manner.

1. Definitions

"Subscription" refers to the end customer subscription to the *mobile*^{IoT} service made available by the OEM.

"**Subscription period**" refers to the end customer's period of subscription.

"Activation date" refers to the date on which the end customer or one of its end users first enables the *mobile*^{IoT} service, or otherwise to the start of the *mobile*^{IoT} services, as agreed between the end customer and the OEM.

"Malicious code" refers to a code, files, scripts or programs intended to do harm, including but not limited to viruses, worms, malware and trojans.

"Data platform" refers to the cloud-based data platform in combination with Web Portal, Realtime Client, REST API and other IT systems on which and via which the software runs the *mobile*^{IoT} service, saves the machine data, and allows the end customers and their end users licensed access in the frame of a subscription.

"Derivations" refers to all derivations, modifications, error corrections, patches, bug fixes, metadata, configuration and calibration settings, software updates and software upgrades, improvements, further developments and enhancements and subsequent releases of the software, independent of the author.

"End Customer" refers to the economic entity authorised in the frame of a subscription to use the *mobile*^{IoT} service bought by the OEM from its licensor.

"End User" refers to the end customer's permanent and temporary employees authorised by End Customer to use the *mobile*^{IoT} service in End Customer's name pursuant to the regulations of this EUA.

"Firmware" refers to the software and/or application programming interface embedded in the communication unit (CU) connected with the machine, including any adjustments or other derivations

thereof (by any author whatsoever), which ensure that the CU is compatible with the communication log of the machine to allow for communication between CU and machine.

"Licensor's Intellectual Property" refers to the firmware, software, data platform, web portal, the manuals and the *mobile*^{IoT} service.

"Communication Units" or **"CUs"** (short for: Communication Units) refers to the on-board hardware devices sold by the OEM to the End Customer and installed in End Customer's machines which transmit End Customer's machine data from and to the data platform and permit the End Customer and its End Users licensed access to the web portal under the subscription.

"Licensor" refers to ifm electronic gmbh or one of its affiliated companies.

"Machine" refers to a vehicle, a machine or another asset bought or leased by End Customer for business purposes from the customer or a distributor for which machine data is transmitted via the *mobile*^{IoT} service.

"Machine data" refers to: (a) the machine-readable raw data collected and transmitted to the platform by the Communication Units, and (b) the usage data on an End Customer's machines procured from such raw data by the *mobile*^{IoT} service in form of single or overall data, such as status, geographic site, operating hours, and other vehicle and machine data transmitted between the platform and the Communication Units.

"Mobile Communication Service" refers to all communication standards used by the CUs, such as LTE, 5G, or another communication service used for transmitting machine data to and from the CUs and the platform.

„mobileIoT Service" or "Service" refers to the online service provided by the software on the platform and called up by End Customers and their End Users via the web portal which presents machine data transmitted to and from the CUs installed in machines located within the territory.

"Software" refers to the software in object code format which executes the *mobile*^{IoT} Service on the data platform, including Web Portal, Realtime Client and REST API, software updates and upgrades, metadata, configuration and calibration settings and the required tools, as well as installation manuals and operating instructions and other appurtenant software documentation.

"Web Portal" refers to the website configured for the OEM's name and trademark through which the End Customers and their End Users gain online access for use of the *mobile*^{IoT} Services.

2. Grant of a limited license for the *mobile*^{IoT} Service

Starting on the date of activation and for the duration of the subscription, the OEM herewith grants the End Customer and its End Users (in the Licensor's name) a limited, cancellable, personal, non-exclusive and non-transferable:

a) licence to use the firmware,

b) licence to use the software,

c) right of access to and use of the ***mobile***^{IoT} Service via the web portal (in the scope of the service level) for the Customer's internal business purpose of allowing its End Users to monitor and control their machines, and

d) licence to use the resulting machine data generated by the ***mobile***^{IoT} Service and sorted on the data platform, the following being expressly excluded:

   i. any use by other users except the End Customer and its End Users under the subscription;

   ii. any use with CUs or other devices not licensed by the Licensor;

   and

   iii. any use for machines which are not machines of an End Customer's.

