Gantner

GL7p

**Battery-Powered, Door-Mounted Electronic Locker Lock
Identification via RFID (MIFARE®, ISO 15693, NFC, HID iCLASS)
and Optional PIN Code**

**Installation, Configuration, Operation
Document Version 1.2**

Liability

Any claims against the manufacturer based on the hardware or software products described in this manual shall depend exclusively on the conditions of the guarantee. Any further-reaching claims are excluded, and in particular the manufacturer accepts no liability for the completeness or accuracy of the contents of this manual. The right is reserved to make alterations, and alterations may be made at any time without prior notice being given.

Trademarks

Attention is drawn at this point to markings and registered trademarks used in this manual. All product and company names, which are mentioned in this manual, are only used for identification and explanation purposes. Some of these names may be trademarks or registered trademarks of the corresponding company.

Availability

The GL7p is not available in North America (United States, Canada).

Contact

The contact information for questions regarding this product or for general enquiries is listed below:

Contact address of manufacturer

GANTNER Electronic GmbH
Bundesstraße 12
6714 Nüziders, Austria
www.gantner.com/locations

Important Information
Dear Customer, Our aim is to ensure that our product operates with safety and to your complete satisfaction. To achieve this aim, please take this opportunity to familiarize yourself with the following guidelines. - Pay attention to the safety messages in this manual. The messages are indicated by the signal words "DANGER", "WARNING", or "CAUTION", and inform you about hazardous situations and how to avoid them. - Pay attention to messages indicated by the "NOTICE" signal word. These messages include important information for avoiding property damage. - Pay attention to the symbols and safety messages on the product. - Read all instructions in this manual carefully before installing or operating the product. - Where not otherwise specifically documented, the appropriate installation, commissioning, operation and maintenance of the product is the customer's responsibility. - Keep this manual in a safe place for quick reference.

Notation of Safety Information and Safety Symbols

This manual includes important safety messages and symbols intended to inform the user about potentially hazardous situations or important information for the safe and proper use of the described product(s). The safety messages also include directives on how to avoid hazardous situations. These safety messages and directives must be read and observed.

The structure of the safety messages and the meaning of the symbols used in this manual are described in this section.

1. Safety Messages for Personal Injury

Personal safety messages contain a signal word, describe the nature of the hazard, and indicate how to avoid the hazard.

The safety alert symbol used without a signal word always precedes important safety information that must be read carefully and the instructions carefully observed. Not doing so may cause personal injury.

Format of safety messages that apply to an entire section:

These safety messages may be used with or without a symbol.

⚠ **CAUTION**

Electrical shock

➔ *Touching current-conducting parts may result in injury due to electrical shock.*
- Do not remove safety protection and covers.
- Do not touch the electrical connections while power is being supplied.

Format of safety messages that are embedded in text and apply to a specific point:

⚠ **CAUTION! Electrical shock.** Never remove safety protection and covers. Do not touch the electrical connections while power is being supplied.

2. Property Damage Messages

Property damage messages are used to describe potentially hazardous situations that may lead to property damage. These messages have the same layout as safety messages but use the signal word "NOTICE" instead of "CAUTION".

Format of property damage messages that apply to an entire section:

NOTICE

Risk of damage to the device and connected devices
Risk of malfunction

- Read the following instructions carefully before installing the device.
- Always adhere to the instructions.

Format of property damage messages that are embedded in text and apply to a specific point:

NOTE! **Risk of damage to the device and connected devices.** Read the following instructions carefully before installing the device.

3. Definition of the Signal Words

⚠ CAUTION	Indicates a hazardous situation that, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates information considered important, but not hazard-related (e.g., messages relating to property damage).

4. Definition of the Safety Symbols

⚠	**Caution: General Information** This symbol indicates general warnings or cautions that are not related to a particular type of hazard.
⚡	**Caution: Electrical Shock** This symbol indicates warnings related to electrical hazards (danger due to high voltage).
🚫	**Prohibited: Do Not Disassemble** This symbol indicates warnings about not disassembling certain components or equipment. Disassembling may lead to damage or malfunction of the device.
❗	**Mandatory Action: General Information** This symbol indicates general information that must be read and followed before proceeding with the accompanying instructions.
📖	**Mandatory Action: Read Instructions** This symbol indicates information referring to an important description in the manual, or other documentation, which must be read and followed.

⚠ Important Safety Information ⚠

− The installation, commissioning, and servicing of our products must be performed only by suitably trained personnel. In particular, electrical connections must only be made by correspondingly qualified specialists. Always observe the relevant installation regulations in accordance with the national Electrical Engineers Association.

➔ Unqualified personnel may potentially perform actions that result in injury due to electrical shock.

− Where not otherwise stated, installation and maintenance work on our products must be carried out when disconnected from the power supply. This applies in particular to appliances that are normally supplied by low-voltage current.

➔ If the appliance is not disconnected from power, touching terminals or other internal parts of the appliance may lead to injury due to electrical shock.

− It is prohibited to alter the products (devices, cabling, etc.).

➔ Alterations to the products may subsequently result in personal injury, property damage, or damage to the products.

− Do not remove protective shields and covers.

➔ Removing protective shields and covers may result in personal injury or property damage.

− Do not attempt to repair a product after a defect, failure, or damage is detected. In addition, do not put the product back into operation. In such cases, it is essential to contact your GANTNER representative or the GANTNER support hotline.

− The installation, commissioning, operation, and maintenance of the product must be carried out in accordance with the technical conditions of operation as described in the corresponding documentation. Therefore, it is essential to read the corresponding chapter of this manual and observe the instructions and information therein.

− If there are still some points that are not entirely clear, please do not take a chance. All queries can be clarified by your GANTNER representative or by ringing the GANTNER support hotline.

− Directly on receipt of the goods, inspect both the packaging and the product itself for any signs of damage. Also check that the delivery is complete and includes all accessories, documentation, auxiliary devices, etc.

− If the packaging or product has been damaged in transport, or should you suspect that it may have a fault, the product must not be put into service. Contact your GANTNER representative who will endeavor to resolve the problem as quickly as possible.

− GANTNER Electronic GmbH accepts no responsibility for any injuries or damage caused as a result of improper use.

Although great care is taken and we are continuously aiming for improvement, we cannot completely exclude the possibility of errors appearing in our documentation. GANTNER Electronic GmbH therefore accepts no responsibility for the completeness or the accuracy of this manual. The right is reserved to make alterations at any time without prior notice.

Should you discover any fault with the product or in its accompanying documentation, or you have any suggestions for improvement, you may confidently inform your GANTNER representative or GANTNER Electronic GmbH directly.

We especially look forward to hearing from you if you want to let us know that everything is functioning perfectly

Gantner

The GL7p was developed and fabricated under the quality management standard ISO 9001 and GANTNER Electronic GmbH is also certified according to standard ISO 14001.

CE	This product is in conformity with the following EC directives, including all applicable amendments: - 2014/53/EU (Radio Equipment Directive) The complete text of the CE Declaration of Conformity is available on the following internet link: http://www.gantner.com/en/produkte/downloads-GL7p_jQ690dP3B6
RoHS	GANTNER is committed to meeting or exceeding the requirements of the RoHS directive (2011/65/EU). The RoHS directive requires that manufacturers eliminate or minimize the use of lead, mercury, hexavalent chromium, cadmium, polybrominated biphenyls and polybrominated diphenyl ethers in electrical and electronic equipment sold in the EU after July 1, 2006.

FCC INFORMATION (U.S.A.)

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that of which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Warning Statement:

[Any] changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Comliance Statement (GL7p.0500, GL7p.150x):

> FCC ID: NC4-GEA1190118A
>
> This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device must not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Compliance Statement (GL7p.2500, GL7p.350x):

> FCC ID: NC4-GEA1190126A
>
> This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device must not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The GL7p.2xxx and GL7p.3xxx contain a wireless module. For those modules the following applies:

> This device contains
> FCC ID: QWO-QS9322PLCS
> IC: 4460A-QS9322PLCS

FCC Radio Frequency Exposure:

WARNING: To comply with RF exposure limits the users must keep at least 20 cm separation distance from the device, except during the identification and operation process at the device (e.g. PIN-code input), which must be performed as described in this manual.

INDUSTRY CANADA INFORMATION

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:
1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:
1. l'appareil ne doit pas produire de brouillage;
2. l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ICES Statement (Canada)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Availability

The GL7p is not available in North America (United States, Canada).

The WEEE symbol on GANTNER products and their packaging indicates that the corresponding material must not be disposed of with normal household waste. Instead such marked waste equipment must be disposed of by handing it over to a designated electronic waste recycling facility. Separating and recycling this waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. Please contact your local authority for further details of your nearest electronic waste recycling facility.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 About this Manual

This manual contains all the information necessary for the installation, commissioning, configuration, operation, and disposal of the GL7p electronic locker locks. The GL7p is available in various variants, all of which are described in this manual. These are the following variants:

- GL7p.0500
- GL7p.1500, GL7p.1501, GL7p.1502
- GL7p.2500
- GL7p.3500, GL7p.3501, GL7p.3502

In this manual, the terms "GL7p" and "lock" are used to represent all listed locks. If information in the manual only applies to a specific lock, the product name concerned is used.

This manual provides an overview of how to configure the GL7p using the configuration software GAT Config Manager. A separate manual is available for GAT Config Manager that explains in detail all functions of the software. In addition, configuration via the MoLA app is possible. This app can be installed from the Google Play Store on a mobile device and includes instructions for use.

1.2 Chapter Overview

In chapter 2 "GENERAL INFORMATION", a functional description of the GL7p, the RFID technologies supported by the device, key terms used in this manual, and a summary of system components can be found.

Chapter 3 "INSTALLATION" contains the measurement diagrams and information required to install the GL7p into lockers.

Chapter 4. "COMMISSIONING" describes how to put the GL7p into operation and includes information on the battery used to power the lock and the USB connection used for PC connection and configuration.

In chapter 5 "CONFIGURATION", you will find information on how the lock is configured with the configuration software GAT Config Manager and with the MoLA App. The main configuration settings for the lock are explained and a table listing every setting is available here.

In chapter 6. "OPERATION", the different operating modes of the GL7p are described. The system data carriers required to maintain the locker system and the LED signaling are also explained in this section.

Chapter 8 "TECHNICAL DATA" contains all the relevant technical information of the different GL7p variants.

1.3 Contact & Inquiries

For all inquiries concerning the GL7p, please contact your local sales partner or one of the GANTNER branch offices directly. The contact details are available via the following link: www.gantner.com/locations

1.4 Target Group

This manual contains information relevant for the different stages in the operating life of the GL7p. Information regarding the installation, commissioning, and service/maintenance is separated into corresponding chapters. When a chapter is intended for a specific audience, this is clarified at the beginning of the chapter.

Information for the following target groups is available in this manual:

- Installation technicians (installation, operation, configuration).
- Service technicians and cleaning personnel (service and maintenance).
- End users of the GL7p (user manual).

Where not explicitly stated, the information in this manual is intended for all target groups in general.

⚠️**CAUTION! Injury and property/equipment damage.** The tasks described in each chapter must only be performed by the specified target group. Unqualified personnel who perform the described tasks risk personal injury or damaging property/equipment.

1.5 Formatting

1.5.1 Safety-Critical Information

The following formatting (with example text) is used in this manual to display important, safety-critical information that must be read and followed.

NOTE! Following on from this signal word in the manual is a reference text that must be read and followed. The reference text contains important information. Non-observance can lead to damage of the device or associated equipment.

1.5.2 Non-Safety-Critical Information

The following formatting (with example text) is used in this manual to display important, but not safety-critical information.

ℹ️ *The text accompanying this symbol contains interesting information relevant to the current chapter. You do not necessarily need to read this text; however, it will help you better understand the information in this section or provide interesting tips for the described device or the operation of the software.*

1.5.3 Instructions and Results

Instructions, which must be completed by the reader, and the results of these instructions are formatted as follows.

- ► This symbol represents an action or instruction that that must be followed.
    - o This symbol represents the result after completing the previous instruction.

2 GENERAL INFORMATION

2.1 Intended Use

The GL7p may only be used for the convenient electronic locking of lockers in facilities such as leisure facilities, universities, companies, depots, and other individual company applications. Depending on the device type, identification at the GL7p is completed using contactless RFID (Radio Frequency Identification) data carriers or via PIN code. Data carriers that use MIFARE® and ISO 15693 RFID technology are supported by the GL7p.

> **i** *The GL7p is not available in North Amercia (United States, Canada)!*

2.2 Highlights

- Free locker selection, assigned lockers, or rental locker function configurable
- Time-controlled use
- Automatic unlocking function
- Maintenance-free "Low-Power Technology"
- Configuration via PC/computer, data carrier, or NFC
- Recording of the last 150 bookings
- Secure data transmission between locker lock and data carrier
- NFC ready
- Mechanical locking and unlocking (motor) for highest reliability
- Status displayed via the button position and multi-colored LED
- Existing lockers easily retrofitted (compatible with standard locker locks)
- Suitable for left and right-hinged doors, low door heights, and various locker materials
- Optional wireless interface for identification via smartphone
- Emergency power supply when the battery is empty

2.3 Functional Description

The GL7p is installed on the inner side of the locker door and is suitable for most types of locker material, e.g., sheet metal, wood, HPL, and solid plastic. The GL7p can be used with left- and right-hinged locker doors alike. The lock can be mounted both vertically and horizontally, which also makes it suitable for use in lockers with very low door heights. Due to its mechanical compatibility with standard locker locks and identical locks from other manufacturers, existing locker installations can be effortlessly upgraded using the GL7p. The existing holes of the previous standard locks can be directly re-used.

The GL7p is powered by one 3.6 V AA lithium battery (see "8 TECHNICAL DATA"), which provides an operating life of up to 10 years* (at 10 activations per day and +20 °C room temperature) before requiring replacement. For configuration, the lock connects to a computer via USB and can then be configured using GAT Config Manager configuration software. The lock can operate in one of five operating modes thereby providing flexibility for different locking requirements within a facility.

