

GENERAL CONTRACTING TERMS AND CONDITIONS OF REMOTE SURVEILLANCE
for the remote surveillance of objects
guarded with an electronic intrusion alarm system or with a stand-alone fire alarm system

PART I

The General Contracting Terms and Conditions of Remote Surveillance (GCTCRS) include the general terms and conditions of the Remote Surveillance Contract (RSC) between Securitas Security Services Hungary Limited Liability Company, as Contractor (the 'Contractor') and the Principal using the remote surveillance property protection service (the 'Principal'), (the Principal and the Contractor hereinafter jointly referred to as 'Parties').

The rights and obligations of the Parties shall be interpreted on the basis of the joint content of the GCTCRS and the RSC (together the "Agreement"). The GCTCRS is an inseparable part (annex) of the RSC.

The Contractor shall send a written notice to the Principal about the amendment of the GCTCRS if it affects the provisions of the contract concluded for the supply of the service used by the Principal, at least 30 (thirty) days before the changes take effect. If the Principal does not object to the changes within 30 (thirty) days from the receipt of the notification, it shall be deemed acceptance by the Principal.

This Agreement shall commence upon the effective date as specified in the RSC. ("Effective Date")

If any Services are provided prior to the Effective Date, this Agreement shall apply to such Services.

I. Definitions

The following terms used in the RSC, its annexes and the GCTCRS shall be used in the following sense:

1. Agreement

Agreement means these General Contracting Terms and Conditions for Remote Surveillance and the Remote Surveillance Contract.

2. Effective Date

Effective Date means the date specified in the Remote Surveillance Contract.

3. Principal

The natural or legal person who uses the object remote surveillance service (hereinafter: the Service) on the basis of the contract and pays its fee.

4 Sanctions

Sanctions means economic or financial sanctions or trade embargoes or other equivalent restrictive measures imposed, administered or enforced from time to time by the European Union, the governments of other member states of the European Union, the United Nations Security Council, the United States government or an United States agency (including OFAC, the US State Department, the US Department of Commerce and the US Department of Treasury) or the equivalent regulator of any other country which is relevant to this Agreement.

5. Sanctions List

Sanctions List means any of the lists of specifically designated nationals or designated persons or entities (or equivalent) in relation to Sanctions, each as amended, supplemented, or substituted from time to time.

6. Local electronic intrusion alarm system or stand-alone fire alarm system (hereinafter: local system)

An electronic intrusion detection system (alarm system) or an independently operating fire alarm system (fire alarm system) in the remotely monitored object, which is the property of the Principal or for which the Principal has the right of use. Components: sensors, network, programmable alarm or fire control panel with or to which a communicator is connected, control unit, sound and light signalling equipment.

7. The remotely monitored object

The object where the local system is installed.

8. Remote Surveillance Centre

The object where the Contractor receives and registers the signals of the local system through an intermediate contractor and takes the measures undertaken in the contract continuously, 24 (twenty-four) hours a day in the remote surveillance dispatch centre operated by the Contractor (remote surveillance or dispatch centre).

8. Intermediate service provider

The telecommunications Contractor through whose network (fixed line, GSM, GPRS) the signals of the local system are received in the remote surveillance centre.

10. Signalling

Electronic signals related to local system status changes and alarms that can be used to identify on-site events.

11. Alarm signal

Types of alerts that trigger an immediate action of the dispatcher when they are received at the remote surveillance centre. Such signals include intrusion (burglary), attack (panic), forced shutdown, fire, sabotage, and medical assistance.

The sensors of the electronic signalling system indicate abnormal, unwanted states of the remotely monitored objects and spaces, as well as any signals of the protected person (e.g., attack signal) and transmit them to the system control panel (alarm control panel), which transmits the signals to the remote surveillance centre through the repeater channel(s).

12. Alarm not requiring an action

If a break-in alarm is received during the day (6:00-22:00) from a malfunction of the Principal's local system and is followed by opening with the correct code within one minute, the alarm does not qualify as a sharp alarm and is not followed by any action by the Contractor.

13. Call-out action group

A group of security guards with the licence and rights specified in the Act CXXXIII of 2005 on the Rules of Security Services and the Activities of Private Investigators (hereinafter: 'Property Protection Act'), whose task is to prevent, eliminate or mitigate personal injuries and property damage as much as possible.

14. Partition

With the help of programming, the alarm system can be divided into "smaller alarms", which can be switched on and off independently. The partitions (areas) created in this way can be switched on and off separately with a code authorised for one partition.

15. Basic service according to how the signal is sent and received

15.1. Landline telephone service (hereinafter: fixed line service)

Receiving signals from sensors and/or keypads (keypads) sent on the fixed line by the control panel of the local system installed in the remote monitoring objects to the remote surveillance centre.

The various signals sent by the local system to the remote surveillance centre generate traffic on the telephone line, the costs of which appear on the Principal's telephone bill.

15.2. GSM service

A GSM communicator will be (was) installed next to the local system, with the help of which the signal will only arrive at the Contractor's dispatcher centre only via the GSM network. The transmission of signals generates GSM traffic at the intermediate Contractor, the fee for which is included in the fee for the remote surveillance service for up to 100 connections per month.

In the case of the GSM service, the SIM card is the property of the Contractor, the GSM communicator can be purchased by the Principal.

15.3. GPRS service

A GPRS communicator will be (was) installed next to the local system, with the use of which the signal will arrive at the Contractor's dispatch centre via the GPRS network or, in the case of failure, via the secondary (back up) GSM network. The transmission of signals generates GPRS and GSM traffic at the intermediate Contractor. The fee for GPRS traffic up to 10 Mbytes / month for data traffic, and the fee for GSM traffic up to 100 connections per month will be included in the fee for the remote surveillance service.

In the case of the GPRS service, the SIM card is the property of the Contractor, the GPRS communicator can be purchased by the Principal, at a previously agreed price.

The GPRS service can be requested with 3 different, optional line test signal frequencies, which are the following:

In the case of the basic GPRS service, a line test signal is sent every 4 (four) hours from the Principal's local system to the Contractor's dispatch centre. In the event of a GPRS network failure, the secondary (backup) GSM repeater signalling is only used for the transmission of alarm signals, but not for the transmission of a line test signal.

In the case of the GPRS enhanced service, a line test signal is sent every 1 (one) hour from the Principal's local system to the Contractor's dispatch centre. In the event of a GPRS network failure, the secondary (backup) GSM repeater signalling is only used for the transmission of alarm signals, but not for the transmission of a line test signal.

In the case of the GPRS priority service, a line test signal is sent every 10 (ten) minutes from the Principal's system to the Contractor's dispatch centre. In the event of a GPRS network failure, the secondary (backup) GSM repeater signalling is only used for the transmission of alarm signals, but not for the transmission of a line test signal. In the case of stand-alone fire alarm systems, only the GPRS priority line test signal is used (The frequency of the line test signal is recorded in the RSC.)

The GPRS service can be requested with 2 different, optional alarm control panel test signal frequencies, which are the following:

- In the case of the basic service, an alarm control panel test signal is sent every 4 (four) hours from the Principal's local system to the Contractor's dispatch centre. In the event of a GPRS network failure, the secondary (backup) GSM repeater signalling is only used for the transmission of alarm signals, but not for the transmission of an alarm control panel test signal.
- In addition to the basic service, the alarm control panel test signal with a frequency of less than 4 (four) hours can be selected as an ancillary service (optionally requested, i.e., not a basic service).

(The frequency of the alarm control panel test signal is specified in the RSC.) In the local control panel, the alarm control panel test signal is set by the installer at the time of connecting the remote surveillance system, based on the special order of the Principal.

15.4. Combined fixed line and GSM/GPRS service (hereinafter: combined service)

A GSM/GPRS communicator will be (was) installed next to the local system suitable for the fixed line remote surveillance service. The signals are transmitted by the local system primarily on the fixed line. In the event of a fault in the fixed line, the GSM/GPRS communicator provides a secondary (backup) signal transmission option. One of the advantages of the combined service is that through line voltage monitoring, the GSM / GPRS communicator immediately detects a fault in the landline telephone line and switches to the GSM/GPRS signal transmission mode.

The various signals sent by the local system to the remote surveillance centre generate traffic on the telephone line, the costs of which appear on the Principal's telephone bill.

The fee for GPRS traffic up to 10 Mbytes / month for data traffic, and the fee for GSM traffic up to 100 connections per month will be included in the fee for the remote surveillance service.

In the case of the Combined Service, the SIM card is the property of the Contractor, the GSM/GPRS communicator can be purchased by the Principal.

16. Technical conditions of using the remote surveillance service

16.1. Technical conditions for using the fixed line service

(Signal reception only for the intrusion detection system.)

The Principal must have the following in the remotely monitored object:

- analogue land-line telephone line
- a local system (alarm) capable of communicating with the remote surveillance centre.

A fixed line service may be provided to a Principal with an ISDN line if they have an uninterrupted, analogue, free access point.

No fixed line service can be provided in the case of RLL and twin telephone exchanges.

In the case of a UPC cable telephone network, the alarm can only be connected with a fixed connection to a line adapter with a minimum of 72 (seventy-two) hours of uninterrupted connection.

In connection with a telephone line that can be used to transmit the signal, the Principal may not use call barring, call waiting and voice announcement services.

The remotely monitoring object may not have devices on the telephone line used for signal transmission in front of or parallel with the alarm control panel, e.g., fax, handset, PBX.

16.2. Technical conditions of using the GSM service

(Signal reception only for the intrusion detection system.)

The Principal must have a local system (alarm) in the remotely monitored object that can communicate with the remote surveillance centre.

The GSM service may be used if the signal strength in the vicinity of the remotely monitored object is sufficient and continuous.

Within the scope of the RSC, the SIM card and the GPRS subscription are provided by the Contractor to the Principal. In the case of GSM services, a GSM communicator must be installed next to the local system, which is purchased by the Principal when requesting the GSM service.

In the case of the GSM remote surveillance service, the GSM communicator is provided to the Principal by the Contractor. If the remotely monitored object is not the property of the Principal, a "Statement of Consent" is required from the owner of the object, which allows the Contractor to enter the object in order to install and dismantle or remove the GSM communicator.

16.3. Technical conditions of using the GPRS service

(The Principal accepts the remote surveillance of stand-alone fire alarm systems and assumes responsibility for the service only with this signalling method.)

The Principal must have an intrusion detection system in the remotely monitored object that can communicate with the remote surveillance system in CID format.