3. Licence restrictions

Neither the End Customer nor its licensed End Users are permitted to:

a) use aspects of the *mobile*^{IoT} Service or other intellectual property of the Licensor to the benefit of a third party, make them/it available to a third party, or allow third parties to use them/it;

b) transfer the *mobile*^{IoT} Service or sell, rent, loan, disclose, or use it for time sharing or outsourcing purposes;

c) use the *mobile*^{IoT} Service or other intellectual property of the Licensor to save or transmit offensive, libellous or otherwise illegal or impermissible material or to save or transmit material which violates third-party data protection rights;

d) use the *mobile*^{IoT} Service or other intellectual property of the Licensor to save or transmit malware;

e) attempt to gain unauthorised access to an aspect of the *mobile*^{IoT} Service or other intellectual property of the Licensor;

f) copy the *mobile*^{IoT} Service or other intellectual property of the Licensor in whole or in part or one or several of its features, functions, or user interfaces;

g) attempt to reverse engineer, decompile, translate, disassemble or discover the source code or basic ideas or algorithms of the Licensor's intellectual property, or to attempt to use the Licensor's intellectual property in any other manner not permitted in these Terms, or to attempt to remove or disguise copyright or trademark references or similar notices on Licensor's intellectual property.

This section 3 shall prevail after termination of this EUA.

4. Licensor's intellectual property

The limited license and the rights granted to you under section 2 do not confer any rights or ownership in Licensor's intellectual property and shall not be construed as a sale of rights in the above-described content. Subject to the limited license and the rights granted to you under section 2, the Licensor remains the owner of all rights, claims and contents from all intellectual property, including: (a) all derivations, improvements, extensions, corrections or customer-specific adjustment to the above-named contents,

irrespective of whether generated or developed by you and/or the Licensor, and (b) all suggestions, recommendations and other feedback received from your side. Nothing in this EUA shall be construed to give you a right to the source code of the software. This section 4 shall prevail after termination of this EUA.

5. Machine data

Subject to the limited license and the rights granted to you under section 2, the Licensor has the right to use the collected and anonymised machine data for marketing purposes and to improve its products and services. This section 5 shall prevail after termination of this EUA.

6. Using the usage history and profile information

With the acceptance of this EUA, whether expressly or by implication via activation of, access to or other use of the *mobile*$^{\text{IoT}}$ Service, you grant the Licensor the right to unlimited access to and use of your: (a) service account profile data and (b) usage history in connection with your use of the *mobile*$^{\text{IoT}}$ Service and the machine data ("**Usage History**"), as for as required for Licensor's configuration and/or reconfiguration of the end customer service accounts for the provision of the *mobile*$^{\text{IoT}}$ Service. Furthermore, the Licensor may from time to time aggregate your usage history with other end users' usage history and compile it in a non-personally identifiable form and share this aggregated usage history with third parties designated by Licensor.

7. Technical Support

The Licensor does not offer the End Customer or its End Users any direct technical support for the *mobile*$^{\text{IoT}}$ Service, the software, the web portal, the CUs or the remote communications service ("**Support Items**"). The OEM is solely responsible for providing technical support for End Customers and/or End Users on the term agreed upon between the OEM and the End Customer.

8. Limitation of liability

THE LICENSOR MAKES NO ASSURANCES AND DOES NOT GIVE THE END CUSTOMER OR ITS END USERS ANY WARRANTY OR GUARANTEES IN RESPECT OF THE MIOT SERVICE OR OTHER SUPPORT ITEMS. HEREWITH, ALL WRITTEN OR ORAL ASSURANCES AND WARRANTIES IN RESPECT OF THE SUPPORT ITEMS AS WELL AS IMPLICIT ASSURANCES AND GUARANTEES IN RESPECT OF THE ECONOMIC EFFICIENCY AND SUITABILITY FOR A CERTAIN PURPOSE ARE EXPRESSLY EXCLUDED. The OEM is solely responsible for the assumption (if applicable) of warranties and guarantees vis-à-vis End Customers and/or End Users for the Support Items (if applicable) under the terms agreed upon between the OEM and the End Customer. This section 8 shall prevail after termination of this EUA.