Using a locker

To use a locker, the user closes the door of their locker and while holding the door shut, presses the button of the GL7p in using their data carrier. The GL7p reads the data carrier information and determines whether the user is authorized to use the locker. When the user is authorized, the GL7p locks the locker door. The LED signals the locking action and the button remains in the pressed-in position.

To unlock a previously locked locker, the user presses their data carrier onto the lock button. The GL7p reads the data carrier and checks that the authorization is valid before automatically unlocking the locker door.

* Different operating modes or configurations can reduce the battery lifespan.

2.4 GL7p Variants

Various options are available for identifying users of the GL7p locker locks. Depending on the variant of the lock used, one or more of these options can be used.

Variant	RFID [1]	Wireless [2]	PIN Code [3]	Mounting method [4]
GL7p.0500	X	-	-	vertical top | horizontal right | horizontal left
GL7p.1500	X	-	X	vertical top
GL7p.1501	X	-	X	horizontal right
GL7p.1502	X	-	X	horizontal left
GL7p.2500	X	X	-	vertical top | horizontal right | horizontal left
GL7p.3500	X	X	X	vertical top
GL7p.3501	X	X	X	horizontal right
GL7p.3502	X	X	X	horizontal left

1) Identification via radio frequency (13.56 MHz) over a short distance of up to a few centimeters (RFID = Radio-Frequency Identification). A distinction must be made between the different technologies (e.g., MIFARE Classic, MIFARE Ultralight, ISO 15693, HID iCLASS, NFC). A list of all supported technologies is provided on the next page.

2) Identification via wireless technology (2.402 to 2.480 GHz) over long distances of up to several meters. This option can be used, e.g., for identification at the lock using a smartphone with a specific app.

3) PIN-code keypad for identification.

4) Alignment of the lock depends on the printing of the PIN-code keypad (see next page).

Table 2.1 – *GL7p variants*

2.4.1 RFID Technologies

The following data carriers can be used for RFID identification with the GL7p.

MIFARE® (manufacturer NXP/Infineon)
- MIFARE® Classic (1k and 4k)
- DESFire EV1® and EV2®
- MIFARE Ultralight®

HID iClass
- Reading of unique number only

ISO 15693
- The GL7p operates with all currently known ISO 15693 data carriers.

In addition to the different RFID technologies, data carriers are available in a variety of shapes and sizes. The GL7p is designed to operate with all different types of data carrier media.

2.4.2 Lock Orientation

For the GL7p variants with a PIN-code keypad, the printing of the PIN-code keypad must be observed (recognizable by the last digit of the model identifier). The different variants must be mounted as follows.
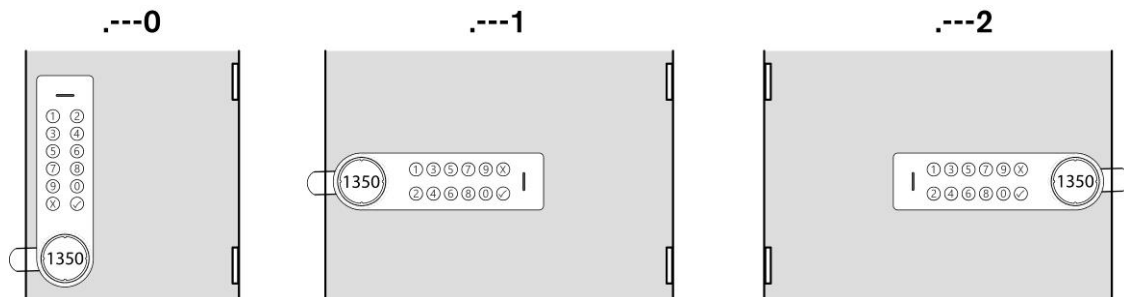
0 ... vertical top
1 ... horizontal, right-hinged door (i.e., the lock is on the left and the door opens on the left)
2 ... horizontal, left-hinged door (i.e., the lock is on the right and the door opens on the right)

Figure 2.1 – *Orientation of the GL7p variants with PIN-code keypad*

2.5 Terminology

Several key terms that are used often in this manual are defined below.

Computer / PC
These terms refer to all desktop and laptop computers running a Microsoft® Windows® operating system.

Data Carrier
A data carrier is a form of identification media that is used by staff and visitors in a facility for identification. Data carriers are available in a variety of different forms such as plastic wristbands and chip cards. Data carriers are also available to suit different RFID technologies (LEGIC, MIFARE®, ISO 15693).

System Data Carrier
Several different types of System Data Carriers are used for programming, service and maintenance tasks. These data carriers have special functions and as they are essential for operation of the GL7p and have security-related features, they must be kept in a secure place and be protected against unauthorized use. Most of the System Data Carriers are included in the GAT ECO.Basic Set FD; however, some must be ordered separately as required.

FID (Company ID) and Site Key
LEGIC systems use the FID number and in MIFARE® systems the site key is used, which is a combination of the FID and the read and write keys. The FID and site key are unique for every facility. These numbers are encoded in every data carrier and device used in the facility thereby ensuring that data carriers from one installation cannot be used in other installations.

GAT Config Manager
GANTNER developed PC software that is used to configure GANTNER devices such as the GL7p. A separate manual is available and integrated into the software. While the software is open, click on the "Help" drop-down menu and select "How Do I".

Lock
General term for the GL7p.

Locker
The term "locker" is used to describe all possible locker applications that can be fitted with a GANTNER electronic lock. Typical applications include a changing room locker, a deposit box, or a private box.

RFID (Radio-Frequency Identification)
Identification over a short distance using radio frequency. An RFID data carrier is used to identify users in GANTNER systems.

Wireless
Identification via a wireless interface in the range 2.402 to 2.48 GHz, over which identification and locker operation from several meters, e.g., via an app on a smartphone, is possible.

User / Guest / Visitor
These general terms refer to the people in a facility who use the locker system with GANTNER locker locks, data carriers, and other GANTNER devices on a daily basis.

Gantner

2.6 System Components

The GL7p locker locking system includes the following system parts. A description of the individual components is provided on the following page.

3. GL7p.1501
4. GL7p.3501

7. GL7p.1502
7. GL7p.3502

1. GL7p.0500
5. GL7p.2500

2. GL7p.1500
6. GL7p.3500

9. GL7p Battery CoverKey

10. GAT ECO.Basic Set FD

11. Batterie 3.6V Lithium SL-860/S

12. GAT Key Tag F Open

13. GL7p Button Plate

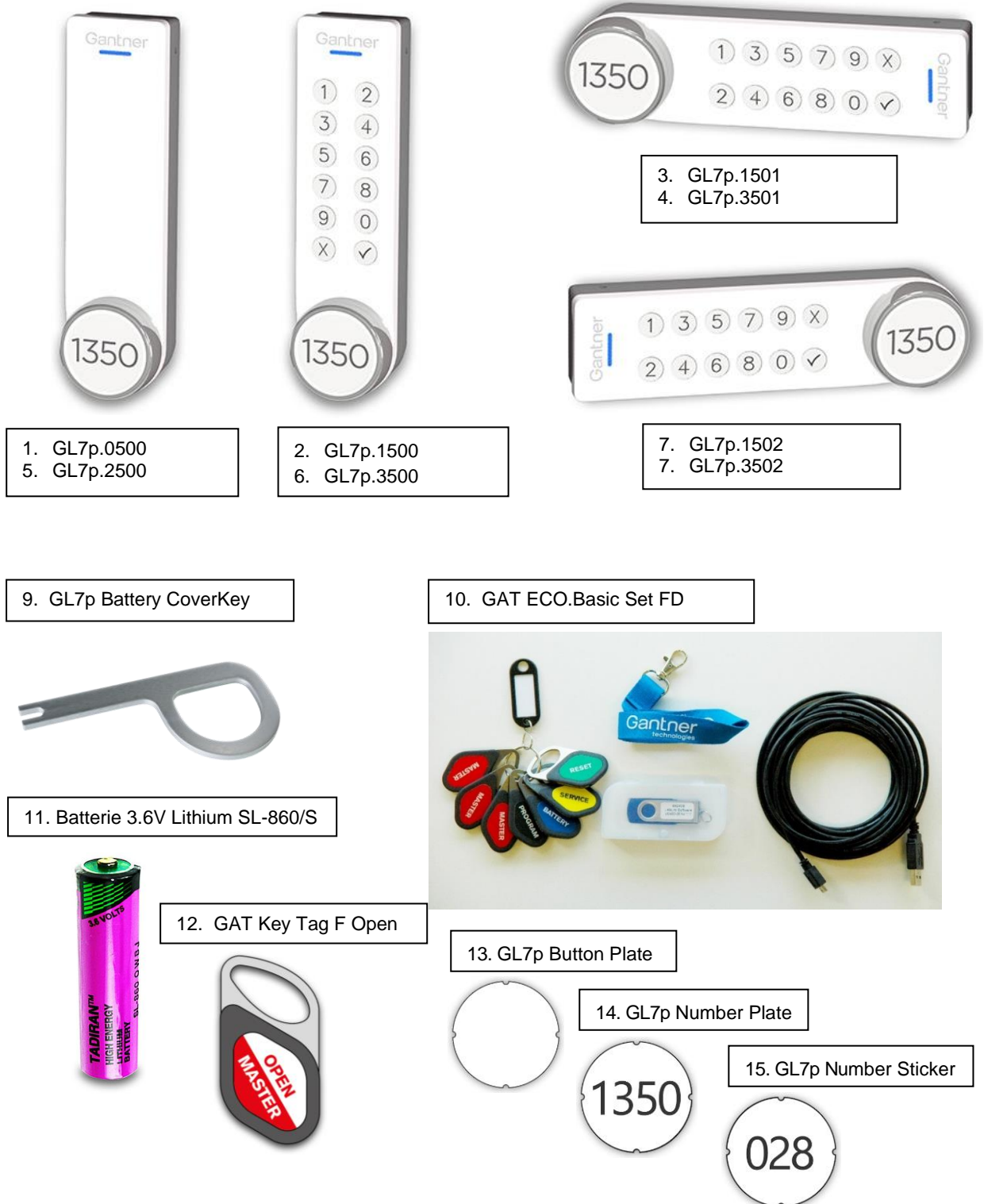14. GL7p Number Plate

15. GL7p Number Sticker

***Figure 2.1** – Components of the GL7p locker system*

1. GL7p.0500 (Part No. 922728)
    Battery lock for MIFARE® and ISO 15693 data carriers, without PIN keypad, without battery.

2. GL7p.1500 (Part No. 922627)
    Battery lock for MIFARE® and ISO 15693 data carriers, with PIN keypad, vertical mounting, without battery.

3. GL7p.1501 (Part No. 922425)
    Battery lock for MIFARE® and ISO 15693 data carriers, with PIN keypad, mounting on right-hinged door, without battery.

4. GL7p.1502 (Part No. 922526)
    Battery lock for MIFARE® and ISO 15693 data carriers, with PIN keypad, mounting on left-hinged door, without battery.

5. GL7p.2500 (Part No. 922324)
    Battery lock for MIFARE® and ISO 15693 data carriers, with wireless interface, without PIN keypad, without battery.

6. GL7p.3500 (Part No. 922223)
    Battery lock for MIFARE® and ISO 15693 data carriers, with wireless interface, with PIN keypad, vertical mounting, without battery.

7. GL7p.3501 (Part No. 922021)
    Battery lock for MIFARE® and ISO 15693 data carriers, with wireless interface, with PIN keypad, mounting on right-hinged door, without battery.

8. GL7p.3502 (Part No. 922122)
    Battery lock for MIFARE® and ISO 15693 data carriers, with wireless interface, with PIN keypad, mounting on left-hinged door, without battery.

9. GL7p Battery CoverKey (Part No. 749230)
    Tool for opening the battery compartment.

10. GAT ECO.Basic Set FD (Part No. 1100550)
    Set for the configuration and maintenance of the GL7p system. Contains configuration software, USB charging cable, 3 MASTER data carriers, 5 system data carriers with special functions, and a battery compartment key. See section "6.4 GAT ECO.Basic Set FD" for more information on the GAT ECO.Basic Set FD.

11. Batterie 3.6V Lithium SL-860/S (Part No. 914430)
    GANTNER approved battery for the GL7p. Alternative = Tadiran TL-4903/S

12. GAT Key Tag FD Open Master (Part No. 1100369)
    Optional data carrier. Not included in the GAT ECO.Basic Set FD. MIFARE data carrier that can open every GL7p locker in the assigned system (=master key function) instead of a MASTER data carrier. In contrast to the MASTER data carrier, this data carrier can only unlock a locker but not lock it again. See section "6.5.2 OPEN MASTER Data Carrier (Optional Accessory)" for more information.

13. GL7p Button Plate (Part No. 748633) – included with the GL7p
    Self-adhesive number plate, thickness 0.8 mm, white unprinted, for attaching to the button.

14. GL7p Number Plate (Part No. 1103180)
    Self-adhesive number plate, thickness 0.8 mm, white with lasered locker number (standard font), can be attached to the button instead of the number plate Part No. 748633.

15. GL7p Number Sticker

Self-adhesive button sticker that can be attached to the accompanying GL7p Button Plate (Part No. 748633). Printable with a customer-specific design. This item is available in sheets of 50 stickers with pre-printed numbers in the following number ranges:
- GL7p Number Sticker 001-050 (Part No. 1103040)
- GL7p Number Sticker 051-100 (Part No. 1103041)
- GL7p Number Sticker 101-150 (Part No. 1103042)
- GL7p Number Sticker 151-200 (Part No. 1103043)
- GL7p Number Sticker 201-250 (Part No. 1103044)
- GL7p Number Sticker 251-300 (Part No. 1103045)
- GL7p Number Sticker 301-350 (Part No. 1103046)
- GL7p Number Sticker 351-400 (Part No. 1103047)
- GL7p Number Sticker 401-450 (Part No. 1103048)
- GL7p Number Sticker 451-500 (Part No. 1103049)

2.7 GL7p Dimensions and Components

1. LED status indicator
2. Button (a = "unlocked", b = "locked")
3. Latch
4. Front part
5. Rear part
6. Mounting thread (M19x1)
7. Fixing nut
8. Spacer sleeve
9. Screw for anti-rotation protection
10. Battery compartment cover
11. Battery compartment key

Figure 2.2 – GL7p dimensions and components (dimensions in mm – inches shown in brackets)

3 INSTALLATION

NOTE! These installation instructions describe how to install the GL7p locker lock. Please read this section carefully prior to working on the lockers or installing the locks.