The GPRS service may be used if the signal strength in the vicinity of the remotely monitored object is sufficient and continuous. Within the scope of the RSC, the SIM card and the GPRS subscription are provided by the Contractor to the Principal.

In the case of GPRS services, a GPRS communicator must be installed (which is a special type of GSM communicator) next to the local system, which the Contractor provides to the Principal within the scope of the RSC.

If the remotely monitored object is not the property of the Principal, a “Statement of Consent” is required from the owner of the object, which allows the Contractor to enter the object in order to install and dismantle or remove the GPRS communicator.

16.4. Technical conditions of using the combined service

In order to use the combined service, the combined conditions for the use of the fixed line and GSM/GPRS service must be fulfilled.

When requesting a combined service, the GSM/GPRS communicator is provided to the Principal by the Contractor within the scope of the RSC.

In the case of a combined service, if the remotely monitored object is not the property of the Principal, a “Statement of Consent” is required from the owner of the object, which allows the Contractor to enter the object in order to and dismantle or remove the GSM/GPRS communicator.

II. Conclusion of the contract

- Of the contract and its annexes, the Password form is made in two copies, the first copy of which shall be kept by the Contractor and the second copy shall be kept by the Principal. The GCTCRS form an inseparable part (annex) of the RSC, the receipt and acceptance of the contents of which are acknowledged by the Principal by signing the RSC.
- When the call-out service is used, in order to support the effective action required at the time of the alarm, the Contractor shall conduct an on-site inspection at the remotely monitored object at the time of the connection but no later than within one week. During the on-site inspection, the patrol officer of the call-out service shall record in writing the circumstances affecting the measure on the spot (risk assessment). The risk assessment is not annexed to the contract.

III. Scope and Modification of the Contract

1. Geographic scope of the Contract

- The Contractor undertakes the notification service for receiving signals from local systems installed in objects located in the territory of Hungary.
- The geographical area of the call-out services within Hungary is determined by the agreements between the call-out service and the Contractor. The performance of the call-out service is assessed individually by the Contractor.
- The Parties shall limit the territorial scope of the contract to areas covered by the sensors of the local system.

2. Term of the Contract

- The contract is concluded for an indefinite period of time and enters into force in the 24th (twenty-fourth) hour after the connection to the remote surveillance system (signing of the Certificate of Performance).
- The Datasheet is signed by the installation specialist connecting the local system to the Contractor's remote surveillance centre and the Principal's representative present at the time of connection. The Datasheet is not an annex to the contract, but its data content affects the conditions for the performance of the service. The Principal and the Contractor mutually accept the data declared by the Principal's representative in charge of connection supervision.
- The successful connection of the local system to the Contractor's remote surveillance system may precede the completion and signing of the contract and its annexes. In this case, if sufficient information is available to receive the signals and take action, the Contractor will provide the service immediately, but will only be liable for damages after the contract enters into force.
- The basic condition for the supply of the service is the full completion of the Datasheet or sending all the corresponding data content to the Contractor, as well as the functionality of the alarm system and the routes providing the signalling.

3. Amendment of the Contract

- The Contract may be amended by mutual agreement of the Parties in writing.
- The Principal shall notify the Contractor in writing of any contract amendment request at least 3 (three) working days in advance, e.g., password change. If the contract amendment requires the construction of a new technical facility (the use of another additional service) the amendment (in case of acceptance by the contractor) shall take effect from the 2nd (second) working day following the documented construction of the new technical facility.
- The Contractor shall notify the Principal in writing of any contract amendment request at least 15 (fifteen) working days in advance. An exception to this is the Contractor's proposal for an amendment relating to a fee increase, in which case the Principal must be notified in writing at least 60 (sixty) days in advance.

4. No guarantee

Contractor does not guarantee a function or result of the Services or accept overall responsibility for the security at the Principal's Site. Unless otherwise agreed in this GCTCRS, Contractor is not engaged as a security consultant. Contractor makes no representation, express or implied, that its Services will prevent any loss or damage.

IV. Payment terms and fees

The Contractor shall invoice the Principal for regular, one-off and occasional fees (hereinafter together: Service Fee) in connection with the performance of the remote surveillance service and the related service elements.

The Principal undertakes to pay the Service Fee according to the following conditions:

- Method of fee payment: regular and one-time, as well as ad hoc fees must be paid by postal check or bank transfer.
- The frequency of payment of regular fees is recorded in the RSC and can be monthly, quarterly, semi-annually and annually, taking into account calendar periods.
- The payment deadline: 15 (fifteen) days after receipt of the invoice.
- The fees for the remote surveillance basic and ancillary service selected by the Principal are stated in the RSC.
- Regular fees are due in advance, at the beginning of the period according to the chosen fee payment frequency. After connection, the first fee instalment will be billed in proportion to the number of days remaining from the fee payment period in the month of connection.
- The fees do not include the fees for the repair and maintenance of local systems. If the Contractor undertakes to eliminate a local system fault, or maintain the local system, it shall do so on the basis of a separate agreement and remuneration.
- The date of payment is the day on which the money is credited to the Contractor's bank account.
- In the event of arrears in fee payment, the Principal shall pay the default interest as stated in the Civil Code in force at any time.

- The deadline for investigation of and responding to invoice-related complaints by the Contractor is 30 (thirty) days.
- On 1 April of each year, the Contractor is entitled to increase the service fee at the rate of inflation (indexation) of KSH for the previous calendar year. When a loyalty period is stipulated, the Contractor provides the Principal a discounted fee from the list price and the annual indexation will be validated during the loyalty period as well.
- If the GSM/GPRS communicator develops a fault because the Principal does not use them properly or the Principal does not ensure the dismantling of the GSM/GPRS communicator owned by the Contractor, the Principal shall pay 1.5 times the amount of the current new purchase price of the GSM/GPRS communicator and the originally agreed call-out fee with an 8 (eight) day payment deadline.

Service Fee adjustments

The Contractor has a right to amend the Service Fee at any time in the following cases in addition to adjustment due to inflation:

if the costs for the provision of the Services increases, due to:

- increased costs for producing the services including all labour costs
- changes in legislation or regulations relating to the Services
- increased production costs or increase prices from manufacturer

VAT and other taxes

All sums payable under the Agreement are exclusive of VAT and any other applicable tax or duty, which shall be payable in addition to the specified Service Fees.

V. Termination of the Contract

1. Ways and cases of termination of the contract

- Termination by either party with 60-day (sixty) notice without justification.
- With extraordinary termination by, with immediate effect:
- In the event of termination of the contract with the intermediate service provider or exclusion from the telecommunications service.
- In the case of proven loss of interest or impossibility of performance, at the time of the loss of interest or impossibility of performance (the object is sold or used by a third party, or there is a change of ownership under any title, bankruptcy or liquidation proceedings are initiated against the Principal, death of the Principal, etc.).

2. Termination of the contract by the Principal

- The Principal may terminate the contract at any time in writing, without justification, with a notice period of 60 (sixty) days, which shall terminate the contract in the 24th (twenty-fourth) hour of the last day of the period. The calculation of the notice period begins when the Contractor receives the notice.
- The Principal may terminate the contract in writing with an extraordinary notice and immediate effect if the Contractor commits a serious breach of contract and does not remedy it within 15 (fifteen) days despite the Principal's written request.
- If the Principal unlawfully terminates the contract with immediate effect or fails to comply with the notice period upon ordinary termination, the Principal shall pay a penalty equal to three-quarters of the fee for the one-year contract period to the Contractor.

3. Termination of the contract by the Contractor

- The Contractor may terminate the contract at any time in writing, without justification, with a notice period of 60 (sixty) days, which shall terminate the contract in the 24th (twenty-fourth) hour of the last day of the period. The calculation of the notice period begins when the Contractor receives the notice.
- The Contractor may terminate the contract in writing with extraordinary termination and immediate effect if the Principal does not or did not use properly the devices supporting the use of the service and are owned by the Contractor. The termination may take immediate effect if the Principal does not terminate such abnormal use following the Contractor becoming aware of it and communicating it and/or does not declare in writing within 3 (three) working days the method of compensation for the damage incurred.
- The Contractor may terminate the contract in writing with extraordinary termination, with immediate effect, if justified or requested by an authority.
- The Contractor may terminate the contract in writing with extraordinary termination, with immediate effect, if the Principal incurs a fee debt exceeding 30 (thirty) days and the Principal does not pay it despite the written notice of the Contractor. The Contractor may terminate the contract with extraordinary termination in writing with immediate effect if the Principal commits another serious breach of contract in addition to the above, and the Principal does not remedy it within 15 (fifteen) days despite the Contractor's written request.
- If the Contractor exercises the right of extraordinary termination as described above (except in the case described in indented paragraph 3), the Principal shall pay to the Contractor a penalty equal to 75% of the fee for a one-year contract period.
- The Contractor may terminate this Agreement for cause by giving not less than ten (10) days prior written notice to the Principal if:
 - the Principal commits a material breach,
 - there is a change in applicable laws or regulations that has a material effect on, or causes a material change to, the obligations of the Contractor under Agreement,
 - if the other Party becomes insolvent an application for insolvency procedure or similar has been submitted by or against the company,

Relating to Sanctions. If it is or becomes unlawful, or contrary to any law, enabling legislation, executive order or regulation in relation to Sanctions, for the Contractor to perform any of its obligations under this Agreement, or if the Principal or its direct or indirect owner is added to a Sanctions List:

a The Contractor may, in its absolute discretion cease performing its obligations under this Agreement immediately and/or terminate this Agreement; and

b The Principal agrees that the Contractor will not be liable to the Principal for any loss (including any consequential loss), damage or delay whatsoever as a result of Contractor ceasing to perform its obligations and/or terminating this Agreement in accordance with Article the above.