9. Limitation of liability

AS FAR AS PERMISSIBLE ACCORDING TO APPLICABLE LAW, THE LICENSOR OR ITS AFFILIATED COMPANIES ARE GENERALLY NOT LIABLE FOR ACCIDENTAL, DIRECT OR INDIRECT DAMAGE, CONSEQUENTIAL DAMAGE, PUNITIVE DAMAGES OR OTHER DAMAGE RESULTING FROM THE USE OR IMPOSSIBILITY TO USE THE MIOT SERVICE, OR IN CONNECTION WITH THE COLLECTION OF MACHINE DATA, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, ABSOLUTE LIABILITY, OR ANOTHER LEGAL FOUNDATION. THIS LIMITATION OF LIABILITY ALSO APPLIES IF THE LICENSOR OR ITS AFFILIATED COMPANIES HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGE, OR IF A LEGAL REMEDY FAILS ITS MAIN PURPOSE. This section 9 shall prevail after termination of this EUA.

10. Termination

This EUA can be terminated at any time by means of: (a) termination of the subscription, (b) termination of the mIoT Agreement between OEM and Licensor, (c) Licensor's announcement to the End Customer in case of violation of one of the conditions of this EUA by the End Customer or its End Users. In case of termination of this EUA for any reason: (a) the license granted in section 2 and all other licenses or rights conferred elsewhere in this EUA will be terminated automatically and simultaneously, and (b) you will have to immediately stop using the mobileIoT Service and Licensor's other intellectual property.

11. Applicable law, place of jurisdiction

The law of the Federal Republic of Germany shall apply without the conflict rules of international private law and excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG). Essen Regional Court is the only place of jurisdiction.

Annex 5

Agreement on data processing on behalf of the controller

between

(Customer – referred to as Controller in the following)

and

(Contractor – referred to as Processor in the following)

Preamble

Since 25 May 2018, the General Data Protection Regulation (GDPR) has been in force in the EU and accordingly also in Germany; it replaces the German Data Protection Act, as amended. In Art. 28 GDPR, this Regulation specifies binding regulations for processing of personal data by third parties on behalf of the Controller. Pursuant to Art. 28 para. 3 GDPR, processing must take place on the basis of a contract and under consideration of the contents specified therein.

In addition to "classical processing" of personal data on behalf of the Controller, where personal data is transferred to the Processor, the contract between the Controller and the Processor may cover IT maintenance or remote maintenance (e.g. error analysis, support work on the controller's systems). If these tasks involve the need or at least the possibility of access to personal data by the Processor, they are likewise to be considered a form or a part of processing on behalf of the Controller, and the requirements of Art. 28 GDPR – for example the conclusion of a contract for data processing on behalf of the Controller – must be implemented.

This Agreement substantiates the parties' obligations under data protection law in consequence of the mIoT Agreement. Regarding data processing pursuant to the terms of this Data Processing Agreement, the parties as set out in the following:

Terms and definitions

Personal data
All information relating to an identified or identifiable natural person (in the following, "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing of personal data
Any action executed with or without automated processes or any such series of processes in connection with personal data, such as collection, recording, management, organisation, saving, adjustment or modification, read-out, querying, use, disclosure by way of collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art. 4 No. 2 GDPR).

Controller

The natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data; if the purposes and means of such processing are determined by the law of the European Union or a member state, the Controller or the criteria of their appointment may be defined by Union or member state law.

Processor
A natural or legal entity, public authority, agency or other body which processes personal data on behalf of the Controller.

1. Object and duration of the commission

(1) Object

The Controller's commission to the Processor covers the following tasks and/or services:

Provision of the protected Internet portal and transmission of the machine data

Type and purpose of processing the personal data by the Processor on behalf of the Controller are described in detail in the mIoT Agreement.