NOTICE

Risk of damage or failure to the GL7p
- *Read the information in this section carefully before installing the GL7p.*
- *Carefully observe the installation diagrams.*
- *Use the correct tools to install the GL7p.*

3.1 Target Group

This chapter provides information for technicians who install the GL7p. Experience in mechanical work and basic electrical knowledge is required. Previous knowledge of the GL7p is not required.

3.2 Test Installation

As the GL7p is suitable for a wide range of installation applications, always perform a test installation including functional testing of the GL7p in a sample locker from the facility before starting with the mass production of lockers.

Ensure that the latch of the lock slides easily in and out without resistance of the opening in the locker body. Also test that the GL7p locks and unlocks as required, ideally using a data carrier of the same type to be used with the locker system to ensure that the data carrier functions as required.

3.3 Replacement after a Burglary Attempt

If a burglary (forced opening) is attempted or occurs at a locker, the entire GL7p including the locker door must be replaced with a new one.

3.4 Operating Conditions

The GL7p is suitable for locker doors made of metallic and non-metallic materials. The lock may only be used indoors (see section "8.8 Environmental Conditions").

The installation in lockers with metallic doors does not differ from the installation of lockers with non-metallic doors.

Gantner

3.5 Door Width and Thickness

The GL7p is suitable for locker doors with a door leaf thickness of 1 to max. 28 mm. Depending on the thickness of the door leaf, different screws and/or the supplied spacer sleeve must be used for anti-rotation prevention. For details, see "3.8.2 Instructions for Installing the GL7p".

When installing the GL7p in lockers with narrow doors, ensure that the GL7p does not touch the locker body when opening and closing the door (see following picture).
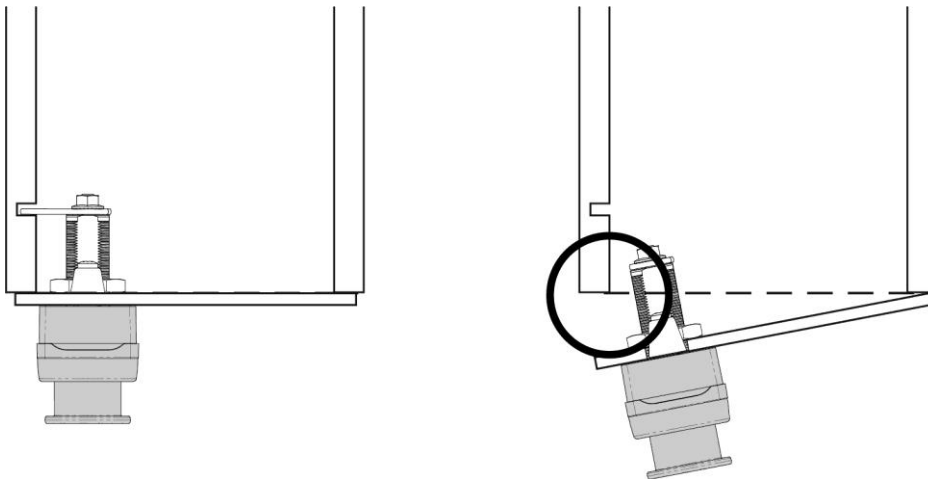
Figure 3.1 *– Width and thickness of the locker door*

3.6 Latch Types

The GL7p comes with a standard latch. This has a straight shape and when installing in a new locker, the position of the latch stop in the locker body must be aligned accordingly so that the latch is present at the stop when the door is closed. The distance from the underside (mounting side) of the GL7p to the latch is 34 mm (1.34 in) (see following picture).
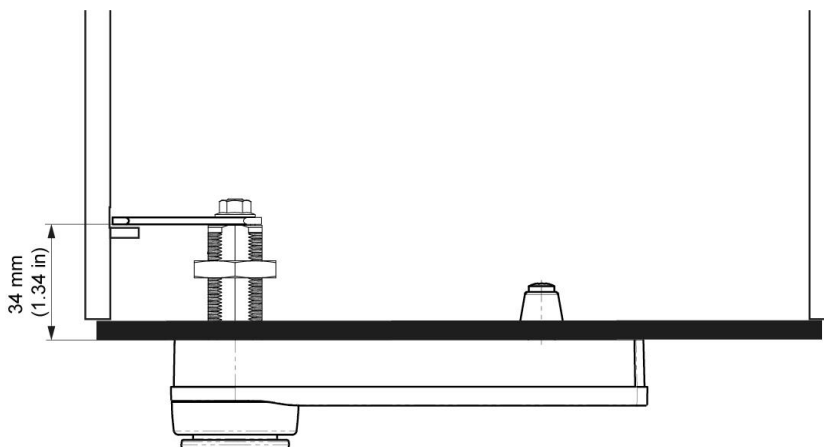
Figure 3.2 *– Standard latch included*

Gantner

To retrofit the GL7p into existing lockers, GANTNER also offers offset latches that can be adapted to an existing latch stop. In this case, please contact GANTNER Electronic GmbH or your local sales partner to order a suitable latch.

NOTE! To ensure the safe operation of the GL7p, do not bend or modify the supplied latch yourself.

To find the exact measurement for the latch, follow these steps.

► Install the supplied standard latch.
► Lock the GL7p using a valid data carrier or PIN code while keeping the locker door closed so far that the latch retracts exactly into the existing latch opening in the locker wall.
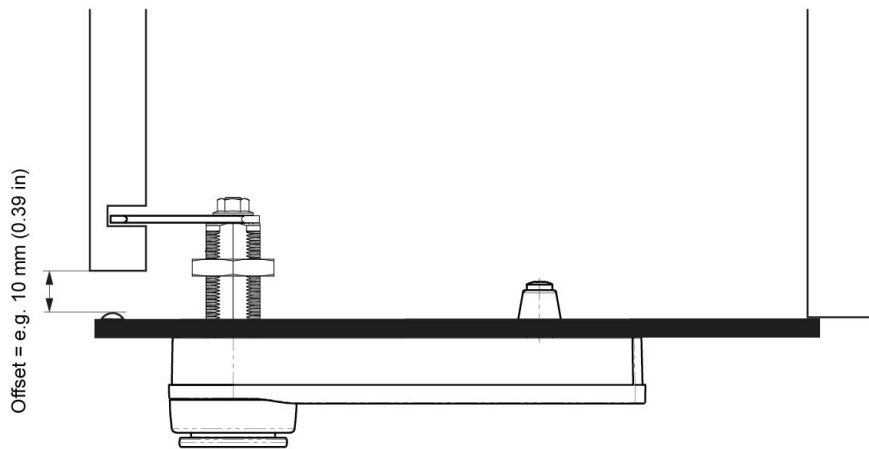
Figure 3.3 – *Measuring the required latch offset using the supplied latch*

► Measure the gap size of the door from the edge of the locker body to the point of impact on the door (i.e., to the inside of the door or any bump stops).
► The latch must be offset by the measured gap size. Please provide this dimension to your distributor or GANTNER Electronic when ordering the offset latch.
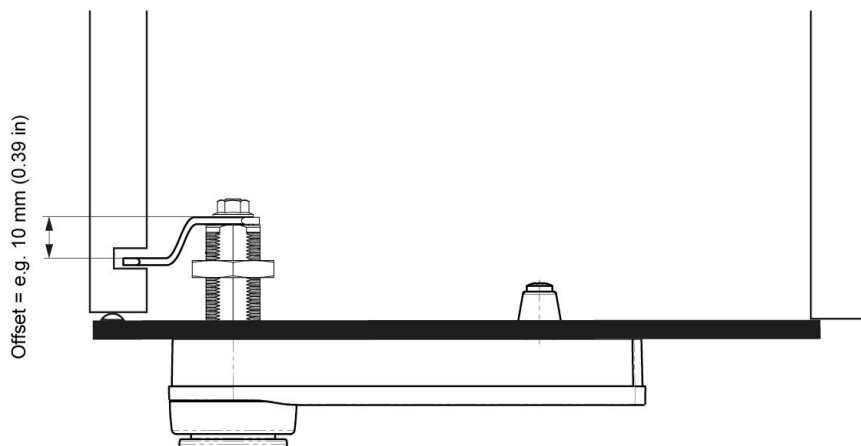
Figure 3.4 – *Example of offset latch for existing locker*

3.7 Definition of the Door Hinge (Right of Left-Hinged Door)

For installation, it is important to determine whether the locked door is hinged on the left or right side, which is defined as follows:
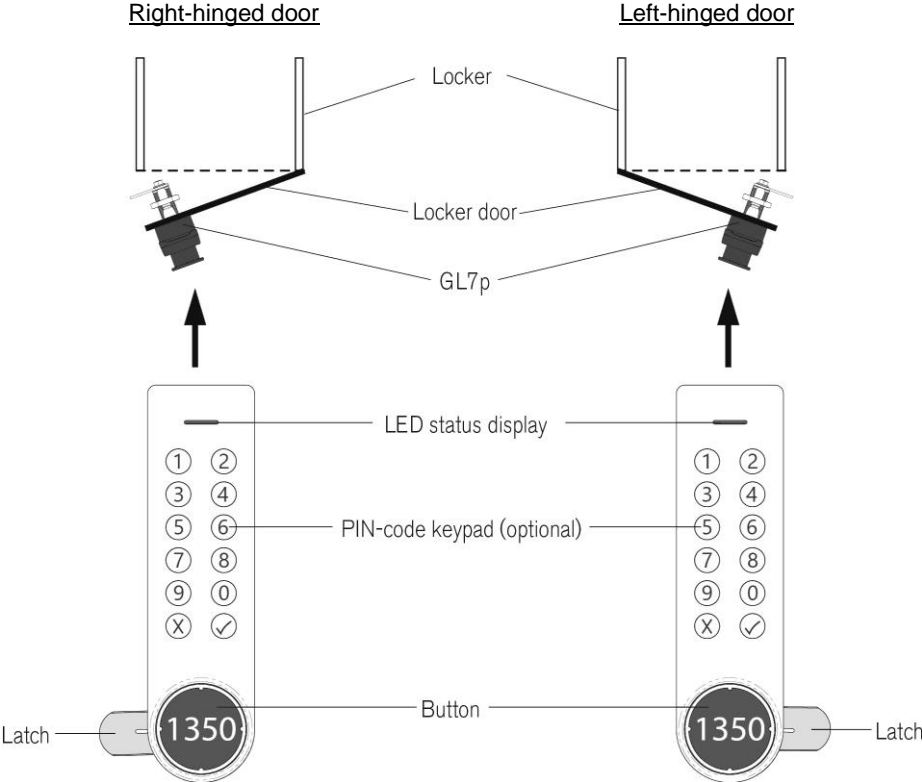
Figure 3.5 – Locker door hinge definition (left/right) for vertical mounting of the lock
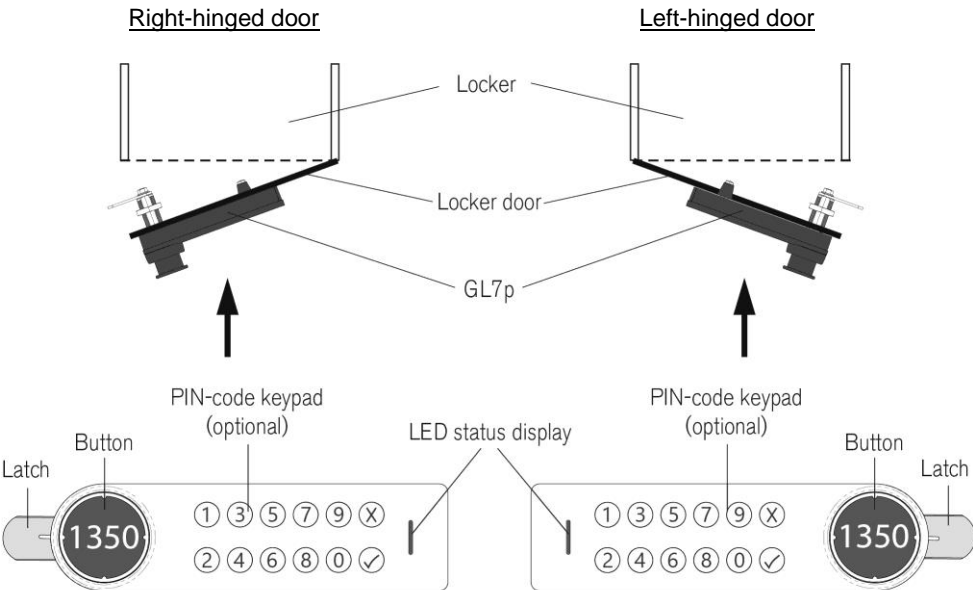
Figure 3.6 – Locker door hinge definition (left/right) for horizontal mounting of the lock

The position of the latch of the GL7p is different for right and left-hinged doors. You can make this change yourself (see "3.8.2 Instructions for Installing the GL7p").

The installation for right-hinged doors is described in the following pages. The installation process for left-hinged doors is the same as for right-hinged doors, except that the locker door is rotated 180° and when the GL7p is mounted horizontally, the lock is also rotated 180°.

3.8 Installation of the GL7p

After determining the alignment of the lock and the door stop, the mounting holes can be drilled. The following description shows the holes for a right-hinged door with vertical lock mounting.

NOTE! Before installing all locks in a new locker system, a test installation of one lock into a completed locker and a functional check must be performed. See section "3.2. Test Installation".

3.8.1 Mounting Holes in the Door

Two holes must be drilled in the door. If a DD cut-out with 19.1 x 16.1 mm (0.75 x 0.63 in) already exists, e.g., when replacing an existing mechanical lock, this can also be used.