4. Commitments made at the cessation of the contract

- The Contractor shall monitor and take action on the signals received from the remotely monitored object until the 24th (twenty-fourth) hour of the day of termination of the contract.
- The programming of the local system from the remote surveillance centre is the responsibility of the Principal, the cost of which is also borne by the Principal.
- If the Principal terminates the contract before the expiry of the loyalty period, or it is terminated or its performance becomes impossible by the Contractor due to a reason attributable to the Principal or in the Principal's interest, the Principal shall pay the full service fee for the remaining time of the loyalty period in a lump sum as penalty and shall return the GSM/GPRS modem and SIM card and pay the individually determined call-out service fee, within 8 (eight) days after the receipt of the invoice.
- In the case of GSM/GPRS services, the Contractor shall disconnect the communicators owned by them from the remotely monitored local system. The Principal shall designate a time interval of 2 (two) hours for the Contractor for access to the remotely monitored object, removal and removal of the SIM card and GSM/GPRS, at least twice on working days within 2 (two) weeks after the termination of the contract. The Contractor determines the call-out service fee individually. If the Principal does not provide the conditions for access and work necessary for dismantling, the Principal shall pay 1.5 times the amount of the current

new purchase price of the SIM card and the GSM/GPRS communicator and the originally agreed call-out fee with an 8 (eight) day payment deadline. (The price of the new GSM or the new GPRS communicator is included in the price list of the current remote surveillance services applied by the Contractor.) The Principal undertakes to facilitate the dismantling and removing the Contractor's devices even in the case of loss of interest.

VI. Responsibility related to the remote surveillance service and its extent

1. Notwithstanding anything to the contrary in this Agreement, the Contractor's aggregate obligation to indemnify the Principal under this Agreement for damages caused by the Contractor's breach of this Agreement, due to the Contractor's fault or negligence, shall be limited as follows:

- a. if the Principal has property insurance for the real property and movable assets in it, its nature (general movables, special movables, cash, valuables, etc.) and storage conditions (according to MABISZ's recommendation and insurers' regulations), the proven damage not reimbursed by the insurer but not exceeding HUF 2,000,000;
- b. if the Principal does not have the property insurance according to paragraph a), the proven damage, but not exceeding HUF 50,000.

The Principal shall notify the Contractor of any claim within 5 working days after becoming aware of the occurrence giving rise to the claim. The Principal acknowledges that if the Principal fails to provide such notice to the Contractor within that time period, the Contractor shall have no obligation to make any payment whatsoever relating to such claim. The condition for assessing the claim is that the Principal reports the crime to the police and attaches a site inspection report prepared by the police.

2. The Contractor shall be liable for the damage caused by a criminal offense or the preparation or attempt thereof, and which has occurred or can be traced back only to the breach of contract by the Contractor; thus, the Contractor is not liable in particular for the damage that would have occurred even if the Contractor had acted in accordance with the contract. The Contractor's liability covers damage to the property and movable property stored there but is always subject to the liability cap set out in Clause 1 and 3. The Contractor shall in no event be liable for indirect and consequential damages and lost property benefits. For the avoidance of any doubts the liability is only fault and negligence based.

3. The Contractor limits its liability for damage and loss in cash, in cash substitutes, valuables (securities, deposit books, documents, precious stones, precious metals, pearls, collections of coins and stamps, jewellery, gold and platinum objects) and in fine and applied arts objects (for which the Contractor is liable only if they have property insurance according to Section 1 a)) within the value limit specified in Section 1 a), according to the following indemnity limits:

cash, cash substitutes not stored in a vault: up to HUF 50,000; when stored in a vault, up to the limit recommended by MABISZ in "Recommended underwriting limits for vaults for insurers" but not more than HUF 2,000,000;
valuables not stored in a vault: up to HUF 250,000; when stored in a vault, up to the limit recommended by MABISZ in "Recommended underwriting limits for vaults for insurers" but not more than HUF 2,000,000;
for fine and applied art objects up to HUF 2,000,000, provided that the Principal has an invoice for them or another document that authentically proves the value of the assets, in the absence thereof, up to HUF 1,000,000.

4. In the case of properties not situated in a residential area or non-residential Properties (suburban area, enclosed garden, holiday home, etc.), the Contractor's liability for damages is limited to 50% of the amounts specified in Section 1 a) and Section 3.

5. The Contractor shall not be liable for indirect damages, such as lost income, revenue, lost market, damages resulting from data loss, data violation, loss of production or services, loss of profit or other similar losses incurred by the Principal or a third party.

The Contractor shall not be obliged to indemnify for damage caused by incomplete or inaccurate information provided by the Principal, or for other reasons within the Principal's responsibility, and caused by a person not included in the Contractor's staff but acting on behalf and in the name of the Principal.

The exclusion or limitation of the Contractor's liability does not apply to damage where the law prohibits the exclusion or limitation of liability.

The Principal is responsible for ensuring that the underlying information to provide security services (scope of work) are complete and accurate.

Indemnification

The Principal shall indemnify and hold Contractor harmless from and against any Losses, which Contractor may incur or which may be made against Contractor by any third party as a result of or in connection with the performance of the Contractor under the Agreement unless such Losses arise from any negligent act or omission on the part of Contractor, its employees, agents or subcontractors.

6. Personnel

Personnel providing the services are Contractor employees or sub-contractors hired by Contractor. Contractor shall have the right to change personnel assigned for the Services at any time. Principal may request changes in Contractor personnel, but Contractor in its sole discretion will determine any actions to be taken based upon such a request. Principal requests to change personnel shall be made in writing, stipulating the reasons for requesting the change.

The Contractor is exempt from liability in the following cases:

- If the damage is due to the fault of the telecommunications (intermediate) service providers (including the sabotage and cutting of the telephone cables), or the faulty service of the electricity service providers, or permanent (more than 1 hour) unavailability of service.
- For signal failures caused by faults in the local electronic signalling system owned or operated by the Principal and for damage events occurring for reasons listed below. Such causes may include: improper, unauthorized, or unprofessional handling, damage for any reason, natural forces, off-mode of the local system, or other local faults outside the remote surveillance centre.
- The basic service of 15 (fifteen) minute call-out action or other time-limited call-out service is selected, any event within the first fifteen minutes from the detection of the alarm signals received from the remotely monitored object to the computer in the Contractor's remote surveillance centre, or until the agreed time limit.
- The Principal fails to comply with the obligation to change the data in the data concerning the remote surveillance service, at all or beyond the agreed deadline and this will lead to the occurrence of the damage. (E.g.: change of person to be notified, change of address or telephone number, expansion of local system, change of security conditions, etc.)
- The Principal does not notify the Contractor in writing of the claim for compensation within 6 (six) months.
- The Principal fails to provide the information referred to in Part I, Section VII/5.
- The Principal did not provide access to the area of the object to the call-out team, the official and/or other special permits necessary for entering the area, and thus the necessary security check of the object could not be performed by the call-out service patrol officer.
- At the time of the given damage event, no authentically recorded log of the opening and closing times for the period of the damage event is available. (The Principal does not require the remote surveillance of the opening and closing reports, or prevents the reading of the opening and closing times from the event log of the local alarm system after a damage event.)
- In the case of with fixed line, GSM services, at least one alarm control panel test signal per day is not received from the Principal's local system, or at least one in every 4 (four) hours in the case of GPRS basic service, or at least one in every 1 (one) hour in the case of GPRS enhanced service, or in the case of GPRS priority service no identifiable line test signal is received at least every 5 (five) minutes at the Contractor's remote surveillance centre.
- The Principal provides the SIM card at its own expense, and it is a top-up (non-subscription) card and there is no amount available on the card due to the sending of signals and the GSM service provider does not transmit the signals from the local system to the remote surveillance centre.

- In the event of a service interruption requested by the Principal or due to the expired debt of the Principal, or in the event of damage events reported by the Contractor or occurring during the period of extraordinary shutdown independent of the Contractor
- The Principal defines less than two persons to be notified, and the persons to be notified specified in the RSC are not accessible.
- Damages recovered from elsewhere for the Principal. (The Principal has property insurance, on the basis of which it receives compensation from its insurer. The Contractor's liability for damages does not extend to the amount paid by the Insurer.)
- If the damage occurred because the Principal did not inform the Contractor of the replacement of the affected locks or the change of the access method (e.g., a new gate code and/or key is required) or did arrange for the Contractor to collect the new key/code.
- If the damage occurred because the remotely monitored object could not be approached/inspected because of the aggressive behaviour of the dog.
- If the damage occurred because the person to be notified by the remote surveillance centre or another authorised person on the site cannot ensure the internal inspection of the remotely monitored object.
- The Contractor shall not be liable for damages resulting from disconnecting the alarm control panel from the remote surveillance (telephone fee).
- The Contractor's liability extends only to value items and valuables placed within the factory-defined scope of a properly functioning local system, excluding cash, securities, foreign-owned items, antiques, and unlocked jewellery. The Contractor shall not be liable for damages resulting from the loss of data and for lost profits.
- If a third party files a claim for damages against either contracting party under or in connection with the contract, the party concerned shall immediately notify the other party. In the event of a claim against the Contractor by a third party, the Principal shall indemnify the Contractor to the extent that the Contractor is liable to the third party for any damage for which it is not liable to the Principal under the relevant terms of the contract.
- If a damage event occurs, the Principal is obliged to notify the Contractor in writing. The notification shall be sent to the Contractor no later than within 5 (five) working days from the detection of the damage. The limitation period of the Principal's claim for compensation is 6 (six) months.
- Within 4 (four) working days after the notification of the claim, the Principal must attach all the documents and files requested by the Contractor's insurer, on the basis of which the claim for damages can be assessed.
- The Contractor's insurer shall indemnify the damages assessed by them in Hungarian forints, at the obsolete value and in the proportion in which the Contractor's liability exists in accordance with the law and this contract.

By concluding the RSC, the Principal expressly accepts all these conditions for the limitation of liability.

VII. Principal's obligations

The Principal shall at all times cooperate with Contractor to allow Contractor to provide the Services under the best possible conditions. This shall include, but not be limited to, the Principal providing (i) a safe, healthy working environment as well as the material, personal and organizational conditions of first aid at work for Securitas personnel in accordance with applicable laws and regulations (ii) any necessary licenses, permissions and consents which may be required before the date on which the Services are to start.

VIII. Other provisions

1. Confidentiality

The Parties and their employees, contractors and other contributors shall be bound by professional secrecy with respect to any information obtained by them under the contract in connection with the Parties' security measures, business or professional secrets and its disclosure violates or threatens the equitable business interests of the Parties.

The transfer of information by the Contractor to a third party (subcontractor, other contractor, other contributor) involved in the performance does not constitute disclosure.

In accordance with the provisions of the Property Protection Act, the Principal agrees to the registration of their name and address (or registered office or, failing that, business site) by the Contractor and to those records being inspected by the police authority during the inspection of the activity.