(2) Duration

The duration of this commission is identical with the duration of the mIoT Agreement.

The contractually agreed data processing services shall be provided exclusively in a member state of the European Union or in other Contracting States to the Agreement on the European Economic Area.

2. Type(s) of personal data:

If you or your End Customers set up an access to our platform / our Internet portal, we shall collect the following information:

- Customer's employee(s)
  - First and last name
  - Phone number (land line and/or cell phone)
  - E-mail address
- Login times
- User actions
- Machine data
- GPS data (pseudonymized)*

*"Pseudonymization" means: The processing of personal data in such a way that they can no longer be attributed to a specific data subject without additional information, provided that this additional information is kept separately and is subject to technical and organisational measures which ensure that the personal data is not attributed to an identified or identifiable natural person.

Legal basis of processing is the fulfilment of a contract. Storage of the data for setting up your data access can be revoked at any time.

3. Technical-operational measures

(1) The Processor shall document the implementation of the technical and operational measures described and required prior to the award of the commission before to the start of the processing, in particular with regard to the specific execution of the commission, and shall hand them over to the Controller for verification. If accepted by the Controller, the documented measures shall become the basis of the commission. If the examination/audit by the Controller reveals a need for adjustment, this shall be implemented by mutual agreement.

(2) The Processor shall provide for security pursuant to Art. Art. 28 para. 3 lit. c, 32 GDPR, in particular in connection with Art. 5 para. 1, para. 2 GDPR. In general, the measures to be taken are data security measures and measures to ensure a level of protection of confidentiality, integrity, availability and resilience of systems commensurate with the risk. In doing so, the state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 para. 1 GDPR must be taken into account.

(3) The technical and operational measures are subject to technical progress and further development. Insofar, the Processor is allowed to implement adequate alternative measures. These measures must not reduce the level of security compared to the originally specified measures. Significant changes must be documented. The technical and operational measures are described in details in a separate **Enclosure** to this Agreement.

4. Rectification, restriction and erasure of data

If comprised in the scope of services, the Processor shall directly provide for an erasure concept, right to be forgotten, rectification, data portability and information in compliance with Controller's documented instructions.

5. Quality assurance and other obligations of the Processor's

In addition to the compliance with the regulations of this commission, the Processor is subject to legal obligations pursuant to Art. 28 through 33 GDPR; insofar, it shall in particular warrant compliance with the following instructions:

a) Written order by a data security officer, if specified by law.

The Processor's appointed Data Security Officer is:

Gindat GmbH – Gesellschaft für IT-Normierung und Datenschutz
Wetterauer Str. 6
42897 Remscheid

b) Maintenance of confidentiality pursuant to Art. 28 para. 3 S. 2 lit. b, 29, 32 para. 4 GDPR. The Processor shall assign the tasks only to employees who have been bound to confidentiality and have previously been acquainted with the data protection regulations relevant for them.
The Processor and any person reporting to the Processor who has access to personal data may process such data only in accordance with Controller's instructions, including the powers granted by this Agreement, unless they are legally obliged to process the data.
c) When called upon to do, the Controller and the Processor shall cooperate with the regulatory authority in the performance of its tasks.
d) The Controller shall be informed without delay of control actions and measures taken by the supervisory authority, insofar as they relate to this commission. This also applies if a responsible authority investigates in the frame of a regulatory or criminal offence procedure in connection with processing of personal data on behalf of the Controller by Processor.
e) As far as the Controller is subject to an investigation by a regulatory authority, a regulatory or criminal offence procedure, the liability claim of a data subject or a third person, or another claim in connection with data processing by the Processor, Processor shall endeavour to support the Controller.
f) The Processor regularly checks the internal processes and technical and operational measures to ensure that the requirements of the applicable data protection law are fulfilled in its range of responsibilities and that the protection of the data subjects' rights is ensured.