Vertical mounting   **Horizontal mounting**
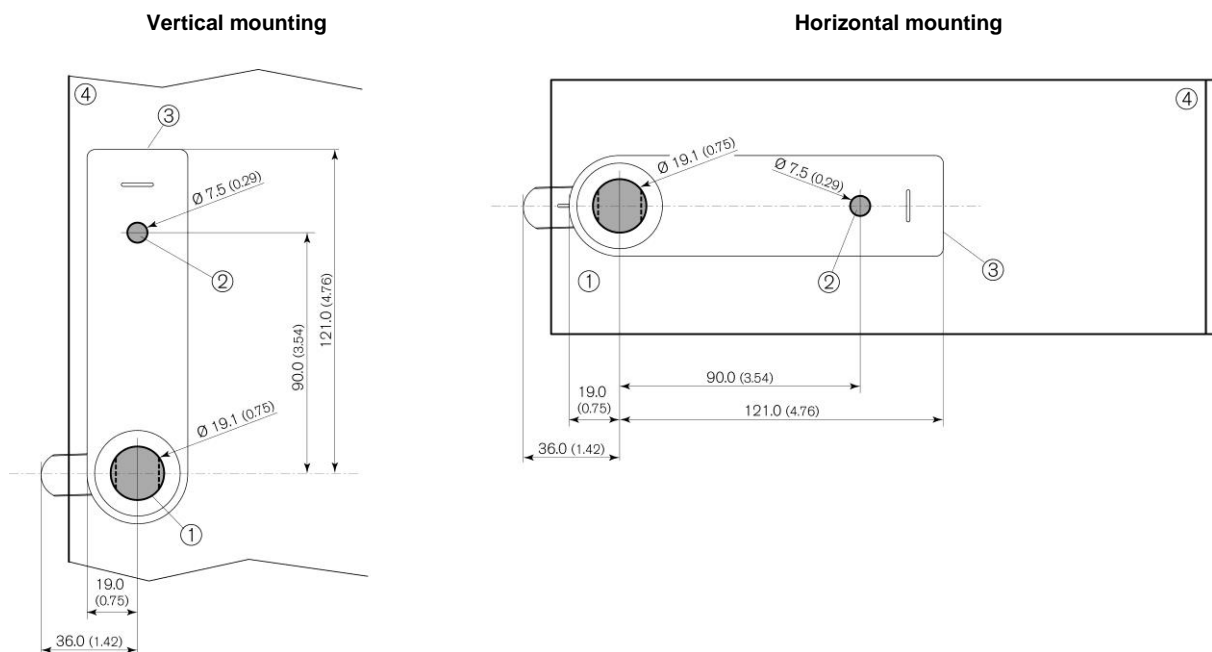
1. Hole or DD cut-out for mounting thread
2. Hole for anti-rotation prevention
3. Lock position after installation
4. Locker door

(Measurements in mm, inches shown in brackets)

***Figure 3.7** – Mounting holes in the door*

► For the mounting thread, drill a hole (1) of Ø 19.1 mm (0.75 in) in the locker door. If a DD cut-out with 19.1 x 16.1 mm (0.75 x 0.63 in) already exists, e.g., when replacing an existing mechanical lock, this can also be used.

► A second hole (2) of Ø 7.5 mm (0.29 in) is also required in the locker door to prevent rotation of the lock.

3.8.2 Instructions for Installing the GL7p

After drilling the mounting holes, complete the following steps to install the GL7p according to the installation diagram.
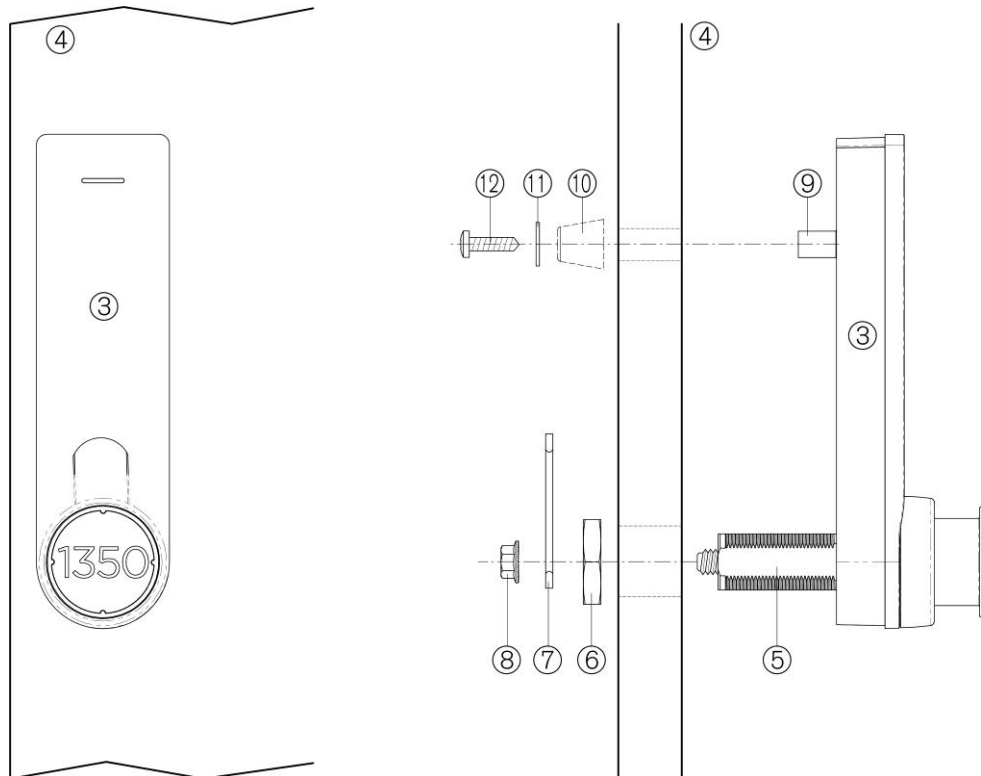
3. GL7p	8. Lock nut
4. Locker door	9. Anti-rotation dome
5. Mounting thread	10. Spacer sleeve (only for thin doors under 10 mm, e.g., single-wall metal door)
6. Fixing nut	11. Washer (only if spacer is not used)
7. Latch	12. Screw for anti-rotation [1]

1) For doors with a thickness of 1 to 5 mm and 13 to 18 mm, a corresponding KA35 screw is included with the delivery. For other door thicknesses, use appropriate KA35 or 3.5 mm self-tapping screws.

Figure 3.8 – Installation of the GL7p

► Mount the GL7p onto the locker door by inserting the mounting thread (5) and anti-rotation dome (9) into the holes in the locker door.

► Screw the fixing nut (6) onto the mounting thread and tighten the nut so that the lock is held firmly on the door (torque max. 5 Nm).

► Insert the latch (7) in the correct orientation onto the fixing screw.

Gantner

Vertical mounting	Horizontal mounting, right door	Horizontal mounting, left door
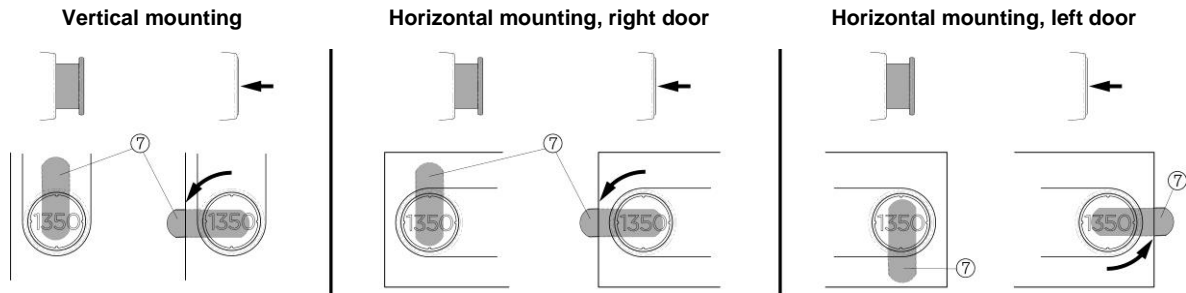
► Tighten the lock nut (8) so that the latch is firmly attached (torque max. 1.5 Nm).

► Secure the anti-rotation (tightening torque max. 1.0 Nm) using a screw suitable for the door thickness and, if necessary, the spacer sleeve and/or washer:

- For door thicknesses 1 to 5 mm: supplied screw + spacer sleeve

- For door thicknesses 5 to 10 mm: KA35x20 screw + spacer sleeve

- For door thicknesses greater than 10 mm: supplied washer + KA35 screw suitable for the door thickness or 3.5 mm tapping screws

Door thickness > 9.5 mm	Door thickness < 9.5 mm
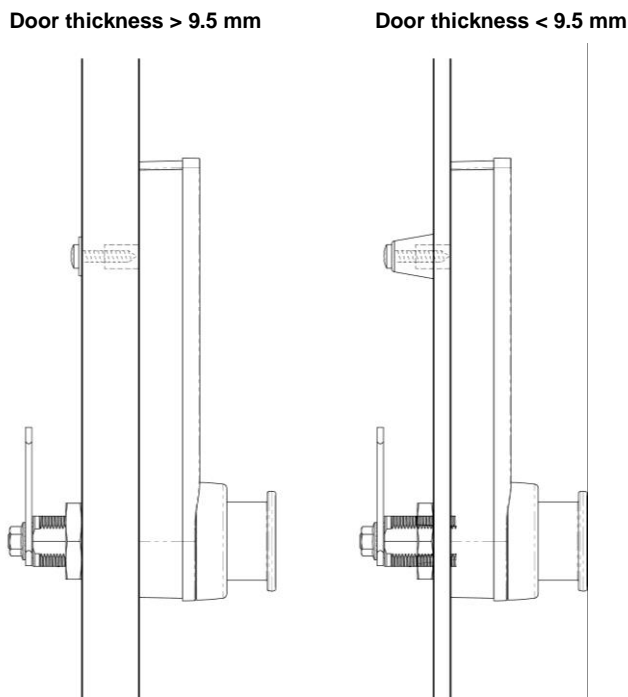
Figure 3.9 – Side view of the GL7p after installation with different door thicknesses

► Finally, ensure that the latch can be closed and opened without resistance (press the button).

► When the locker is locked, ensure that the door is held in the closed position by the latch without creating a door gap.

ℹ *See chapter "4 COMMISSIONING" for information on how to insert the batteries and commission the GL7p.*

3.9 Attaching the Number Plate

On the button of the GL7p, the round number plate (0.8 mm thickness) must be attached. A neutral-white number plate without printing is included with the GL7p upon delivery (GL7p Button Plate, Part No. 748633). The number plate can also be ordered with laser numbering. This will be delivered as standard with a 4-digit number (GL7p Number Plate, Part No. 1103180).

In addition, a button sticker (GL7p Number Sticker) can be attached to the number plate; however, this is not mandatory. The button sticker is available with pre-printed numbers ranging from 001 to 500. The stickers can be ordered in sheets with 50 consecutive numbers (for article numbers see "2.6. System Components").

The button sticker can also be ordered with customized printing, e.g., with a logo, color, individual number, or text. Please contact GANTNER Electronic GmbH for more information.

1. GL7p
2. Button
3. Number plate
4. Button sticker (optional)
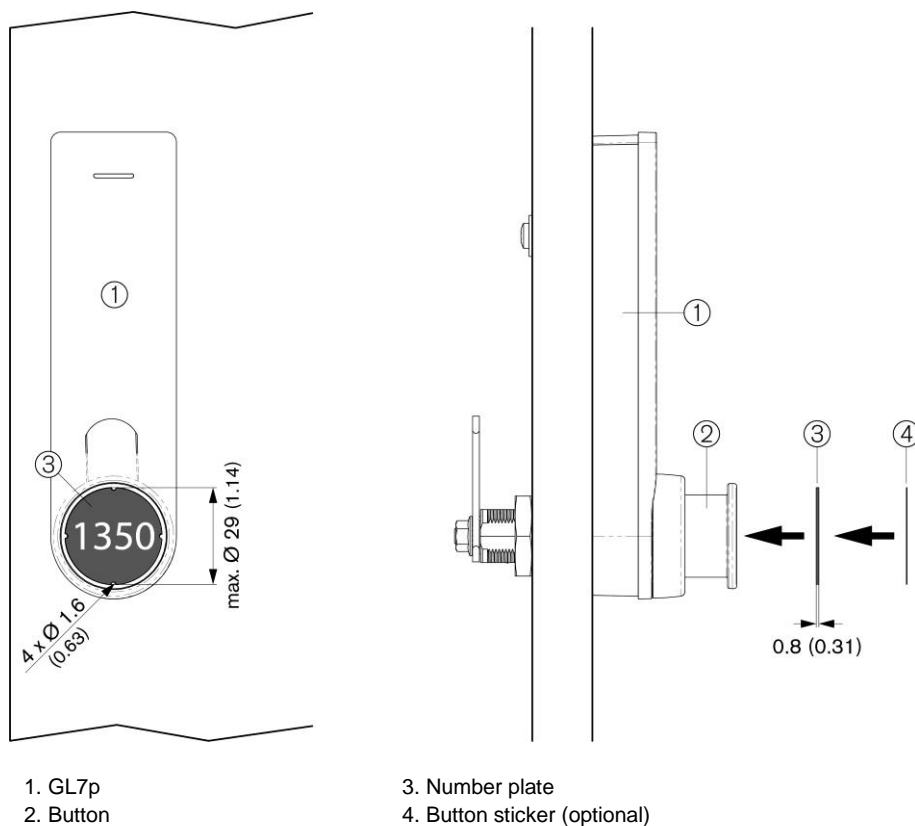
***Figure 3.10** – Number plate and button sticker on a right-hinged door*

Gantner

► Before attaching the number plate, ensure that the surface of the button is free of dirt and dust.

► Align the number plate with the 4 tabs in the button and attach it.

► If applicable, align the button sticker with the 4 tabs in the button and attach it to the number plate.

i *For more information on the design and printing of customized button stickers, please contact your GANTNER reseller.*

4 COMMISSIONING

4.1 Target Group

This chapter provides information for technicians responsible for putting the GL7p into operation. A base knowledge of electronics is assumed. Previous knowledge of the GL7p is not required.