Each party shall keep confidential and shall not disclose any confidential information of the other party disclosed to it in connection with the contract except as required for the purpose of the delivery of Services and performance of any other duties under the contract. Information shall be considered to be confidential if it has been designated as confidential by the disclosing party at the time of disclosure, or if it, considering all the circumstances surrounding the disclosure, ought reasonably to be understood by the receiving party to be confidential. For purposes of clarity, Securitas' service plans (the "Security Manual" and/or similar documentation) shall always be considered as confidential information for the purpose of this point and is protected by intellectual property rights. Neither party will have any duty of confidentiality under the contract with respect to information which:

- (i) is or subsequently becomes publicly available without breach of any obligation under the Agreement;
- (ii) was in the possession of the other party prior to the time of first disclosure hereunder;
- (iii) is developed by the other party without any use of or reference to any confidential information received from the disclosing party;
- (iv) is obtained without restriction from a third party reasonably believed by the other party to be free to provide such information without breach of any obligation owed to the disclosing party;
- (v) is disclosed with the prior written approval of the disclosing party; or
- (vi) is disclosed pursuant to the order or requirement of a court, administrative agency, or other government body.

Without prejudice to the forgoing, Contractor may circulate confidential information between all the relevant entities of the Securitas Group.

2. Employment of subcontractors

The Contractor is entitled to use a subcontractor to provide the service undertaken in RSC. The Contractor shall be liable for the subcontractor's activities as if they had been carried out by them. Upon the written request of the Principal, the Contractor shall provide information on the Subcontractor.

3. Notification of the Parties, transfer, invalidity

The Parties shall inform each other immediately about the facts and data (data change) that are important for the contract. If the Principal violates the obligation to provide information and thereby causes damage to the Contractor, it shall be fully liable for damages.

All notices and notifications related to the contract are valid in the form of an electronic mail (e-mail) in compliance with the provisions of Section 6:7 (3) of the Civil Code.

Termination of the contract (both ordinary and extraordinary), request for suspension, resumption of service, engineer and master code request shall only be valid in the form of a letter delivered with written acknowledgment of receipt (by registered mail or registered mail with return receipt) or a confirmed e-mail message. Unless the Parties provide otherwise, a written notice in a letter shall be deemed to have been delivered at the time of certified receipt or, until proven otherwise, on the 5th (fifth) working day following the date of posting of the registered mail to the address indicated in the RSC.

Termination or information sent to the other Party by registered mail with return receipt shall be deemed to have been delivered on the 5th (fifth) working day following the day of the second attempt of delivery, even if it is returned to the sender as "not claimed", "unknown addressee", "moved". The termination or information shall be deemed to have been delivered on the day of the attempted delivery, if the return receipt is returned to the sender with the indication "acceptance refused". In the event of a delivery dispute, the sender shall prove the fact of dispatch.

In the case of delivery in person or by courier, the mail shall be deemed to have been delivered if it is handed over to the Party concerned with proof. In the case of notification by fax/e-mail, the date of delivery is the day on which the Party sends the item to the fax number/e-mail address of the other party's notification address with proof of receipt.

The Parties agree that notification sent by fax/e-mail shall be deemed equivalent to notification sent by post on condition that when the sender sends a notification simultaneously by post and fax/e-mail, they shall deem the date of sending by fax/e-mail the delivery date and the delivery deadlines (if any) stated in the notification shall be calculated from the first day after the delivery date.

The Principal has the right to transfer the services to a third party in order for the third party to use them based on the legal relationship between the principal and them.

The Principal is obliged to notify the Contractor about the fact of the transfer and the essential duration elements necessary for the performance of the service (e.g., contact details of third parties, personal data, etc.) in writing 5 (five) working days prior to the transfer. In the absence of this information, the Contractor shall not be liable to any third party. In the case of a transfer, the Principal is jointly and severally liable for the fulfilment of the contractual obligations and for the proper use of the assets, services and any regulations.

The Contractor has the right to transfer the contract in whole or in part to any company belonging to the Securitas Group (interest group) with the consent of the Principal.

Should any part of the contract become invalid, the Contracting Parties undertake to amend the contract immediately by replacing the invalid part with a contract agreement, which is closest to their economic purpose, and renders that part of the contract valid. Even in the absence of such an amendment, the invalidity of each provision shall not affect the validity of the rest of the contract; the relevant legal provisions shall apply instead of the invalid part.

4. Settlement of disputed issues

The Parties shall use their best endeavours to settle any disputes arising out of or in connection with the Contract, its annexes, or the Property Protection Directive, any document regulating the legal relationship between the Parties or related thereto through joint negotiations. In the event of a dispute that cannot be settled amicably, the Parties submit themselves to the exclusive jurisdiction of the Buda District Court and the Budapest Environs Regional Court, depending on the jurisdiction.

In matters not regulated within this Contract, the relevant provisions of the Civil Code and the Property Protection Act shall prevail.

5. Information supply

The Principal undertakes to make available for the Contractor the current data on the remotely monitored object, the latest information on the contacts and persons to be notified.

The Principal shall inform the Contractor of any special risks related to the object, such as toxins, flammable substances, and any factors known to the Principal that may pose a risk or cause injury or affect the performance of the remote surveillance service.

The Principal shall, as necessary, inform its employees and lessees, as well as other lawful users of the object, of the tasks expected in connection with the remote surveillance service. If the information has changed, the other party must be notified immediately. If the Principal does not supply the necessary information to the Contractor, or if the Contractor is unable to act on the information provided for reasons beyond its control, the Contractor has the right to take measures that may be considered reasonable taking into account the circumstances, the extent of the expected damage and the values to be protected.

If the fire brigade, the police or the ambulance service can be called on the basis of the provisions of this Contract and the conditions in the remotely monitored object, the Principal shall bear the costs caused by any unjustified alarm (false alarm). The Contractor shall not take any responsibility for whether the fire brigade, the police, or the ambulance service actually go out to the remotely monitored object.

6. Transfer of employment

Exclusion of continuous employment

Parties agree that If Contractor employs employees who have been employed by a previous security service provider being in contractual relationship with Principal, Contractor shall enter into a separate employment contract with them, which excludes continuous employment. For the avoidance of doubt, Parties clarify that the rights and obligations arising from the previous employment shall not be transferred to Contractor.

7. Sanction list

7.1 Sanctioned Ownership. Principal represents and warrants that it is not a person that is listed on, or owned (whether directly or indirectly) or controlled by a person listed on, a Sanctions List. For the purposes of this Article 7.1, “ownership” and control” have the meaning given to them in the applicable Sanctions or in any official guidance in relation to such Sanctions.

7.2 Sanctioned Activities. Principal represents and warrants that it does not, directly or indirectly, engage, without prior authorisation from a competent authority (where permitted), in activities that are prohibited by Sanctions.

8 Data Protection

The parties acknowledge that access and distribution of personal information of the other party or its employees, agents or related parties may be necessary for the proper performance of the Services as set out in the contract. Both parties agree to use any personal information obtained throughout the performance of the contract with care, in keeping with all applicable rules and regulations and to use such information only for the purpose of performing their duties as set out in the Agreement.

Securitas and the Securitas group want to be able to offer their customers up-to-date and innovative security services at all times, and therefore have a continuous focus on the development of their services and products. Securitas and the Securitas group are thus entitled to use and process data and information that Securitas collects and/or produces in relation to the service, to improve our services and/or develop new services.

9 Intellectual Property

9.1. IP-rights on back-office and production systems.

The Securitas Group and/or its licensors are the exclusive owners of all back-office and production systems used for the supply of the Services, including monitoring, guard deployment, dispatch, remote guarding and reporting systems, and including all technical infrastructure, systems, software, tools, hardware, equipment, documentation, information, data and other materials contained and generated therein. The Customer is not granted any rights of access or use of such production systems, unless specifically set out in this article 9.

9.2 IP-rights on materials produced by the Securitas Group.

The Securitas Group is and shall remain the exclusive owner of all documentation and other materials produced by the Securitas Group in connection with the supply of the Services (the “Security Manual” and/or similar documentation) under the Agreement.

9.3 No transfer of IP-rights.

For the avoidance of any doubt, the parties agree that nothing in the contract shall be construed as granting to a party, unless expressly agreed in writing, any rights by licence or otherwise, expressed or implied, to or in any of the intellectual or industrial property of the other party.

9.4 IP-rights on hardware and equipment.

The Securitas Group and/or its licensors are the exclusive owners of all hardware and other equipment, and related software and documentation, to be installed at the Principal's premises for the purposes of receiving the Services during the term of the contract. The Customer's right to use such hardware and other equipment, and related software and documentation, expires upon the termination of the contract.

9.5 IP-rights on joint developments.

In the event that Contractor and Principal agree that Contactor (or another company within the Securitas Group) shall develop certain interfaces or other software or materials for integration of Contractor's and Principal's systems and equipment, the parties will agree in each individual case on ownership and licenses thereto (including maintenance and costs if relevant), and where no such agreement has been effected then the Securitas Group shall be the owner of any such interfaces or other integration software or materials, and the Principal be granted a license to use it for the purposes of receiving the Services during the term of the Agreement. In such case, the Principal's right to use such interfaces or other integration software or materials expires upon the termination of the contract. The Securitas Group shall further own and have all rights to any other improvements, suggested changes and adaptations of intellectual property rights related to the Services.

9.6 License to use reporting tool applications.

For certain Services, the Securitas Group may provide certain reporting tool applications for use on e.g. mobile devices.

The Principal is hereby granted a non-exclusive license to use any such reporting tool applications, limited to use for the purpose of receiving the Services during the term of the contract. The Principal's right to use any such reporting tool applications expires upon the termination of the contract.

9.7 Right to use information and data shared or created.

The parties agree that any information and data shared or created under the contract, may be used by the parties, their respective advisors and within the Securitas Group (provided that these advisors and other relevant third parties are bound by confidentiality obligations at least as stringent as the confidentiality obligations set forth in these general terms and conditions) for the purpose of analysing, improving the Services and/or reporting capabilities.

9.8 IP-rights on trademarks.

The Securitas Group and/or its licensors are the exclusive owner of all trademarks, product names and other brand names used for or in relation to the Services. The Principal is not granted any rights to use any such trademarks, product names and other brand names.

10. Securitas Values and Ethics Code

Principal declares that it accepts the provisions of Securitas Values and Ethics Code as binding for itself and for the fulfilment partners / collaborators it has engaged with the prior written consent of Contractor (Securitas Values and Ethics Code and the declaration of commitment are an integral part of the Agreement).