6. Subcontractors

(1) The Controller and the responsible institutions permit the Processor to commission subcontractors with processing of personal data. The Controller is responsible for any violations of the Agreement attributable to its subcontractors.

(2) In respect of the processing of personal data, subcontractors are subject to the same obligations as applicable to the Processor (or subcontractor-processor) when processing data on behalf of the Controller.

(3) Before selecting a subcontractor-processor, Processor shall inspect the former's measures for guaranteeing security, data privacy, and confidentiality. Subcontractor-processors can prove the use of adequate security measures by submitting security certificates. Otherwise, the Processor shall in regular intervals check each subcontractor processor's security measures for handling the data.

(4) The Processor uses subcontractor-processors at its own discretion under the condition that the following prerequisites are met:

(a) The Processor notifies the Controller in advance (via email or the Support Portal) of any changes regarding the subcontractor-processors occurring after the date this Agreement becomes final (except replacement in an emergency or deletion of a subcontractor-processor without replacement).

(b) If the Controller has a legitimate reason to object to the processing of personal data by a subcontractor-processor, Controller may object to the Processor's assignment of a subcontractor-processor by informing the Processor in writing within thirty (30) days after an notification of a change. If the Controller objects to the assignment of the subcontractor-processor, the parties shall meet in good faith to find a unanimous solution. The Processor can decide (i) not to use the subcontractor-processor or (ii) to continue using the subcontractor-processor after having taken the corrective measures specified by the Controller in its objection. If none of these options is reasonably feasible and the Controller keeps up its legitimate objection, each party may terminate this Agreement by giving notice in writing within thirty (30) days of receipt of the notification. If the Controller does not object within thirty (30) days of receiving the notification of the change, the new subcontractor-processor is considered accepted by the Controller.

(c) If the Controller's objection has not been cleared within sixty (60) days of raising and if the Processor has not received any notice of termination, the new subcontractor-processor is considered accepted by the Controller.

(5) The Processor may replace a subcontractor-processor if the reason for the replacement is outside of the Processor's range of control. In this case, the Processor shall inform the Controller as soon as possible about the new subcontractor-processor. According to section 6 (5) (b), the Controller has the right to object to a new subcontractor-processor.

7. Controller's control rights

(1) The Controller has the right to carry out inspections in consultation with the Processor or to have them carried out by inspectors to be appointed in individual cases. It the right to verify by means of spot checks, which must normally be notified in good time, compliance with this Agreement on the part of the Processor at its premises. Making available the Processor's employees within the scope of such an inspection is free of charge up to a volume of four hours/year, from the fifth hour onwards the Processor is entitled to demand reasonable remuneration.

(2) The Processor ensures that the Controller can convince itself of the fulfilment of the Processor's obligations pursuant to Art. 28 GDPR. The Processor undertakes to give the Controller on request the required information and above all to submit proof of the implementation of the technical and operational measures.

(3) Alternatively, the Processor can fulfil its obligations pursuant to paragraphs 1) and 2) by:

- compliance with approved codes of conduct pursuant to Art. 40 GDPR
- certification pursuant to an approved certification mechanism pursuant to Art. 42 GDPR

- current certificates, reports or excerpts from reports of independent authorities (e.g. certified public accountants, audits, data security officers, IT security department, data protection auditors, quality auditors)
- suitable certification by IT security or data protection audit (e.g. pursuant to BSI-Grundschutz, DIN-ISO 27001).

8. Notification in case of violations by the Processor

(1) The Processor shall support the Controller in complying with the obligations specified in Art. 32 to Art. 36 GDPR for the protection of personal data, notification of a personal data breach to the supervising authority, data protection impact assessments, and previous consultations. This includes without limitation:

a) ensuring an adequate level of protection by technical and operational measures that take into account the circumstances and purposes of the processing operation and the predicted probability and severity of a possible breach of rights by security flaws and allow for the immediate detection of relevant breach events
b) the obligation to report personal data breaches immediately to the Controller
c) the obligation to support the Controller in the context of its duty to inform the data subject and to provide it without delay with all relevant information in this connection. The Processor has the right to charge a reasonable fee for this service.
d) supporting the Controller in its data protection impact assessment
e) supporting the Controller in the frame of previous consultations with the supervisory authority

(2) The Processor may charge a fee for support services not comprised in the specification of services or not attributable to Processor's fault.