4.2 Power Supply

4.2.1 Battery Information

The GL7p is powered by one 3.6 V AA lithium battery (see "8. TECHNICAL DATA"). The life of the battery depends on the number of locking cycles (frequency of use of the lock) and the ambient conditions. The battery must be replaced with a new one when the battery voltage becomes too low. If the battery becomes too weak, the locker can no longer be locked. The GL7p indicates a low battery condition by blinking the LED 5 times red during an unlocking and a locking attempt, and the lock emitting 5 beeps.

NOTE! Only the GANTNER approved batteries may be used to power the GL7p (see "8. TECHNICAL DATA").

4.2.2 Inserting the Battery

To put the GL7p into operation, insert the battery into the battery compartment of the GL7p. To access the battery compartment, the battery cover must be opened using the battery key included in the "GAT ECO.Basic Set FD".
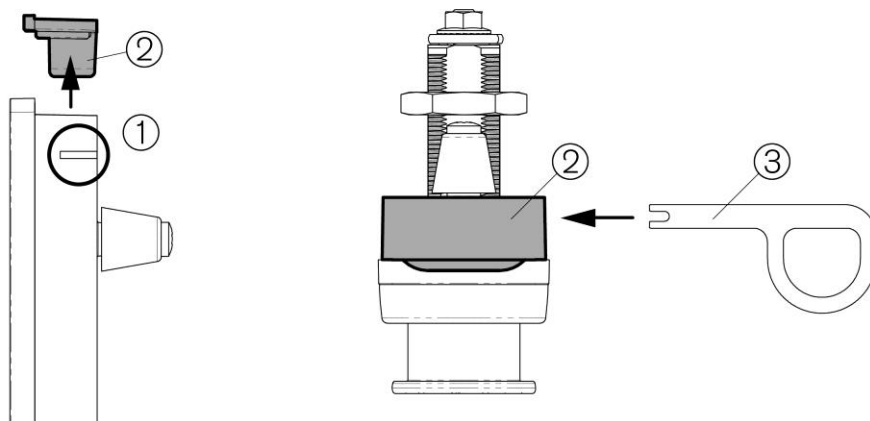
***Figure 4.1** – Opening the battery compartment of the GL7p*

► Insert the battery compartment key (3) into the slot (1) on the side of the GL7p.
  o The battery compartment cover unlocks.

► Remove the battery compartment cover (2).

► Insert the battery (4) into the battery compartment with the polarity as shown in the following picture.
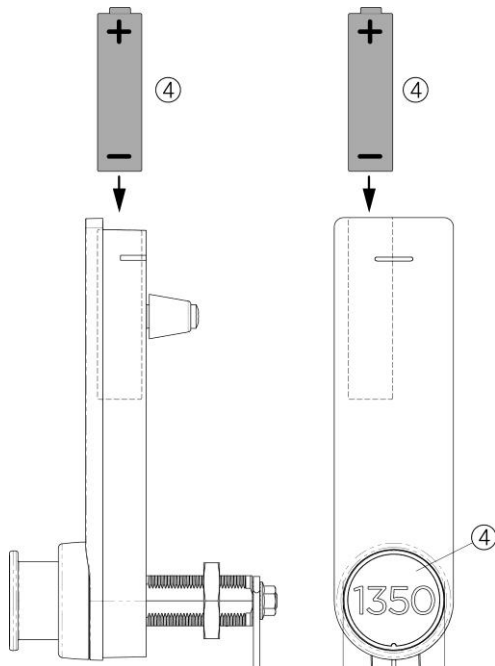
Figure 4.2 – *Insert battery - observe the correct polarity*

► Replace the battery compartment cover onto the battery compartment and push it down until it clicks into place.

► Press the button of the GL7p in completely using the BATTERY data carrier.
  o The BATTERY data carrier is read by the GL7p and, if read correctly, the GL7p is enabled.

4.2.3 Replacing the Battery

The battery of the GL7p must be replaced when the LED flashes red 5 times and 5 acoustic signals are emitted during a locking or unlocking attempt. In this state, the GL7p can no longer be locked until the batteries are replaced.

Always dispose of used batteries in an environmentally friendly manner, e.g., at an electronic waste recycling facility.

To ensure that the time and date remain correct after a battery change, the battery replacement must not take longer than 3 minutes. If the GL7p is without battery for more than 3 minutes, the time and date must be reset. Since the time may be different from the real time after prolonged use of the GL7p, GANTNER recommends resetting the time and date after each battery change (see section "5. CONFIGURATION").

Following battery replacement, the GL7p must be returned to its normal operating mode using the "BATTERY" data carrier (= battery cover key) (see section "6.5.5. BATTERY Data Carrier").

► Complete the instructions described in section "4.2.2. Inserting the Battery".

► Press the locker door shut with one hand and hold it shut.

► Press the button of the GL7p in completely using the BATTERY data carrier.

    o The BATTERY data carrier is read by the GL7p and, if read correctly, the GL7p is enabled.
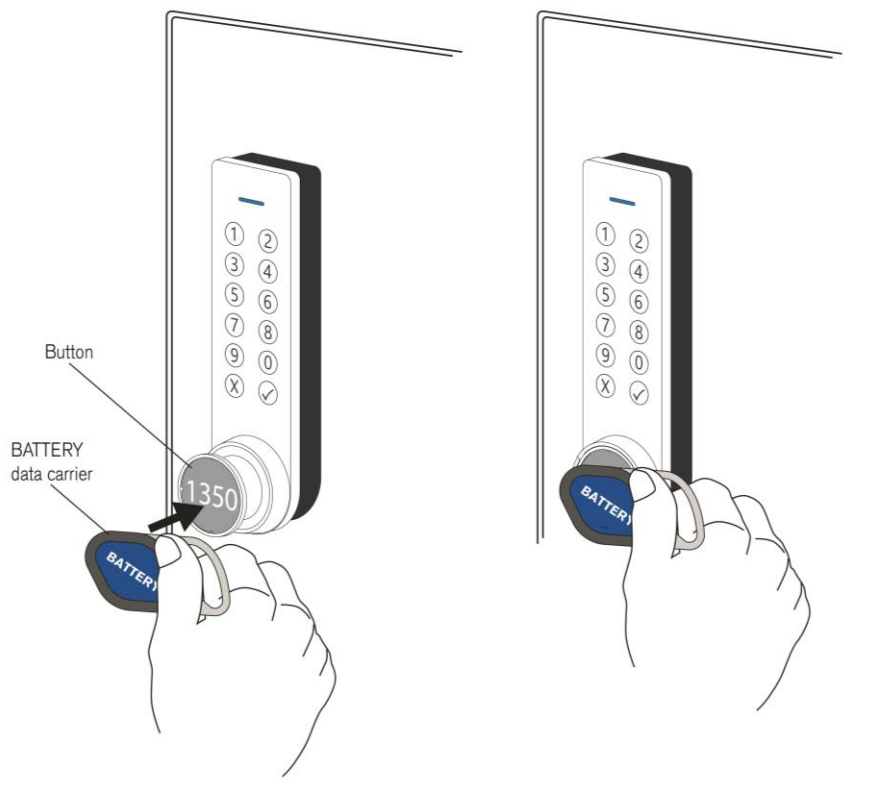
Figure 4.3 – *Activating the GL7p with the BATTERY data carrier*

After battery replacement, it is recommended to always check the date and time of the GL7p and set them correctly if necessary.

4.3 USB Connection

To connect to a computer with Windows® operating system (Windows® 7 or higher), a Micro-B USB port is provided on the side of the GL7p. The USB port location on the side of the lock allows configuration to be carried out even while the lock is installed.

NOTE! The maximum cable length between the GL7p and a computer is 5 m. The Micro-B USB connector can have a maximum width of 4 mm.

After the USB cable is connected, the SERVICE data carrier (see "6.5.6 SERVICE Data Carrier") is used to put the GL7p into configuration mode. A 3 m USB cable, the SERVICE data carrier, and GAT Config Manager configuration software are included in the GAT ECO.Basic Set (see section "6.4 GAT ECO.Basic Set FD").

To configure the GL7p via PC/laptop:

► Start GAT Config Manager on the PC/laptop.

► Connect the USB cable (type-A end) to a spare USB port on the PC/laptop.
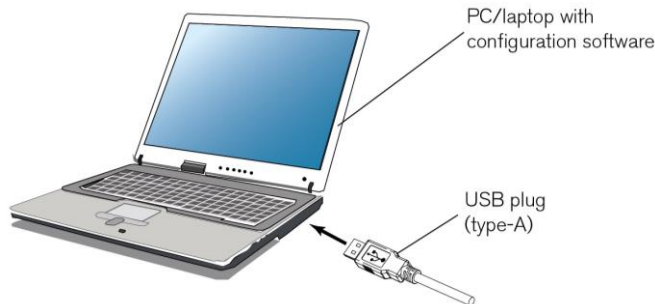
► Open the battery compartment (see section "4.2.2. Inserting the Battery")

► Connect the Micro-B connector of the USB cable into the USB port on the GL7p.
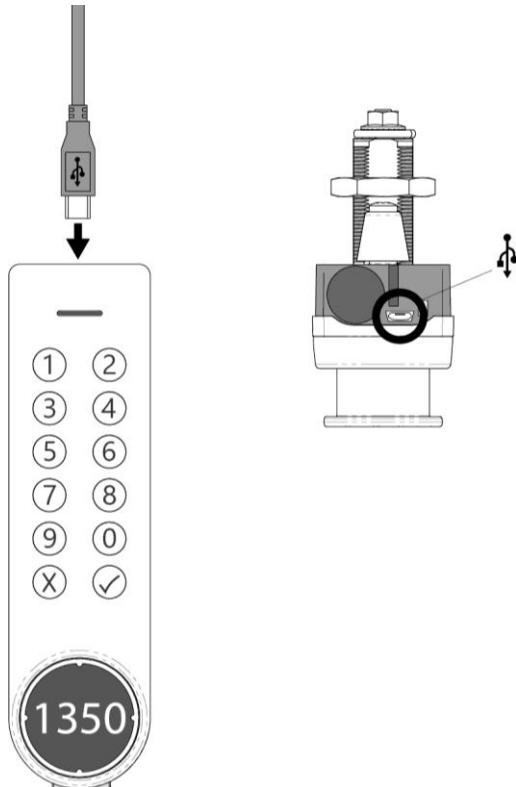
    o   When the GL7p is connected to the computer for the first time, the driver is automatically installed and the lock recognized.

ℹ️ *If the automatic driver installation does not work and you need the driver, it is availble on the "Leisure Software" USB stick in the GAT ECO.Basic Set or via the partner area of the GANTNER website.*

► After connecting to the computer, the LED flashes red/green alternately (if the GL7p has already been configured once).

► Now press the button of the GL7p to activate configuration mode.

    a) If the lock has not been configured yet (default setting), the GL7p only has to be connected.

    b) If the lock has already been configured at least once, i.e., the default setting has been deactivated, the button must be pressed with the SERVICE data carrier from the Basic Set.
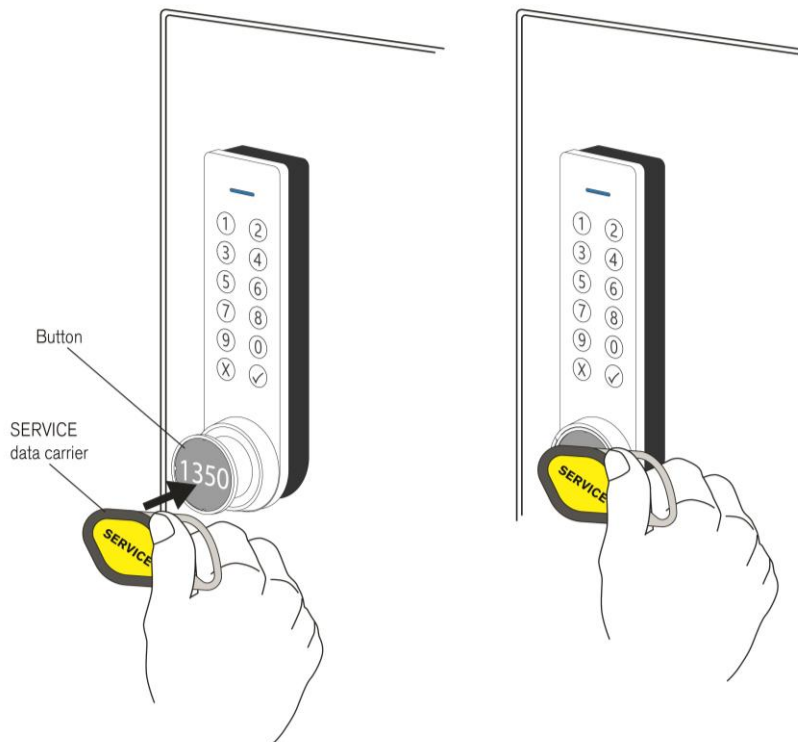
    o   The GL7p enters into configuration mode and the LED slowly pulses green to indicate this state.

► In GAT Config Manager, click on "Configure" to open the configuration settings.

Further information regarding configuring the GL7p is available in "5. CONFIGURATION".

5 CONFIGURATION

RF exposure statement

The users must keep at least 20 cm separation distance from the device, except during the identification and operation process at the device (e.g. PIN-code input), which must be performed as described in this manual.

5.1 General Information

The GL7p is configured using a PC/laptop and GAT Config Manager software or with the MoLA app on a mobile device. The configuration file must only be uploaded to the lock once. The configuration file of the first lock in the system is saved in GAT Config Manager after which the file is uploaded to each lock that requires the same configuration. Locks that require a different configuration need a separate configuration file to be made in GAT Config Manager.

The MoLA app can be downloaded from the Google Play Store and used with mobile devices with an Android operating system. The app uses NFC for configuration, which means that the mobile device must also support NFC communication. See more details in section "5.3. Configuration with the MoLA App".

NOTE! After importing the configuration file to the first lock, complete an operational test to ensure the user and MASTER data carriers and the general lock functionality perform as expected.