PART II

I. Basic rights and obligations

1. The Contractor's remote surveillance centre shall take measures based on the incoming signals on the basis of the data of the Datasheet filled in by the Principal, in accordance with the Remote Surveillance Procedures.

- If necessary, in the call-out area, the Contractor's own or authorised patrol officer will go to the site if the subscribed service is extended with the call-out action. If the authenticity of the signal is confirmed (e.g., based on the patrol officer's feedback), the Contractor will notify the police.
- Outside the call-out area or in the case of a notification service, the remote surveillance centre will call the persons to be notified listed in the Datasheet and inform the first person available by telephone.

2. The Principal undertakes to fill in the Datasheet forming part of the contract responsibly, to describe the service to the persons to be notified by him, and to notify the Contractor in writing of any changes in their data without any delay. The Principal acknowledges that the Contractor is not liable for damages resulting from the incorrect completion of the Datasheet or the inaccuracy of the data.

3. The Contractor shall not be liable for damages resulting from the unavailability of the persons to be notified indicated in the Datasheet, their conduct following the notification, the failure to take police action, or occurring until the arrival of the patrolman at the scene, if the arrival takes place within the time agreed in the contract. The Contractor limits its liability in the event of "a call-out at the request of the Principal" in accordance with the provisions of the Remote Surveillance Procedures.

4. The Principal acknowledges that the remote surveillance service can only operate if the routes providing the remote signalling are also operational. Within the framework of this contract, the Contractor shall not be liable for damages resulting from the failure of the signalling of the telecommunication service, including the sabotage (cutting) of the telephone line, or from the failure of the electronic signalling system operated by the Principal. (If the Principal's electronic signalling system has not been installed by the Contractor, the Principal should, if necessary, ask the installer to repair the system). The Principal is obliged to notify the remote surveillance contractor of any changes affecting the alarm system (e.g., change of zones, change of the number of partitions). The Contractor shall not be liable for damages resulting from the absence of this.

The alarm system checks the connection between the Principal's alarm system and the remote surveillance centre with test reports at a given time, depending on the programming. The failure of test reports indicates a telecommunication service provider error or an alarm device problem.

For systems that do not send a test report (control report), the communication error of the alarm control panel may go unnoticed and alarm signals may not be received by the remote surveillance centre either. The Contractor shall not be liable for damages resulting from a communication error in systems that do not send a test report.

The Contractor shall notify the Principal by telephone of the absence of the test reports, after which it shall have the right to turn off the monitoring of the test reports until the error is remedied, of which the Principal shall be notified in writing.

5. The Contractor certifies in a report receiving the keys necessary for accessing the object, which will be used during the call-out service, when necessary.

If, in the absence of keys, access to the object is not feasible resolved, the Contractor shall not undertake to inspect the object. The Contractor undertakes to keep the Principal's data and the keys entrusted to them as secret. The Contractor may make 1 copy of the received keys for service reasons, which shall be returned together with the original at the Principal's request.

The Principal undertakes to immediately inform the Contractor about the replacement of the affected locks or the change of the access method (e.g., a new gate code and/or key is required) and to arrange for the collection of the new key/code. The Contractor shall not be liable for damages resulting from failure to do so.

In order to approach the object, the Principal is obliged to inform the Contractor of keeping of a dog. If the object cannot be accessed due to the offensive behaviour of the dog, the Contractor shall not be liable for damages resulting from the lack of inspection.

6. By signing this Contract, the Principal expressly consents to and acknowledges the following:

- Telephone conversations with the Contractor's remote surveillance centre and customer service will be recorded, and the voice recording will be stored by the Contractor for a period in accordance with the regulations in force at any given time.
- In the case of a call-out service, the Contractor may take an image on the spot, which shall be stored for a period in accordance with the regulations in force at any given time.
- Pursuant to the Property Protection Act, the representative of the police body may inspect the records of contracts (not the content of the contract) during the inspection of the Contractor. The Principal agrees that in the event of an official (police, prosecutor's office, court) request or order, the Contractor shall release the data requested by the authority.
- If an unjustified police action is taken on the basis of a false signal, its costs shall be borne by the Principal. A claim of the police against the Contractor under the Property Protection Act may be re-invoiced by the Contractor to the Principal.
- The Principal shall settle the cost of the call-out service of the fire brigade directly with the fire brigade, and the Contractor shall not be liable for it. Any invoices received from the fire brigade may be re-invoiced by the Contractor to the Principal.
- The activity of the Contractor's patrol service is complete if the person to be notified by the remote surveillance centre or another authorized person goes to the site and has the key as well as the code of the alarm device, so they can ensure the internal inspection of the remotely monitored object. The Contractor shall not be liable for damages resulting from the absence of the above conditions.
- The Contractor shall arrange for the call-out service free of charge if the fault is caused by a technical failure of the warranty system installed by the Contractor or by a defective technical system, for the maintenance of which the Parties have entered into a contract or was caused by a real event or a threat of a real event.
- In addition to the above, the Contractor shall arrange for an unnecessary call-out service free of charge within 60 (sixty) days after the connection to the remote surveillance centre.
- The Principal is obliged to reimburse the following in accordance with the fee schedule of the Contractor in force at any time, the fee of unnecessary call-out service not included in the listed cases and 60 (sixty) days after the connection to the remote surveillance centre, and the fee of the call-out service at the special request of the Principal or its representative, not based on a signal. (Unjustified call-out service, as well as call-out at the request of the Principal, is specified in the Remote Surveillance Procedures.)
- If the number of unjustified call-outs exceeds 4 (four) occasions per month, or the system generates a quantity of false alarms that unduly burdens the reception and action capacity of the remote surveillance centre, the Contractor has the right to temporarily suspend the remote surveillance service until the cause of the false alarms ceases after the Contractor has informed the Principal by telephone. The Contractor shall not invoice a service fee for the duration of the suspension. If the error was not corrected by the Contractor, the Principal shall request the restart of the service in writing.

7. If the Principal has an overdue debt under any title to the Contractor, the Contractor has the right to suspend the remote surveillance service, of which the Contractor is obliged to notify the Principal in writing (by post, e-mail or fax). During the period of suspension, the Contract shall not be terminated, but the Contractor shall not be liable for damages resulting from the failure to take action.

8. If the duty activity is interrupted due to the fault of the Contractor, the Contractor shall immediately notify the Principal in a verifiable manner. Following the notification, the Contractor shall not be liable for the protection of the object. If the suspension exceeds 24 (twenty-four) hours, the Principal may claim a refund for days in excess of 24 (twenty-four) hours.

9. The Principal may request the suspension of the remote surveillance service from the Contractor in writing 5 (five) working days before the start of the suspension. The written request for suspension must include the name, address, telephone number of the Principal and the expected duration of the suspension.

The start and end date of the suspension is the date indicated in the letter, failing which the 3rd (third) working day following the receipt of the order. The maximum duration of the suspension may be 3 (three) months.

The local system in the remotely surveyed object also sends its signals during the service suspension, but these signals are only recorded and no action is taken. In the case of fixed line, GSM and GPRS repeater signals, the transmission of signals will generate calls, of which the fixed line will appear on the Principal's telephone bill.

In the event of suspension at the request of the Principal, the Contractor undertakes to resume the service no later than from the 24th (twenty-fourth) hour of the working day following the receipt of the written order. If the restart of the service requires on-site intervention, the time of programming will be agreed upon by the Contractor with the Principal.

If suspension is due to fee arrears, when the Principal pays the fee arrears to the Contractor, unless otherwise stated by the Principal, the Contractor shall activate the remote surveillance service no later than on the 24th (twenty-fourth) hour of the working day after crediting the arrear.

10. The Principal undertakes not to terminate the RSC during the loyalty period. After the expiration of the loyalty period, the contract is for an indefinite period of time, or in case of suspension, the loyalty period automatically extends with the duration of the suspension.

11. If the remotely monitored object is not the property of the Principal, the Principal, being aware of their criminal liability, must declare that they enter into the RSC with the consent of the owner of the property. The Principal acknowledges that in case of the untrue content of the declaration, it is obliged to bear the legal consequences and damages caused by it. They further acknowledge that, at the written request of the owner, the Contractor may suspend or terminate the Contract with immediate effect.

By signing the RSC, a representative of a legal person or an organisation without legal personality, being aware of their criminal liability, declares that they have the necessary authorisation with regard to RSC as a legal (organisational) or proxy (derivative) representative.

12. If the Principal and the Invoice Payer are not the same, the RSC must be signed by both parties. If the Principal and the Invoice Payer is not the same, in case of non-payment of the Invoice Payer, the liability of the Invoice Payer and the Principal to the Contractor shall be joint and several.

13. The Contractor shall not be liable for damages attributable to Force Majeure (an unforeseeable fact, circumstance, natural disaster unavoidable by human power that occurs for reasons beyond the Contractor's control such as: as fire, war, mobilization or military call up of a comparable scope, requisition, seizure, currency restrictions, insurrection and civil commotion, hi-jacking or an act of terrorism, epidemic, pandemic, shortage of transport, general shortage of materials or personnel, strikes or other industrial disputes and defects or delays in deliveries by sub-contractors). It shall be considered force majeure if the signals arrive at the Contractor's remote surveillance centre in a mass that, as agreed in the contract, it cannot process or start the call-out action group with the available personal and material capacity according to the EU standards.

II. Ancillary services

In order to increase security, ancillary services can be chosen in addition to the basic service, for a separate fee on top of the basic service fee. The fee for ancillary services is included in the Contractor's currently effective fee schedule.

1. Monthly posting of event list by e-mail or letter

Sending a list of signals sent by the security system (e.g., opening and closing, alarms), signals generated at the remote surveillance centre (e.g., missed inspection report) and comments on measures (logging) to the postal or e-mail address provided by the Principal for a given elapsed period.

2. Expectation monitoring

If the expected event occurs by the date specified by the Principal, the remote surveillance centre will not take action. If the event does not occur by the specified time, the remote surveillance centre shall notify the person first available in the order or specifically designated for this purpose.

Example: The office opens at various times, but after cleaning, it must be closed and the alarm shall be put on no later than 20:00. If the alarm is not put on (closing is not performed), we notify the company manager. (This service does not indicate that those with the key and access code enter the office at any time of the day, even at night.)

3. Time interval monitoring

The remote surveillance centre monitors the event specified by the Principal in the defined time interval. If the event occurs within the specified time interval, the remote surveillance centre will not take action. If the event falls outside the specified time interval (forbidden interval), the duty officer shall notify the person first available in the order or specifically designated for this purpose.