9. Controller's authority to issue directives

(1) The Processor shall process the Controller's personal data only according to the Controller's directives. The Controller shall immediately confirm oral directives (minimum requirement: written form).

(2) The Processor shall immediately inform the Controller if it thinks that a directive is in violation of data protection law. The Processor has the right to suspend the execution of the respective directive until confirmed or changed by Controller.

10. Erasure and return of personal data

(1) No data shall be copied or duplicated without the Controller's knowledge. This shall not apply to backup copies as far as they are required to ensure due data processing, as well as to data required to be archived pursuant to statutory obligation to retain data.

(2) Upon completion of the contractually agreed work or earlier upon request by the Controller – at the latest upon termination of the service agreement - the Processor shall hand over to Controller all documents that have come into its possession, generated processing and usage results, as well as data stocks connected with the contractual relationship, or destroy them in accordance with data protection laws upon prior consent. This also goes for test material and rejected material. Erasure or deletion must be confirmed upon Controller's request. Any additional costs incurred by the Processor due to handover or erasure of data shall be borne by Controller.

(3) The Processor shall retain any documentations evidencing due data processing in keeping with the commission beyond the end of the Agreement in compliance with the respective retention periods. For its convenience, Processor may hand over such documentations to Controller at the termination of the Agreement.

11. Obligation of secrecy

(1) Both parties undertake to treat all information they receive in connection with the execution of this Agreement as confidential for an unlimited period of time and to use it only for the execution of the Agreement.

(2) The aforementioned obligation does not apply to information which one of the parties has demonstrably received from third parties without being obliged to maintain secrecy or which is publicly known.

12. Final provisions

(1) The written form is required for side agreements.

(2) Should individual parts of this Agreement be invalid, this shall not affect the validity of the remaining provisions of the Agreement.

Enclosure to the Data Processing Agreement (DPA)

IT security concept – Technical and operational measures

Organisations which collect, process or use personal data for themselves or on behalf of another party must take suitable technical and operational measures required to ensure compliance with the data protection law regulations. Measures are only required as far as their cost is proportionate to the protection objective pursued. The Processor meets this requirement by way of the following measure(s) / IT security concept:

1. Legal framework

Compliance with the applicable statutory regulations or binding directives of other institutions must be ensured. All measures necessary for this will be documented in a suitable place and published. The software used in the company must be licensed pursuant to the legal requirements, the appurtenant documentation must be kept up-to-date.

2.**Workstations**

2.1_Obligation / Sensitisation

Every IT user is obligated to adhere to statutory provisions and internal guidelines. Besides taking note of and implementing corresponding information, this also involves raising awareness to avoid and recognise faults which can result from violations of IT security guidelines.

2.2_General utilisation policy

- authorised use is only permitted for business purposes
- only authorised software may be used
- the use of private hard- and software is only permitted with express consent
- changes to system settings, particularly installations, uninstallations and configuration changes to the basic system may only carried out by administrators

2.3_Identity management

To manage and control the various authorisations and to ensure these are used correctly, comprehensive identity management must be set up. This must include complete documentation of the following minimum information for each user, which must be kept up-to-date:

- Assets (provision of hardware and software licences)
- Criticality of the workstation (relation to business process)
- Authorisations (access authorisations)

Furthermore, processes must be defined which regulate the setup and the withdrawal of IT users.

2.4_Physical and virtual access policy

The workstation must be kept tidy, so that unauthorised persons are not able to gain access to information or applications. Separate regulations apply. As a mandatory and fundamental security measure, the disclosure of user IDs and passwords and other means of authentication is forbidden. If there is a suspicion that access authorisations are being used without permission by a third party, appropriate measures must be taken to re-establish the confidentiality of these authorisations. An overview must be prepared and kept up-to-date listing the authorisations of every user, in particular access to data and information classified as "confidential".