The following data is imported into the GL7p during configuration:

-   Site key
-   Sub-site number
-   Locker number
-   Lock operating mode ("free locker", "free locker universal", "free locker unique number", "personal locker programming card", or "personal locker expiry date". See section "6.3. Operating Modes")
-   Free locker: Sector number of the data on the data carrier and the time setting for the "duration of use" function
-   Date and time
-   Unique numbers of the MASTER data carriers (and OPEN MASTER data carriers, if used)

> *The MASTER data carriers and OPEN MASTER data carriers can also be directly programmed into the GL7p (see section "6.5.1 MASTER Data Carrier"). However, the most efficient way to program the data carrier numbers into multiple locks is via PC and GAT Config Manager.*

NOTE! The GL7p does not set the daylight-saving time automatically. Time changes due to daylight saving must be considered when evaluating bookings and also when authorizing data carriers with expiry dates/times!

5.2 Configuration with GAT Config Manager

5.2.1 Setup for Configuration in GAT Config Manager

Once the GL7p is connected to the computer via the USB cable (see "4.3. USB Connection"), and the SERVICE data carrier used to activate configuration mode (see "6.5.6 SERVICE Data Carrier"), the settings can be viewed and configured using GAT Config Manager.

NOTE! Min. version 3.13 of GAT Config Manager software is required to configure the GL7p.

NOTE! The GL7p is powered by the USB cable, which means that the battery does not have to be inserted in the lock during configuration. Ensure however that the GL7p is not de-energized for more than 1 minute (e.g., after disconnecting the USB cable until the battery is inserted), otherwise the time and date will be erased.
Complete the following steps to configure the GL7p via GAT Config Manager.

> *There is a separate manual with detailed information on each function available in GAT Config Manager. To access the manual while the software is open, click on the "Help" menu and select "How Do I".*

► After installing the software, open GAT Configuration Manager via "Start" -> "All Programs" -> "GANTNER Electronic GmbH" -> "GAT Config Manager" -> "GAT Config Manager".

   o The default start window of GAT Config Manager is displayed.

► Click on the "Open Project" icon ("1" in Figure 5.1) to find an existing project.

► Alternatively, click on the "Create Project" icon ("2" in Figure 5.1) to start a new project.
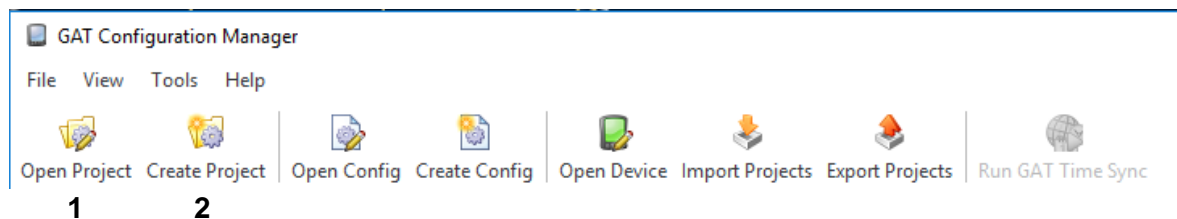
Figure 5.1 – *GAT Config Manager – Project setup*

► Once a project is established, locations and sub-locations for the project can be added to the "Devices" directory (2 in Figure 5.2) by clicking on the "Add location" button (1 in Figure 5.2).
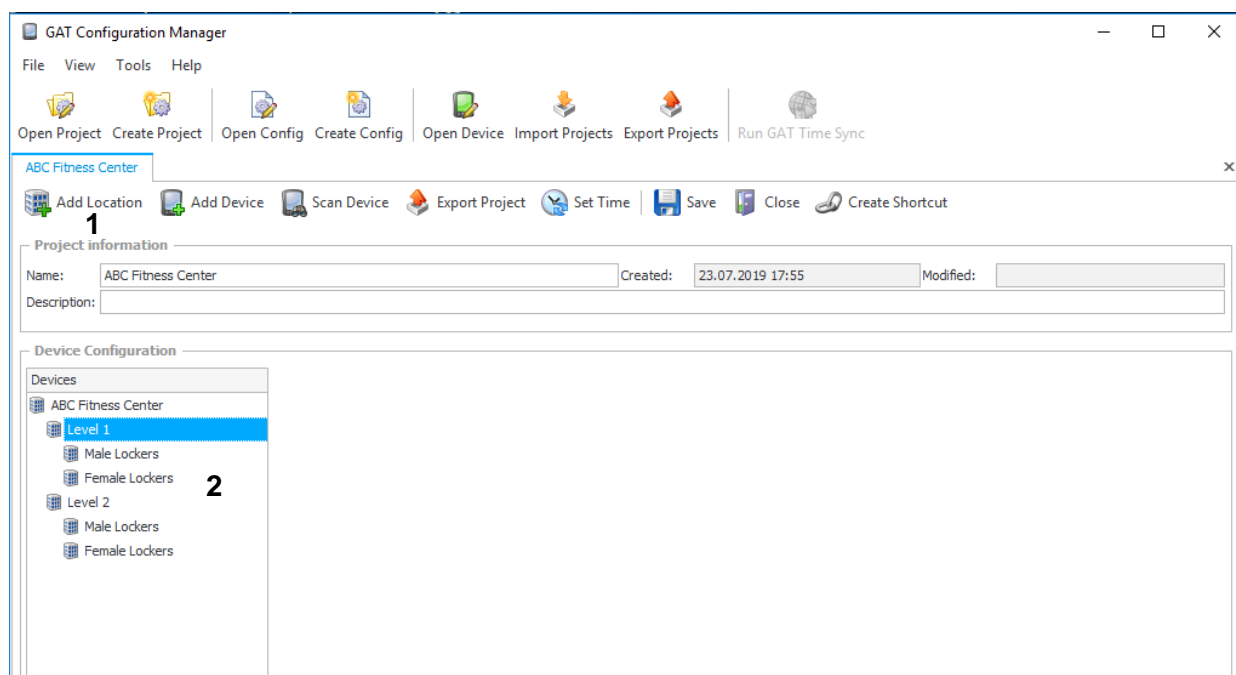
Figure 5.2 – *GAT Config Manager – Add location*

► To add a GL7p to a location, right-click on the location and select "Add GAT Lock 7000 Series" from the "Add Device" menu (Figure 5.3).

  o The GL7p is added to the selected location.
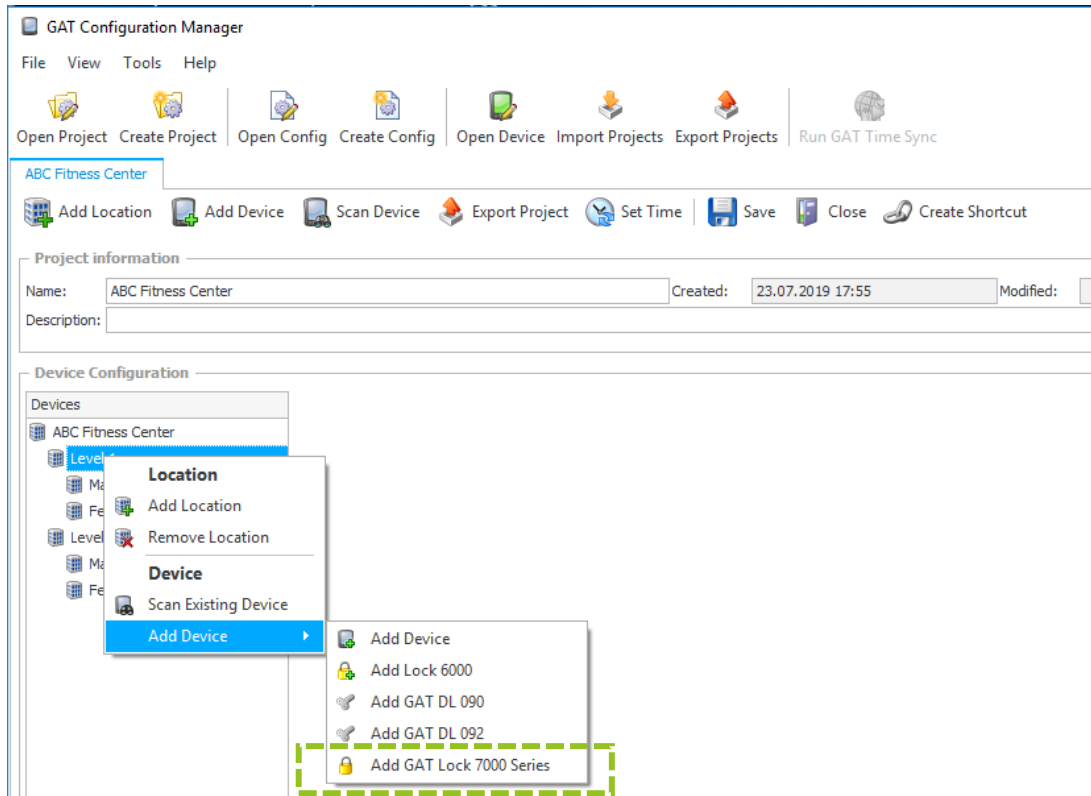
***Figure 5.3** – GAT Config Manager – Adding a GL7p*

5.2.2 View and Edit the GL7p Configuration Settings

Once the GL7p has been added to the device list and you have connected the lock to the PC (see "4.3. USB Connection"), you can now view and edit the lock configuration settings. Complete the following steps to view the configuration settings.

► Select the GL7p from the "Devices" list (1 in Figure 5.4).

  o The GL7p is highlighted in color.
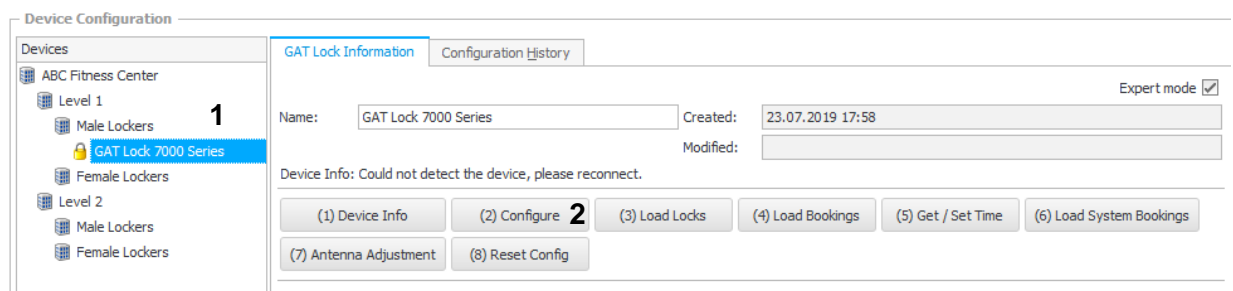
***Figure 5.4** – GAT Config Manager - View configuration settings*

► Click on the "(2) Configure" button (2 in Figure 5.4).
  o The "GAT Configurator" window opens (Figure 5.5).
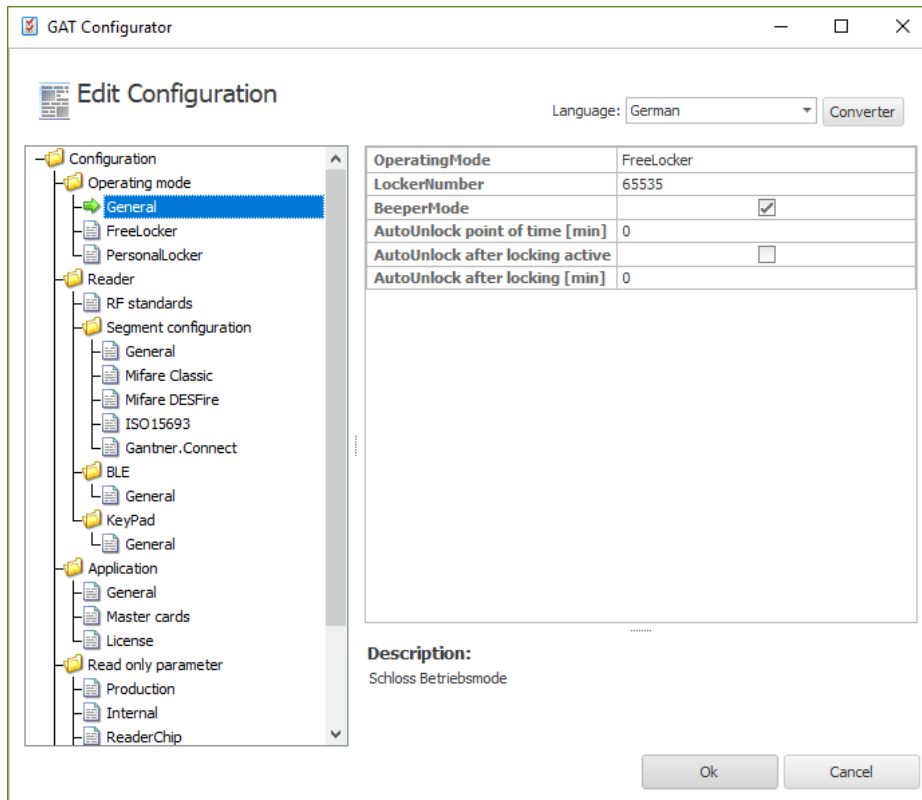
Figure 5.5 – *"GAT Configurator" configuration window*

5.2.3   Upload Configuration Settings to the GAT ECO.Lock 7xxx F/ISO

When you are finished configuring the GL7p settings in GAT Config Manager, it is important to finalize the configuration by uploading the file to the GL7p. Complete the following steps to finalize the configuration.

► Click on "OK" in the GAT Configurator window (Figure 5.5).
  o The confirm upload window opens.

► Click "Yes" to apply the configuration to the lock.
  o The configuration settings are uploaded to the GL7p.

5.2.4 Updating the GL7p Firmware

GANTNER periodically releases firmware updates for the GL7p. In order to take advantage of the latest features, it is recommended to update the GL7p to the latest firmware during configuration or at regular intervals.