Example: The store must be open between 6:45 and 7:00 and closed between 17:00 and 18:00. If the employee opens later or enters the store during the forbidden period, between 18:00 and 6:45, even using a valid code, the remote surveillance centre will notify the owner or the store manager.

4. Relative expectation monitoring

Another event expected from the date of an event within the time period specified by the Principal. If this does not occur, the duty officer shall notify the person first available in the order or specifically designated for this purpose.

Example: Trucks pre-loaded with goods leave the site at night. There is half an hour from the time of entering the site to collect the documents and leave. If the alarm is not put on (closing) within 30 (thirty) minutes of the alarm being turned off (opening), the remote surveillance centre will notify the site manager.

5. Remote surveillance of technical equipment

The remote surveillance centre shall inform the person to be notified designated by the Principal about the operation of permanent operation equipment (e.g., cooling, heating, air-conditioning systems) outside the range specified by the Principal.

6. Sending SMS (on technical signals)

In addition to notifying the person to be notified by telephone, the remote surveillance software immediately notifies the person to be notified designated by the Principal of certain technical signals (e.g., power cut, battery running down, temperature rise/fall) by SMS (subject to individual agreement upon special request).

III. Contractor's contact information:

Duty service, error reporting:

- E-mail: technika@securitas.hu
- Phone: +36 -1- 323-0859
- Fax: +36 -1- 323-1040

IV. Remote Surveillance Order of Action

1. Passwords and codes

The Contractor checks the authority of the persons acting during the Remote Surveillance, using passwords and codes, as follows.

To be notified: the person or organisation specified by the Principal, who or which the Contractor, in possession of the appropriate level of password, notifies of the signal related to the Local Property Protection System and the need for related actions in the cases and in the manner specified in the GCTC. The Person to be Notified is also the Authorised Person.

Authorised Person: the person or organisation who or which, in possession of the appropriate level of password, is entitled to take the actions specified in the GCTC, give instructions, request information, etc. at the Contractor.

1.1. General password: in case of contact by phone, the Remote Surveillance Centre **identifies** the person taking the action **with the general password**. The general passwords and the associated password levels are defined by the Principal on the Datasheet, to which the following authorisations are attached.

Password level	Related authorisations	Recommended
Level 1 password	Level 2 password authorisations, and - modification of the postal and invoicing data of RSC, and the data in the Datasheet (in writing, confirmed by a signature) - ordering ancillary services - determination of the level of GSM connection control (if owned by the contractor)	e.g., Principal company manager owner
Level 2 password	Level 3 password authorisations, and - temporary disconnection of the Local Property Protection System from remote surveillance for up to 24 hours* - a provision on the partial omission of the actions of the Remote Surveillance Centre or on actions other than the instructions of the GCTCRS or the Principal, verbally for maximum 24 hours, otherwise in writing, signed.* <i>E.g., "I'm not asking for notification to signal the bedroom's motion sensor until six in the morning tomorrow." "I will not take action for two days for failing the inspection report because the telephone line will be repaired."</i> - request for information on the content of the RSC, the actions of the Contractor and the technical condition of the Local Property Protection System, - ordering ancillary services; - reporting a technical error	e.g., middle manager
Level 3 password	- in case of alarm signals triggering mandatory action, cancellation of the action of the Contractor, requesting information in this area; - ordering ancillary services	e.g., an employee

* In the disconnected state of the Local Property Protection System, the Contractor does not take any action from the signals received from the Local Property Protection System. The Contractor shall not be liable for damages due to the exclusion or failure to act on the instructions of the Authorised Persons!

At least one person with a level 1 password to be notified must be provided, and the same password cannot be entered for different levels of authority. For security reasons, it is recommended that each Authorised Person have an individual password and that the password for each Authorised Person not be disclosed to a third party.

The Principal acknowledges that the Contractor identifies the Authorised Persons with password during the telephone contact. In the absence of a password, the Contractor shall not accept any instructions or provide information, so the service will only be complete if the Authorised Persons (including the Persons to be Notified) have the appropriate level of password.

The Principal further acknowledges that the person with the password is presumed by the Contractor to be the Principal's agent, therefore the instructions from these persons corresponding to the password level are accepted by the Contractor and it is not examined whether the person with the password is included in Persons to be Notified. Based on the above, the Principal undertakes to acts with great care in determining password levels.

1.2. Counter-password: The password of the Remote Surveillance Centre, which allows a person called by the Remote Surveillance Centre to identify that they are actually called by the Remote Surveillance Centre. The Counter-password is provided by the Principal to the Contractor on the Datasheet. Providing a counter-password is optional, but recommended to increase security.

1.3. Forced Password (trap password): During the telephone contact, the person concerned may, using a Forced Password, inform the Contractor that they are in emergency, e.g., the perpetrator forces them to cancel the alarm with a password during contacting after the alarm. Providing a Forced Password is optional, but recommended to increase security.

1.4. Installer password: the password of the specialist authorised to install the Local Property Protection System, which is determined by the Principal on the Datasheet. A person with an installer password may request information from the Contractor about the technical condition of the Local Property Protection System, as well as request the temporary shutdown of the Local Property Protection System from remote monitoring for up to 10 hours*. (see provision marked with * in Section 1.1)

1.5. Trap code (forced opening): The operator of the Local Property Protection System can use the Trap Code to notify the Remote Surveillance Centre that the system is forced to shut down. The Trap Code disarms the Local Property Protection System, but signals a forced opening to the Remote Surveillance Centre. To increase security, it is recommended to programming a Trap Code on the Local Property Protection System

1.6. General code (access / user code): The combination of numbers that switches on or disconnects the Local Property Protection System. The remote surveillance system logs the Close signal (alarm on) and the Open signal (disconnection), provided that the Local Property Protection System has been programmed this way.

1.7. Knowledge of passwords and codes can fundamentally influence the security of a Remotely Monitored Property. The Contractor therefore draws the attention of the Principal and its representatives to the need to act in great care when using passwords and codes, and to ensure that unauthorised persons do not gain access to the passwords or codes. For security reasons, it is recommended that passwords and codes are changed annually, and immediately in the event of personal changes. In order to protect the passwords, the Principal places the Datasheet in an envelope after it has been completed and signed it, signs the envelope at the sealed part, and thus hands it over to the person acting on behalf of the Contractor.

By signing the RSC, the Principal declares that they have understood this warning, and also acknowledges that the passwords provided by them are treated confidentially by the Contractor and may not be disclosed to third parties. In view of this, in case of misuse of passwords, the Contractor shall not be liable if the misuse is attributable to the act of a person who received or obtained the password from the Principal or a person acting on behalf of the Principal, without disclosure, inferred it themselves or applied it at random.

2. Actions of the Remote Surveillance Centre

2.1. The Principal acknowledges that the Contractor **can only act on signals received** from the Local Property Protection System.

2.2. Depending on the type of signals received from the Local Property Protection System, the Remote Surveillance Centre performs **signal filtering**, i.e., it collects information from the Authorised Persons and the signals registered in the Remote Surveillance Centre based on their logic and order to decide on the need for action.

If an action is justified after the signal filtering performed by the Contractor, the Remote Surveillance Centre shall, depending on the nature of the Service and the signal, unless otherwise instructed by the Principal,

- a) try to notify the persons to be notified indicated by the Principal on the Datasheet at least once on the telephone numbers provided there and informs the person first available of them identified by the password, and/or*
- b) initiate the call-out action group to the site.*

In the case of paragraph a), the Contractor's notification obligation applies to informing a person to be notified, if there is one of the persons to be notified who can be reached by the Contractor at the telephone number provided in the Datasheet. See also Section II.2.1 and 2.2 of Annex 3.

The Contractor notifies the police only if the Call-out Action Group is convinced of the authenticity of the signal (Section 14/A of the Security Services Act).

2.3. Cancellation of action: The Contractor's action by telephone, with the exception of the attack signal detailed in Section 3.1, can only be cancelled **with a password**. We draw the attention of the Principal to the fact that, in the interests of their safety, **the action of the Contractor will be cancelled by the Authorised Persons only if they have clear, on-site information on the cause of the alarm**. With the exception of the fire alarm detailed in Section 3.4 of this Annex, the action shall be cancelled if the Local Property Protection System is **deactivated** during the day (06:00–22:00) within 1 (one) minute of receiving the alarm signal **with the General Code** and the Opening Signal arrives at the Remote Surveillance Centre.

3. Alarm signals subject to action

Alarm signal: an electronic signal coming from the Local Property Protection System to the Remote Surveillance Centre, which is generated by the Local Property Protection System because its sensors indicate the unusual, undesirable condition of the monitored objects, spaces, or this type of signal is generated by the protected person (e.g., Attack signal). **Signals from the Local Property Protection System will only reach the Remote Surveillance Centre if the relay device of the Local Property Protection System is in operational condition and the telecommunications repeater routes are provided.**

3.1. Attack Signal (Panic Signal): This signal is detected in the Remote Surveillance Centre when the Local Property Protection System is disarmed with a Trap Code, or an Attack Signal is sent to the Remote Surveillance Centre, or the alarm is cancelled with a Forced Password.

3.1.1. Action in case of call-out service:

In order to avoid endangering the person sending the signal, the Remote Surveillance Centre will send the call-out action group without notice. In the event of such a signal, the Remote Surveillance Centre shall not accept the cancellation of the action initiated by the Contractor or any other instruction from the Authorised Person, even after identification with a password.

3.1.2 Action in case of telephone notification service:

In the case of a panic signal the Remote Surveillance Centre shall notify the first available person specified (in the absence of an indication, the other person to be notified) in the 'person to be notified' part of the Datasheet in accordance with Section 2.2. a). The notified person may confirm the Attack Signal by using a Trap Password, in which case the Remote Surveillance Centre will notify the police, or use the General Password to cancel further action by the Contractor.

3.2. Intrusion (burglary) signal: this signal is detected in the Remote Surveillance Centre if the sensors of the Local Property Protection System detect an unusual movement, unauthorised intrusion or an attempt to do so in the Property.

3.2.1. Action in case of call-out service:

If the signal is received during the day (06: 00-22: 00) and is followed by an Opening Signal within 1 minute, the Remote Surveillance Centre will not take action.