2.5_Password policy

In internal password directive is in place. The administration is urged to establish suitable technical measures so that adherence is comprehensible and simple for users and operating errors are excluded.

2.6_Security updates

The security settings of all IT systems provided to remedy weak points must be kept up-to-date ("Security Updates").

2.7_Virus protection
Active and up-to-date antivirus protection must be ensured for all IT systems. The configurations may neither be deactivated nor changed by users. Each and every electronic data carrier must be checked for viruses and other malware before use.

2.8_Encryption
Encryption, for which there is an internal classification directive, is of particular importance.

2.9_Emergency service
Each user must regularly back up files which are not or cannot be backed up by central mechanisms. In this context, it is imperative that encryption is used for data backup and that the data carriers are stored safely and check for readability in sufficient intervals.

3. Central systems and networks

3.1_Availability
Depending on their function within the business processes and the agreements with users or user groups of the systems, special availability must be ensured for certain users/user groups.

3.2_Monitoring
Monitoring is to be set up which allows operational irregularities to be detected within an appropriate time. The focus is on monitoring availability, secure communication and the integrity of data. Proper logging and evaluation of relevant processes, also of user activities, must be provided in the frame of statutory regulations. Furthermore, proof that SLAs are being adhered to and an overview of occurrences relevant to security is to be provided by way of monitoring (reporting).

3.3_Access policy
The policy regarding access to the Processor's network from public networks is of special significance. Access regulations are differentiated and must be carefully monitored.

3.3.1_Physical access
Access to local networks, either wired or wireless, must only be possible for authorised persons or systems with clear authorisation. The provision of open access points is only permitted if it has been established that no components relevant to security are affected. Besides physical systems and applications, this particularly includes internal data and information.

3.3.2_Authentication
Each user of the Processor's infrastructure must provide unambiguous authentication (personalised login). Since the authentication also control users' entitlements, so-called group logins, i.e. several users logging in under the same ID, are only allowed in specific exceptional cases. The governing regulations (e.g. the internal password policy) must be observed.

3.3.3_Authorisation
Unsupervised or unlogged access to data and information in the "confidential" or "strictly confidential" classes must be prevented. Requests for access to information in these classes may only be processed in consultation with the owner of the information.

3.4_Data security concept
All data must be backed up in a suitable manner. Depending on its criticality in the event of loss, the volume, frequency, storage, recoverability requirements and any special features must be considered.

3.5_Change management
Any change to the IT infrastructure can affect the protection objectives and may only be carried out following corresponding planning and preparation.

3.6_Desaster recovery
The measures included as part of "disaster recovery" concern faults which fall outside the scope of faults to be expected (catastrophes). The associated specific and comprehensive measures can have a significant bearing on other organisations, processes and guidelines. The basic concept for such cases is compiled separately.

4.External security

The area of external security covers all connections between IT components and public environments. The focus is on the central transitions of an internal network into a public network and the access of individual workstations into the internal network.

4.1 Physical access policy

The requirements listed with regard to workstation security apply in equal measure to building protection. Particularly in security-critical areas, external persons must be supervised constantly. Depending of protection requirements, further restrictive measures are to be implemented.

4.2_Access control / monitoring

Only gateways which prevent unauthorised access and possess logging capabilities which allow attempts of this kind to be detected are permitted. The IT administration must ensure that only known and authorised persons have access to the network. Corresponding documentation and control procedures must be established. External third parties may only obtain access if measures are put in place which allow access to be controlled and permit immediate prevention, where necessary.

4.3 Internet

In the context of security considerations, considerable importance is attached to the gateway to the Internet. It must be ensured that no undetected or unauthorised access to internal IT components, particularly data, is possible from the Internet. If unauthorised access is detected, immediate measures must be taken to prevent it.