► Right-click onto the GL7p in the "Devices" tree and select "Update Firmware".
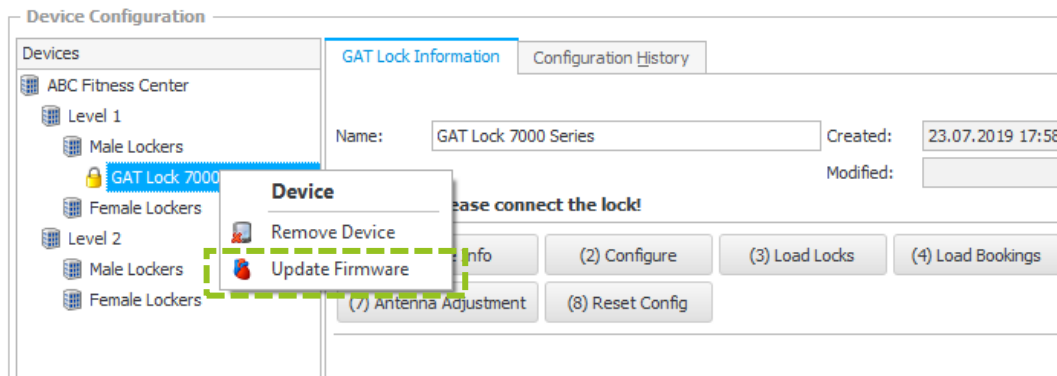
Figure 5.6 – GAT Config Manager - Updating the GL7p firmware

o The "Device update wizard" opens.
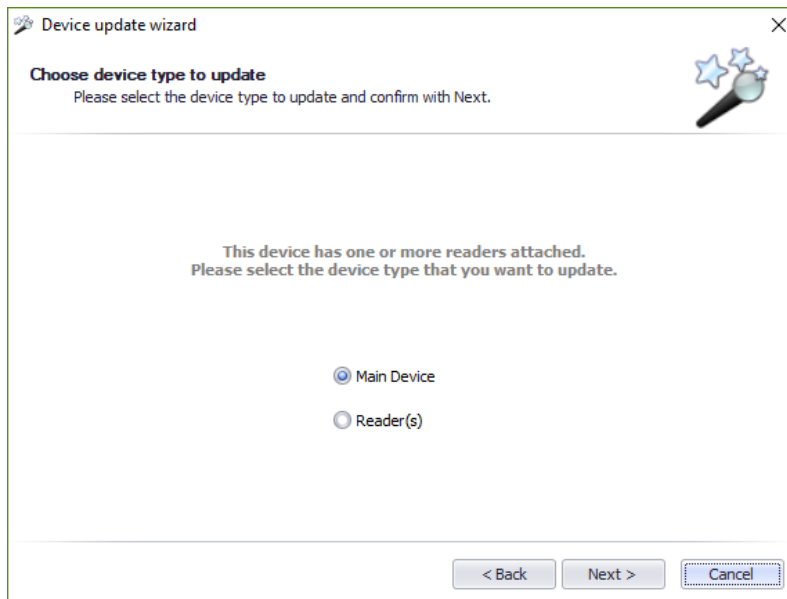
Figure 5.7 – Device update wizard - Device selection

► Select which parts of the GL7p you would like to update:

   - Main Device: Firmware for the main GL7p device, which controls all main functions of the lock.

   - Reader(s): Firmware for one of the readers installed in the GL7p (RFID reader or wireless reader).

► Click on "Next".

o If "Reader(s)" is selected, an additional window opens in which you must select one of the available options for an update (if "Main Device" is selected, this window is skipped).
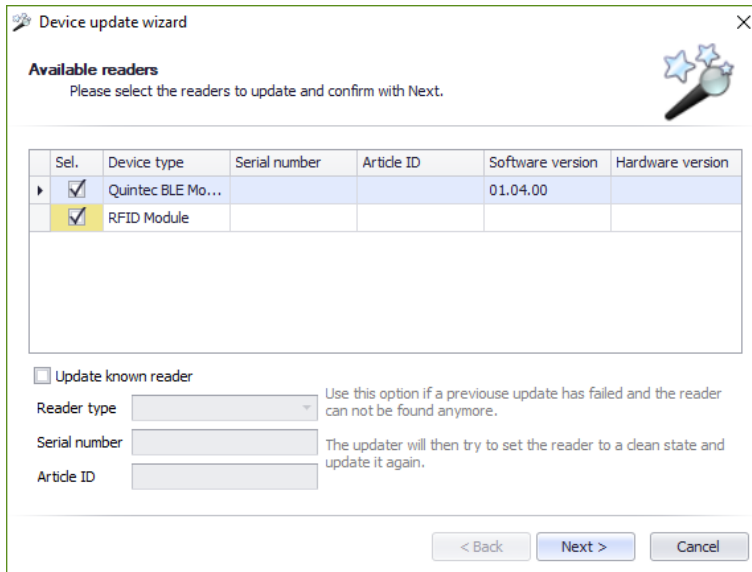
Figure 5.8 – *Device update wizard - Reader selection*

► Select the readers that require a firmware update.

- Quintec BLE Module: The wireless module for identification via radio connection (only for the GL7p.2xxx and GL7p.3xxx locks).

- RFID module: Standard RFID reader that reads the data carriers when the button is pressed.

► Click on "Next".

    o GAT Config Manager searches the GANTNER server for new firmware versions for the selected type (GL7p main device or the selected reader type). If a connection to the server cannot be established, or no new firmware versions are found, a corresponding message is displayed. In this case, click "OK".

    o A window with the available updates is displayed.
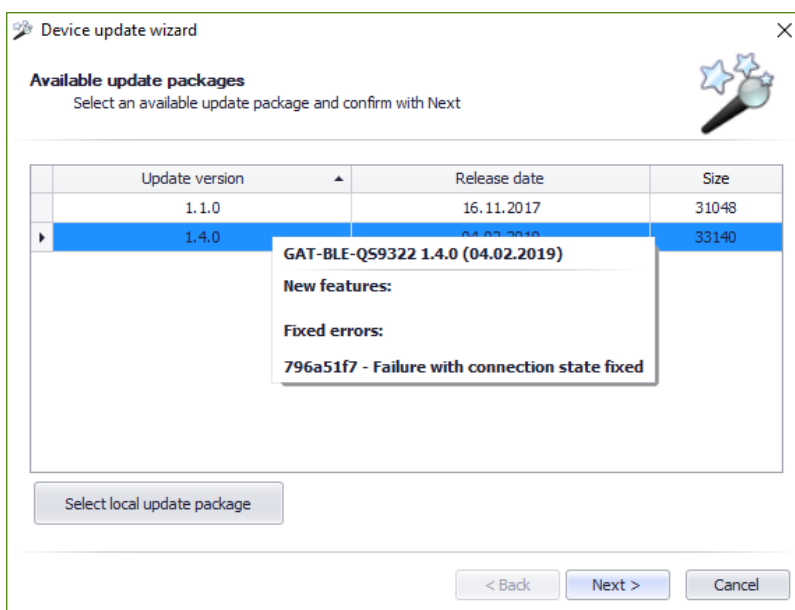
Figure 5.9 – *Device update wizard - Select firmware version or local firmware file*

Gantner

o   All available firmware versions for the previously selected device component (GL7p main device or the selected reader type) are displayed here.

► Hover the mouse over the desired version to see the included new features.

► Select the latest update and click on "Next".

► If no firmware versions are displayed, you can also select a locally stored firmware file by clicking on "Select local update package" and transfer it to the GL7p.

o   The "Device update wizard" downloads the update from the GANTNER server and transfers it to the GL7p. This usually takes about 1 minute. During the update, the LED on the GL7p flashes green and red alternately in rapid succession.

► Click on "Finish" when the update process is finished.

5.3 Configuration with the MoLA App

The MoLA app, which is available for download via Google Play Store, can be used with a mobile device, e.g., a smartphone, to configure the GL7p locks. To use the MoLA app, the following requirements must be fulfilled:

- Mobile device with Android 4.4.0 or later

- Mobile device must be NFC enabled

- Mobile device must not be rooted

- The GL7p must have firmware version 2.4.0 or higher)

- A valid APP KEY data carrier is required for configuring on-site locks

The MoLA app can be downloaded with this link from Google Play Store:

https://play.google.com/store/apps/details?id=com.gantner.mola

Due to technical limitations in iOS, the MoLA app is currently not available on Apple devices.

In MoLA you can change the same configuration settings like in GAT Config Manager (see "5.4. Configuration Settings of the GL7p"). A detailed description about the operation of the app is directly included in MoLA.

The APP KEY data carrier is a special system data carrier (see "6.5. Summary of System Data Carriers") and is included in the GAT ECO.Basic Set. This data carrier is required to change the configuration of a GL7p or to make a new configuration of a lock that has already been configured once.

When the GL7p is in factory mode (default, unconfigured state), the APP KEY is not needed.

Once the APP KEY data carrier is loaded into MoLA, it remains valid for a certain time period. When the session expires, the APP KEY is automatically deleted from the device. This prevents the APP KEY data carrier from being accessed by unwanted third-party apps, malware, etc.

5.4 Configuration Settings of the GL7p

The important configuration settings of the GL7p that can be adjusted in GAT Config Manager are explained in this section. A list and brief explanation of every configuration setting available for the GL7p is provided in section "5.4.10 Configuration Settings Table".

5.4.1 Operating Mode

The GL7p can operate in one of five different operating modes. See "6.3 Operating Modes" for a detailed description of each mode. The operating mode setting is found here:

Configuration > Operating mode > General > Operating mode

► In the "Operating mode" menu, select either:
- "FreeLocker"
- "FreeLockerUniversal"
- "FreeLockerUniqueNumber"
- "PersonalLocker_ProgrammingCard", or
- "PersonalLocker_ExpiryDate"

5.4.2 Locker Number

The number of the locker where the GL7p is installed can be defined. The locker number setting is found here:

Configuration > Operating mode > General > LockerNumber

► Enter the locker number for the GL7p into the "Locker number" field.

5.4.3 Auto-Unlock

The auto-unlock function automatically unlocks the GL7p at a defined point in time or after a specific time has elapsed after locking.

NOTE! When this function is activated, the lock will always unlock at the defined point of time regardless of the operating mode (see "6.3 Operating Modes").

The automatic unlocking function at a certain time after midnight is set via the following menu path:

Configuration > Operating mode > General > AutoUnlock [min]

► Enter a value representing the number of minutes into the field. The countdown time for unlocking begins at 00:00 (24 h). For example, a value of "300" means that the lock will unlock at 05:00 am. A value of "0" means that the function is inactive.

To use the automatic unlocking function after a certain time has elapsed after locking, first enable the option in the following configuration path:

Configuration> Operating mode> General> AutoUnlock after locking active

Next, you have to enter the desired time after a locking here:

Configuration > Operating mode > General > AutoUnlock after locking [min]

► Enter the time in minutes. The unlocking countdown therefore begins after each lock has been performed. For example, a value of "300" means that the lock will be automatically unlocked 5 hours after each time it is locked. If this function is activated, a value must be entered.

NOTE! For the automatic unlocking function, ensure that the correct time is set in the GL7p so that the automatic unlocking occurs at the correct time. Please note that the GL7p does not consider changes between summer and winter times.

5.4.4 Duration of Use

Lockers operating in free locker mode can be configured to limit the user to a defined period of use. See section "6.3.1. Free Locker Mode (with or without Duration of Use Function)" for detailed information. The duration of use function is found here:

Configuration > Operating mode > FreeLocker

► Select either "Duration" or "Point_of_time" from the "UseTimeLimit" menu for the type of time limit.
► Define the time limit in minutes in the "TimeLimit (min)" field.

5.4.5 Locking of Personal Locker without Data Carrier

The functionality of locking personal lockers without data carriers allows the locker to lock automatically when the locker door is pushed shut, without needing to use a data carrier. The locker can be unlocked again using the data carrier(s) authorized to use the personal locker. The function is found here:

Configuration > Operating mode > PersonalLocker > PreLock PersonalLocker

► Select / deselect the "PreLock Personal Locker" option to turn the function on / off.

5.4.6 RF Standards

The GL7p can operate with data carriers that use ISO 15693, ISO 14443A (MIFARE), and HID iCLASS (13.56 MHz UID) technology.

i *The default setting of the GL7p is to operate with ISO 14443A (MIFARE) data carriers.*

The setting for the GL7p to operate with ISO 14443A (MIFARE) data carriers cannot be disabled. The setting for the GL7p to operate with ISO 15693 or HID iCLASS data carriers can be adjusted and is found here:

Configuration > Reader > RF Standards > ISO15693
or
Configuration > Reader > RF Standards > HID

► Select / deselect the "ISO 15693" or "HID" option to turn the setting on / off.

Gantner

5.4.7   MASTER Data Carriers

Up to 10 MASTER data carriers (also called MASTER cards) can be assigned to the GL7p to allow the locker to be opened in special circumstances, e.g., when a user has lost their data carrier. For this functionality, the MASTER data carriers must be first entered, which is done here:

Configuration > Application > Master cards > MasterCard1 - 10

► Enter the number of each MASTER data carrier into the respective fields.

NOTE! The MASTER data carrier numbers must be entered in hexadecimal format.

> *There is also an OPEN MASTER data carrier available (not included in the Basic Set). This special data carrier can be used like the MASTER data carriers to open all lockers; however, it cannot lock the lockers. It is possible to program an OPEN MASTER data carrier by entering the number of the OPEN MASTER data carrier into 1 of the 10 fields. In this case, only 9 MASTER data carriers can be used.*

5.4.8   Wireless Interface

For GL7p variants with a wireless interface (variants GL7p.**2**xxx and GL7p.**3**xxx), the identification can also be transmitted wirelessly, e.g., via smartphone. The wireless interface can be enabled via the following option.

Configuration > Application > Reader > BLE > General > BLE enabled

► Select the option if you want to use the wireless interface.
► You can configure the wireless interface as required via the other fields in this window.

5.4.9   PIN-Code Keypad

For GL7p variants with a PIN-code keypad (variants GL7p.**1**xxx and GL7p.**3**xxx), the identification can also be completed using a PIN code. To allow entry via PIN code, the following option must be enabled.

Configuration > Application > Reader > KeyPad > General > KeyPad enabled

► Select the option if you want to use the PIN-code keypad.
► Via the other fields in this window, you can specify the time within which a PIN code must be entered and set the permitted length of the PIN code.