If the signal is received during the day (06: 00-22: 00) but is not followed by an Opening Signal within 1 minute or if the signal is received during the night (22: 00-06: 00):

The Remote Surveillance Centre will send the call-out action group to the Property and will act in accordance with Section 2.2 a). The authorised person(s) may cancel the call-out to the Property in possession of a password, in which case the Remote Surveillance Centre will reverse the already launched response unit. If the action of the Contractor is cancelled by the person(s) entitled to it within 3 minutes of receipt of the signal, the Contractor shall not charge a fee for the erroneous call-out, unless the call-out action group has already arrived at the Property at the time of the cancellation.

3.2.2. Action in case of telephone notification service:

The Remote Surveillance Centre shall act in accordance with Section 2.2. a).

3.3. Sabotage Signal: This signal is sent by the Local Property Protection System to the Remote Surveillance Centre when the Local Property Protection System is subjected to some physical impact (e.g., a sensor is knocked off the wall).

3.3.1. If the signal is received to the Remote Surveillance Centre in the armed state of the Local Property Protection System or during the night period (22:00-06:00), the Contractor shall act in accordance with Sections 3.2.1 or 3.2.2.

3.3.2. If the signal is received by the Remote Surveillance Centre in the deactivated state of the Local Property Protection System or during the day (06:00-22:00), the Contractor shall call the site, at the contact details given in the Datasheet as the site telephone number, in order to those present to be ensured the authenticity of the signal. If the site is not available, the Contractor shall act in accordance with Sections 3.2.1 or 3.2.2.

3.4. Fire signal: this signal is detected in the Remote Surveillance Centre if the appropriate sensor of the Local Property Protection System detects a physical change in the Property indicating a fire.

If the signal is received at the Remote Surveillance Centre from the Property during the day (06:00-22:00) or between the Opening and Closing Signals, the Contractor shall call the site, at the contact details given in the Datasheet as the site telephone number, in order to those present to be ensure the authenticity of the signal. If the site is not available, the Contractor shall notify the fire brigade.

If a signal is received during the night period (22:00-06:00) or after the Closing Signal, the Contractor shall notify the fire brigade.

In the event of a fire signal, the action of the Contractor can only be cancelled by telephone with a password!

3.5. In case of an alarm signal from an **outdoor sensor**, the Contractor undertakes only the action specified in Section 2.2 a).

4. Technical signals subject to action

Depending on its programming, the Local Property Protection System signals the occurrence of a condition limiting its operation to the Remote Surveillance Centre, on which signals the Contractor will take the following actions.

4.1. Fire and zone error signal: this signal is detected in the Remote Surveillance Centre if the functionality of the Local Property Protection System is limited due to a technical failure. In case of such a signal, the Contractor shall take actions in pursuant to Section 2.2. a) in order for the Principal or its agent to ensure the restoration of the functionality of the Local Property Protection System.

4.2. Reporting a technical error: A technical fault in the Local Property Protection System may also be reported to the Contractor by the Principal or the Authorised Person with the appropriate level of password. The Contractor attempts to provide the appropriate technical assistance to the notifier by phone to rectify the error.

4.3. Network failure (power cut): In case of a network failure, the Local Property Protection System will automatically continue to operate from its battery. The expected operating time depends on the age and condition of the battery. The Remote Surveillance Centre shall take action in accordance with Section 2.2. a) within 8 hours after the registration of the network failure signal. If the network is restored, the Remote Surveillance Centre will not take action.

4.4. Battery running down: If the Remote Surveillance Centre registers the running down of the battery of the Local Property Protection System, the Contractor shall take action on the basis of Section 2.2 a). The Local Property Protection System may become unstable during the running down of the battery and send unpredictable signals to the Remote Surveillance Centre until it is completely discharged. Therefore, the Contractor **suspends the Remote Surveillance until the proper technical condition is restored. It is the responsibility of the Principal to replace the battery and restore it to the proper technical condition.**

4.5. Failure to test report (inspection report): The Remote Surveillance Centre monitors the non-signal and takes action within 1 hour for financial institutions and 24 hours for other Customers from the non-signal on the basis of Section 2.2. a), and may request a test signal to control the connection. Then the Contractor has the right to turn off the monitoring of the test report until the error is rectified.

4.6. GPRS module fails to respond In the case of a **failure** of an expected **response** from the GSM repeater device during the connection control according to Section VI./4.3., the Contractor shall act on the basis of Section 2.2 a).

5. Other measures

5.1. Call-out on special request: the Contractor does not assume the time of arrival, in this case the Contractor is not liable for damages.

5.2. Securing the site on special request: if the patrol officer has visually ascertained the integrity of the Property, they will wait up to 1 hour on site for the Principal or their representative.
If another alarm involving another customer is received during the waiting period, the Contractor may decide that the patrol officer leaves the site.

V. Call-Out Order of Action

Among the call-out services, in the case of the signals specified in Section 3 of Chapter IV and if the call-out is justified, the patrolman of the call-out action group shall take the following measures in site pursuant to Act CXXXIII of 2005 on the Rules of Security Services and the Activities of Private Investigators.

1. The patrol officer arriving at the site will only perform an external inspection of the Property. Effective inspection of the Property requires that the Contractor has the keys (codes) required to enter the external premises of the Property. The activities of the call-out action group are complete if the Principal or a representative with local knowledge arrives at the site as soon as possible and has a key or the code of the local security system, so that they can ensure the internal inspection of the protected object.

2. When inspecting the Property externally, the patrol officer, looking for clear traces to a crime, will ascertain the authenticity of the signal and, if possible, the reason for it. During the inspection of the Property, the patrol officer assesses and documents the condition of the doors and windows and other endangered points.

3. If there has been a burglary or other crime in the Property, the patrol officer will secure the venue until the arrival of the Principal or their representative or the police, and, if circumstances allow, detain the perpetrator until the arrival of the police.

4. The patrol officer verifies the authority of the person(s) found on the site - by requesting a password or verifying the identity. For this, we ask for the cooperation of our Customer.

VI. Control the operating modes/signalling route in case of the GSM relay is operating

1. Parallel repeating

All signals of the alarm system that require action, i.e., all alarm signals and important technical signals (e.g., network failure, battery operation) are transmitted to the remote surveillance centre both via a fixed telephone line and via the GSM relay. Only the GSM relay reports its own status signals (network failure, battery running down, sabotage, or their recovery). By programming the alarm control panel, we can achieve that the signals requiring one minute (e.g., opening, closing) are reported by the control panel on the fixed line and only by the GSM relay, as a backup, in case of a fault in the fixed line. The alarm control panel sends a test signal on a fixed line, which is repeated by the GSM relay, so that the functionality of the alarm system and the GSM relay can be controlled.

2. GSM repeating

Since there is no other transmission route, all signals from the alarm system are only sent to the remote surveillance via GSM repeater.

3. Control the signalling route

In the case of remotely monitored alarm systems, the operability of the relay device and the repeating route (transmission channel) is a basic condition for the arrival of the signal at the remote surveillance centre. The signal repeating security can be enhanced by multiplying relay devices and routes (parallel or backup device) and increasing the frequency of signalling connection controls.

The Contractor's GSM relay device allows the connection between the GSM relay and the remote surveillance centre to be controlled almost continuously (every 5 (five) minutes) with the help of GPRS technology.

Controlling the transmission connection is not the same as monitoring the test signals. The test signal is initiated by the alarm control panel, so it also provides information on its status, so it is still justified to send test signals (inspection reports). The transmission connection control (GPRS query) refers to the existence of a connection between the GSM relay installed at the Principal and the Contractor's remote surveillance centre.

The Contractor's remote surveillance centre shall notify the first available person to be notified in case of a failure to respond to GPRS queries. At a high security level (category 1), the notification is also made in the event of a failure of the GPRS network (e.g., for GSM service provider reasons), so that the Principal can otherwise provide sabotage protection for the alarm system.

Telecommunications service providers guarantee 96% availability time for their GPRS service. Therefore, the Contractor also undertakes to control the signalling route with this availability time. In case of interruption of the telecommunication service, the remote surveillance centre will notify the customers depending on the ordered category.

If the GPRS service is interrupted for any reason, only the enhanced sabotage protection and continuous connection controlling will not work. All signals from the alarm system will continue to reach the remote surveillance centre on the GSM data channel or, in the case of parallel repeater routes, on the other route (e.g., on a switched network landline).

The GSM/GPRS system is MABISZ (Association of Hungarian Insurance Companies) certified.

4. Optional categories for connection control

Category 1 - priority level of protection

- Connection control frequency: 10 (ten) minutes.
- In case of any interruption of the GPRS service provider, the remote surveillance centre shall notify the Principal.
- The opening and closing signals transmitted via the GSM relay are free of charge.
- Ancillary services: opening-closing failure and forbidden interval monitoring.
- Used together with fixed line repeating, it corresponds to the category of high-level safety supervision system recommended by MABISZ.

Category 2 - enhanced level of protection

- Connection control frequency: 1 (one) hour.
- In case of GPRS service provider interruption, the remote surveillance centre will not notify the Principal.
- The opening and closing signals transmitted via the GSM relay are free of charge.
- Ancillary services: opening-closing failure and forbidden interval monitoring.

Category 3 - basic level of protection

- Connection control frequency: 4 (four) hours.
- In case of GPRS service provider interruption, the remote surveillance centre will not notify the Principal.
- Opening-closing signals transmitted on the GSM relay.
- When ordering opening-closing signals, opening-closing failure and prohibited interval monitoring are free of charge.

VII. Error reporting, troubleshooting

The Contractor continuously receives the Principal's error report.

If the error report relates to the local system, the Contractor shall proceed as follows:

- If the local system has been installed by the Contractor under a separate agreement and the error occurs during the warranty period, the Contractor will rectify it as soon as possible. If the cause of the error is a device error or a defect in installation, the troubleshooting is free of charge.
- If the local system has been installed by the Contractor under a separate agreement and the error occurs beyond the warranty period, the Contractor will intend to rectify it as soon as possible. For the troubleshooting, the Contractor invoices a fee, which the Principal is obliged to pay within 8 (eight) days.
- If the local system has not been installed by the Contractor and has failed within the warranty period, the Contractor does not undertake the troubleshooting while maintaining the warranty.
- If the local system has not been installed by the Contractor and it has failed beyond the warranty period, the Contractor may undertake the troubleshooting with the appropriate knowledge of the technical data of the local system. The Contractor shall invoice the Principal for the troubleshooting or its attempt, who shall pay it within 8 (eight) days.
- The Contractor accepts the error report and the troubleshooting order in a documented (written) form.

The Principal can report the error at the following contacts:

- Phone: +36- 1- 323-0859
- Fax: +36 -1 - 323-1040
- E-mail: technika@securitas.hu

Each error report must contain the following information:

- The name and telephone number of the person reporting the error.
- The type of its contractual relationship with the Contractor (installation, remote surveillance, maintenance) on the basis of which the troubleshooting is requested.
- Brief description of the error.

- In the case of an 'Unknown' Principal system, the type of local property protection system Ad hoc troubleshooting fees and service call fees are included in the currently effective fee schedule for the remote surveillance service of the Contractor. With the exception of the warranty systems installed by the Contractor, the tools/materials used for troubleshooting shall be invoiced to the Principal by the Contractor in all cases.
- An itemised list of the materials used and the time spent on troubleshooting are included in the job sheet to be completed during troubleshooting.

By signing the troubleshooting job sheet, the execution of the troubleshooting can be considered accepted, on the basis of which the invoice to be issued by the Contractor can be paid. (The troubleshooting job sheet is signed by the Principal's representative at the troubleshooting site. In this case, the Principal's representative may also be the Principals authorised representative in other areas e.g., property security guard. It is the power of the Principal to decide whether to delegate its own competent employee to the troubleshooting site.) Following the reporting of the error, the Contractor's representative shall recall the Principal's representative before starting to rectify the error. The Principal's representative may then be informed about the fees related to the troubleshooting and place an order for the troubleshooting, accordingly.

Part III

PRIVACY NOTICE

Introduction

This Privacy Notice applies to the processing of personal data related to the use of the remote surveillance service of Securitas Security Services Hungary Ltd. (hereinafter: Securitas Ltd.) Details of the service are included in the Remote Surveillance Contract (RSC) concluded between the Parties.

The Principal (Customer) involved in processing expresses its intention to use the service provided by the Securitas Ltd. by concluding a contract. We process your data to perform the contract.

In order to use the service, it is essential to provide the necessary data, the purpose of which is partly a legal obligation (for example: data required for issuing an invoice) and partly the satisfactory performance (for example, call-out to the site in case of an alarm) and provision of the service (for example: your telephone number).

If any of the Principals (Customers) feels that they have any further questions or remarks in addition to those contained in the Privacy Notice, which are not clear to them under the Notice, need to be explained, they may contact the colleague responsible for ensuring the protection of personal data at the following e-mail address: info@securitas.hu At the request of the Data Subject, the Contractor shall in all cases provide detailed information on the personal data processed, the purpose, legal ground, duration of the processing and the activities related to the processing, in accordance with the request.

Controller

Name: **Securitas Security Services Hungary Ltd. (Securitas Ltd.)**
Registered office: 1139 Budapest, Váci út 99. 1st floor
Phone: +36-1-323-0851
E-mail address: info@securitas.hu
Website: www.securitas.hu

The person involved in the processing

Everyone who provides their data for the purpose of using the remote surveillance service of the Securitas Ltd. when concluding a contract as the Principal (Customer) (hereinafter: the Data Subject).

Identity of the subcontractor

Name: **OBJEKT-ŐR Vagyonvédelmi, Kereskedelmi és Szolgáltató Kft.**
Address: 1118 Budapest, Haraszt utca 9.
Phone: +36-1-766-4566
E-mail address: tavfelugyelet@objekt-or.hu
Website: www.objekt-or.hu

In order to provide the service, the Securitas Ltd. uses a subcontractor during its operation. The subcontractor ensures the performance of the service. The subcontractor also qualifies as a **controller** pursuant to Section 30 (4) of Act CXXXIII of 2005 on the Rules of Security Services and the Activities of Private Investigators (hereinafter: Security Services Act) during the provision of the remote surveillance service. According to the referred part of the Security Services Act, the controller is a security guard “in relation to the data processed within the scope of the operation of the **remote surveillance system**, the security technical system for data and IT protection”.

Consent to processing

During the conclusion of the contract, the Data Subject gives their express and voluntary consent for Securitas Ltd. to process the personal data of the Principals (Customers) in accordance with the provisions of this Privacy Notice, as long as there is a Principal relationship between the Principal (Customer) and the Securitas Ltd.

Principles of processing

The processing related to the use of the service shall be performed by the controller in order to protect and respect the privacy of the Data Subjects in accordance with the relevant legislation in effect, in particular:

- *the currently effective data protection/information security act (hereinafter: Data Protection Act), and*
- *Regulation of the European Parliament and of the Council 2016/679 (27 April 2016) on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation, hereinafter: GDPR) - applicable from 25.05.2018.*

The terms used in this Privacy Notice shall be interpreted in accordance with the terms defined in the Data Protection Act and the interpretative provisions of the GDPR.

Securitas Ltd. processes only the personal data of the Data Subject listed in this Privacy Notice in accordance with the purpose limitation principle, only in the manner, for the time and for the purpose described in this Privacy Notice and to which the Data Subject has given consent at the time of concluding the contract.

Securitas Ltd. undertakes, if it changes its principles and/or practices regarding the processing of personal data, to notify the customers of the Securitas Ltd., the persons involved in the processing and the subcontractor of such changes, so that they always aware exactly the applicable processing principles and practices. Securitas Ltd. hereby undertakes that this Notice on the processing and protection of personal data always reflects the principles actually applied and the real practice.

If we wish to use personal data in a way that differs from the principles and purposes stated when collecting personal data, we will notify the Data Subjects in advance via e-mail, to whom we offer the opportunity to decide whether or not to consent to the processing of their personal data in a different way under the new conditions.

Data security

The Securitas Ltd. and the subcontractor are obliged to take all necessary technical and organisational measures in order to ensure the security of the provided personal data in the entire phase of processing. The established regulation documents all activities with the data of the Data Subjects in a retrievable manner.

The purpose of processing

Performance of the service used by the Data Subject and enforcement of related claims.

Processing description

Processing of the personal data provided by the Data Subject in order to fulfil the ordered service.

Legal ground of processing

The processing takes place after the expression of the intention to order the service (preparation of the contract) and after the conclusion of the contract.

Processed data

- the name of the Principal (Data Subject) (or the name of its company), the name, type and address and, the site telephone number of the property,
- persons to be notified and their associated passwords, other passwords (authorised, installer, trap, counter),
- data related to the ancillary service: event sending address (postal, e-mail), opening and closing period,
- all additional data refers to the data and activities of Your company, which are necessary for the performance of the ordered service;

Although most of the processed data is not personal data, the controller also complies with the principles of personal data processing with regard to this data, and also treats the processed data as a business secret as part of the agreement between the Parties. The Data Subject is solely responsible for the authenticity and accuracy of the personal data and other data provided by the Data Subject.

Data source

A written agreement between the Data Subject and the Controller.

Duration of the processing

- We will store the personal data you provide for as long as it is necessary to perform the service and as long as there is a customer relationship between us.
- In order to fulfil the legal obligation, the data related to the issuance of the invoice will be stored until the end of the 8th year following the year of the last invoice, pursuant to Act C of 2000 on Accounting.
- Other data that does not qualify as personal data (provided during the use of the service) will be stored for 5 years after the performance of the service, in order to be able to certify the service at a later date.

Who may access the personal data provided by the Data Subject?

The data provided can only be accessed by colleagues who have a legal relationship with the controller, and they can only get acquainted with them in order to perform the service, the controller does not transfer the data of the Data Subject to third parties, except in the case of legal obligations.

Data transfer

The controller does not transfer your personal data related to the use of the service to third parties, however, courts, prosecutors' offices, investigative authorities, administrative authorities, the Hungarian National Authority for Data Protection and Freedom of Information or other bodies may contact you to provide information and to disclosure and transfer data. Upon request from these organisations, the controller shall provide the personal data strictly necessary for the purpose of the request, indicating the exact purpose and scope of the data issued by the requesting party.

The rights of data subject in relation to processing, legal remedies and the manner of exercising the right

The Data Subject may exercise the rights and remedies related to processing described in this Privacy Notice in case of proof of their identity and connection with the data.

Right to information

The Data Subject has the right to request information about the personal data processed concerning them at any time. At the request of the Data Subject, the controller shall provide information on the personal data processed concerning the Data Subject, the purpose, legal ground, duration of the processing, the legal ground and the recipient of any data transfer. The controller is obliged to provide the information in writing in a comprehensible form at the request of the Data Subject without delay after the submission of the request, but no later than within 25 days (within one month according to the GDPR applicable from 25 May 2018).

Right to data portability

The Data Subject is entitled to receive the personal data concerning them, which they have provided to the controller, in a structured, commonly used and machine-readable format.

Rectification, erasure, limitation (blocking) of data

The Data Subject may at any time modify or request the rectification, erasure (except for mandatory processing) or blocking of their personal data at the contact details of the controller.

The controller erases the personal data processed in connection with the service if their processing is illegal; the purpose of processing has ceased; or the statutory time limit for the storage of data has expired; it has been ordered by a court or the Hungarian National Authority for Data Protection and Freedom of Information; or if the processing is incomplete or incorrect, and this condition cannot be legally remedied, provided that the erasure is not precluded by law.

Notification obligation

The Controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed. When requested by the data subject, the Controller shall inform the data subject of the recipients.

Objection to the processing of personal data

The Data Subject may object to the processing of their personal data,

- a) if the personal data are controlled or transferred to fulfil the legal obligations of the Controller, or enforce the rightful interests of the Controller, data recipient or third party (except for mandatory processing)
- b) if the personal data are used or transferred for direct marketing, public opinion polls or scientific research purposes; or
- c) in other cases defined by law.

If the controller establishes that the Data Subject's objection is justified, the processing shall be terminated and the data shall be blocked.

Legal remedy

If the Data Subject considers that they have been infringed in connection with the processing of their personal data, they may contact the controller with their questions for legal remedy at the contact details provided above. In addition, they can initiate an investigation with the Hungarian National Authority for Data Protection and Freedom of Information, the contact details of which are: Address: 1055 Budapest, Falk Miksa u. 9-11., website: www.naih.hu, Phone: +36-1-3911400, e-mail address: ugyfelszolgalat@naih.hu. They can also turn directly to the competent court: Court of Registration attached to the Budapest Capital Regional Court, Postal address: 1363 P.O. box: 16., Address: 1055 Budapest, Markó u. 27, but they can also turn to the court of their place of residence.