5.4.10 Configuration Settings Table

The following table lists all the configuration information available for the GL7p in GAT Config Manager.

Options	Description	Format	Default
Operating mode			
General			
OperatingMode	Select the operating mode of the lock: - "FreeLocker" - "PersonalLocker_ProgrammingCard" - "PersonalLocker_ExpiryDate" - "FreeLocker_UniqueNumber" - "FreeLockerUniversal"	List option	Free Locker
LockerNumber	Define the locker number	Integer	65535
BeeperMode	Switch on/off the integrated beeper	Boolean	True
AutoUnlock point of time [min]	Unlock locker at a defined time (input in minutes after midnight), "0" = inactive	Integer	0
AutoUnlock after locking active	Unlock locker automatically after being locked for a certain time	Boolean	True
AutoUnlock after locking [min]	Time in minutes after which the locker is unlocked after locking (if the function is activated, see previous setting)	Integer	0
FreeLocker			
UseTimeLimit	Select the type of time limit for the locker (see "6.3.1. Free Locker Mode (with or without Duration of Use Function)"): "Duration" or "Point of time"	List option	Duration
TimeLimit [min]	Define the time limit. Value must be entered in minutes (if the most significant bit is not set) or in hours (if the most significant Bit is set). Examples: Dec. value 1 up to 32767 -> 1 up to 32767 minutes Dec. value 32768 to 65535 -> 1 up to 32766 hours	Integer	60
TimeLimit Interrupt Timeout [min]	Minimum waiting time from the end of a locker usage period until the next usage period can begin	Integer	60
CardValidityDateRequired	When set to "True", a valid expiration date must be set on the data carriers for them to be used (default: 1.1.2007 is not valid)	Boolean	False
PersonalLocker			
Index PersonalLocker	Define the index of the personal locker	Integer	0
PreLock PersonalLocker	Switch on/off the automatic lock function without data carrier for personnel lockers	Boolean	False
PersonalLockerSecureFlag	When set to "True", a new index or validity date can only be transferred from a data carrier to the lock when the locker is open. When this option is deactivated, transferal is possible even when the locker is locked (see "6.3.5. Personal Locker Expiry Date Mode")	Boolean	False
LastOpenAtExpiredDate	When set to "True", a locker can be reopened after the expiration of its useful life using the data carrier with which it was locked (see "6.3.5. Personal Locker Expiry Date Mode")	Boolean	False
WriteLockerData PL ExpDate	When set to "True", the lock status is written to the data carrier when the data carrier is read	Boolean	False

Reader				
	RF Standards			
	ISO15693	When set to "True", ISO 15693 data carriers can be read by the lock	Boolean	False
	ISO14443A	When set to "True" ISO 14443 (MIFARE) data carriers ca be read by the lock. This setting is not configurable.	Boolean	True
	HID	When set to "True", the device can read HID iCLASS data carriers (UID number only)	Boolean	False
	Segment configuration			
		General		
		SiteKey	Site key of the device. All data carriers must have the same site key to be used with the device.	Hex	9999
		KeySet	DESFire AES keys, encrypted	Hex	
		MIFARE Classic	Options for reading MIFARE Classic data carriers		
		SectorNum	The segment where UID data is stored	Integer	4
		ReadKey	Select the "Read Key" (Key A or Key B)	List option	
		WriteKey	Select the "Write Key" (Key A or Key B)	List option	
		MIFARE DESFire	Options for reading MIFARE DESFire data carriers		
		ReadKeyNum	Number of the "Read Key"	Integer	
		WriteKeyNum	Number of the "Write Key"	Integer	
		ApplicationId	ID of the target DESFire application	Text	
		EncryptionMode	Select the type of encryption mode	List option	
		FileNum	File number to read data from	Integer	
		FileCommMode	File communication mode: "Plain", "Maced", "Enciphered"	List option	
		FileType	Type of file: "Standard", "Backup"	List option	
		FileDataOffset	Data offset in the DESFire locker file	Integer	0
		ISO15693	Options for reading ISO 15693 data carriers		
		GeneralBlockNum	The segment where general data is stored	Integer	13
		CertificateBlockNum	The segment where certificate data is stored	Integer	15
		LockerBlockNum	The segment where locker data is stored	Integer	19
		Gantner.Connect			
		FileId	ID number for Gantner.Connect.	Integer	1
	BLE			
		General		
		BLE enabled	Option to enable/disable the wireless interface for GL7p.2xxx and GL7p.3xxx locks	Boolean	False
		KeySet BLE	Custom key for the wireless interface GANTNER standard = 0	Hex	
		BLE advertise timeout idle mode	Time to detect the wireless interface in idle mode. Input in 100 ms (e.g. 600 = 1 minute). Idle mode begins after activation mode has expired. If you enter "0", idle mode is active indefinitely	Integer	600
		BLE pulse period idle mode	Period between radio pulses in idle mode. Input in 100 ms (e.g. 600 = 1 min.). As each pulse requires energy, the period should be set so large depending on the application that wireless signals are still detectable	Integer	20
		BLE advertise timeout activation	Time to detect the wireless interface in activation mode (after pressing the button). Input in 100 ms (e.g. 600 = 1 min.). When activation mode is over, idle mode starts. If you enter "0", activation mode is active indefinitely and idle mode is not used	Integer	150

	BLE pulse period activation	Period between radio pulses in activation mode. Input in 100 ms (e.g. 600 = 1 min.). As each pulse requires energy, the period should be selected so that wireless signals are still quickly detectable in activation mode.	Integer	5
	BLE PreLock Timeout	Period to lock the GL7p after a wireless command. Input in seconds.	Integer	10
KeyPad				
	General			
	KeyPad enabled	When set to "True", entry via PIN code is possible for the GL7p.1xxx and GL7p.3xxx locks	Boolean	False
	Pin code timeout	Max. input time between 2 digits of the PIN code. If no additional key is pressed during this time and the entry is not confirmed with (✓) or button, the entry is cancelled. Input in 100 ms (e.g., default value 40 = 4 seconds).	Integer	40
	Minimum PIN length	Minimum required PIN code length	Integer	4
	Maximum PIN length	Minimum required PIN code length	Integer	8
	Activate pin code UseTimeLimit	When set to "True", the usage duration is used for PIN code entry, analogous to the operation with data carriers. See "6.3.1. Free Locker Mode (with or without Duration of Use Function)"	Boolean	False
Application				
	General			
	Legacy BasicSetCoding	When set to "True", data carriers in the Basic Set are coded for a predecessor system (previous coding)	Boolean	False
	Master cards			
	MasterCard1 - 10	Fields to enter number for MASTER data carrier 1-10	Integer	
	License			
	License CertificateCheck	When "installed" is displayed here, the certificate check can be switched on/off.	Info	
	CertificateCheck enabled	Switch on/off the certificate check for data carriers	Boolean	False
Read only parameter				
	Production	Production-specific information about the GL7p		
	ArticleNum	Part number of the lock	Integer	
	SerialNum	Serial number of the lock	Integer	
	ManufacturerNum	Manufacturer number of the lock	Integer	
	ProductionYear	Production year of the lock	Integer	
	ProductionWeek	Production week of the lock	Integer	
	HardwareUidNum	Unique ID number of the lock	Integer	
	ControllerType	Type number of the lock		
	HardwareVers	Hardware version of the lock	Integer	
	BootloaderVers	Bootloader version of the lock	Integer	
	FirmwareVers	Firmware version of the lock	Integer	
	LockEngineVers	Version of the lock logic	Integer	
	Internal	Internal data for service purposes		
	Antenna matching	Antenna calibration	Integer	
	CNT Activation	Number of button actuations since resetting the counter	Integer	
	CNT Locking	Number of valid locks (with data carrier or PIN) since resetting the counter	Integer	
	CNT Activation ABS	Total number of button actuations	Integer	
	CNT Locking ABS	Total number of locks (with data carrier or PIN)	Integer	
	Temp. int.	Temperature in the GL7p in °C	Integer	
	BV	Information for service technicians		
	TL	Information for service technicians		
	MC	Information for service technicians		

	BM	Information for service technicians		
ReaderChip				
	FW	Firmware of the RFID reader electronics		
	Telemetry	Status information about the operation of the GL7p		
	Duration Locked [min.]	Counter that shows how long the GL7p was locked (in minutes)	Integer	
	CNT activations last locking	Number of presses of the button since the last locking of the GL7p	Integer	
	CNT door released while locking	Number of cancelled closing operations	Integer	
	CNT write on card failed 1	Number of write errors to data carriers, first attempt	Integer	
	CNT write on card failed 2	Number of write errors to data carriers, second attempt	Integer	
	CNT write on card failed card removed	Number of write errors to data carriers because the data carrier was removed too soon from the reading field	Integer	
	BLE			
	FW	Firmware of the wireless interface electronics		
BatteryMgt				
	Settings			
	Batt Idle MA	Information for service technicians	Integer	
	Batt Idle	Information for service technicians	Integer	

***Table 5.1** – Configuration settings for the GL7p in GAT Config Manager*

6   OPERATION

RF exposure statement

The users must keep at least 20 cm separation distance from the device, except during the identification and operation process at the device (e.g. PIN-code input), which must be performed as described in this manual.

6.1   Target Group

This chapter contains information for the technicians who commission the GL7p and who check it in case of operation problems.

6.2   General

To operate the GL7p (e.g., to lock or unlock a locker), the user must identify themselves at the GL7p with their RFID data carrier or PIN code.

For identification via RFID data carrier, the button must be pressed in with the data carrier. Pressing the button activates the GL7p and the data carrier is read.
For identification via PIN code, the PIN code must be entered in order to lock or unlock the locker. After entering the PIN code, it is confirmed with the "✓" key or by pressing the push button. An RFID data carrier is then not necessary. The length of the PIN code is configurable. So that the personal PIN codes remain protected, the PIN codes entered are not recorded in the lock bookings and cannot be read.

ℹ️ *To save battery power, the GL7p is deactivated in its normal state. For this reason, the electronics must be activated before identification or operation can occur using a data carrier, which is done by pressing the button completely in or by pressing one of the keypad buttons.*

An LED display and audible buzzer indicate the operational states and provide feedback on user interaction.

6.3   Operating Modes

The GL7p can operate in "free locker" mode or "personal locker" mode. In free locker mode, the user can choose any unoccupied locker they want to use. In personal locker mode, the user is assigned a specific locker and only they have access to use the locker.

When free lockers and personal lockers are used together in one system, it is recommended that the locker numbers are unique for both functions. This means that the same locker number should not be used for both a personal locker and a free locker.

The following operating modes are possible:
"Free Locker" Operating Mode
- Free locker selection with or without duration of use function (default)
  NOTE! The duration of use function for free locker mode is only available for MIFARE systems.
- Free locker universal
- Free locker unique number

Gantner

<u>"Personal Locker" Operating Mode</u>
- Personal locker programming card
- Personal locker expiry date

<u>Requirements for MIFARE, ISO 15693, and HID iClass data carriers</u>

All MIFARE and ISO 15693 data carriers that are used in the system must meet the operating mode requirements as specified in the following table.

Operating Mode	Requirements for Data Carriers
Free locker	Data carriers must be coded accordingly
Free locker universal	The locker segment must be unused (encoded with all zeros) and the access keys must be correct
Free locker unique number	All MIFARE, ISO 15693, and HID iClass data carriers are possible
Personal locker programming card	All MIFARE, ISO 15693, and HID iClass data carriers are possible
Personal locker expiry date	Data carrier must be coded accordingly

Figure 6.1 – *Requirements for data carriers*

6.3.1 Free Locker Mode (with or without Duration of Use Function)

In free locker mode, the user has the option of selecting a free locker and locking it using their data carrier. After the locker has been locked, the user cannot occupy any additional lockers within the same locker group. Only once the original locker has been unlocked can the user lock another locker in the locker group.

Locker groups are used to organize the locks within a system into certain functional blocks, e.g., changing room lockers, safe-deposit boxes, etc. Different sector numbers are used on the data carriers to distinguish between the locker groups, which allows two or more lockers from different groups to be used with the same data carrier, depending on the data carrier storage space.

For data carriers that are configured with an expiry date, the date is checked by the GL7p. If the date has passed, the locker cannot be used.

NOTE! The GL7p does not automatically adjust to summer/winter time changes. This must be considered when defining the validity or expiry date.

<u>Locking and unlocking lockers with a data carrier</u>
► Close the locker door.
► Press the button of the GL7p in using a data carrier for approximately 1 second.
  o The information on the data carrier is read.
  a) Valid data carrier: The LED flashes blue briefly and then green and the action (lock/unlock) is carried out.
  b) Invalid data carrier: The LED flashes blue briefly and then red and the GL7p switches off without completing the locking action. Possible reasons for this include:
    - Another locker has already been locked using the data carrier. In this case, the first locker must be unlocked before the data carrier can be used with the new locker.
► When locking the locker, check that it is locked by pulling the locker door.

Gantner

Locking and unlocking lockers with a PIN code

► Close the locker door.

► Enter your PIN code.

NOTE: The length of the PIN code can be defined in the configuration.

► Press the OK button (√) or the button of the GL7p to confirm the PIN code.

   o   The PIN code is checked.

   a) Valid PIN code: The LED flashes green briefly and the action (lock/unlock) is carried out.

   b) Invalid PIN code: The LED flashes red briefly and the GL7p switches off without completing the locking action.

► When locking the locker, check that it is locked by pulling the locker door.

Duration of Use Function

Free locker mode also offers the possibility to define a duration of use for each locker. If a locker with this function is locked with a data carrier, the current time is written onto the data carrier and the time subsequently checked when the user attempts to open the locker again. With PIN code entry, this function is also possible. The timer resets after a new PIN code has been entered.

The locker can be locked/unlocked as often as required during the duration of use period. If the duration of use period is exceeded, the data carrier can no longer unlock the locker. In this case, the user must recode their data carrier at a central station, e.g., at a GAT Info or GT7 Terminal.

NOTE! The data carriers must be coded accordingly for the duration of use function (the corresponding config bits on the data carrier must be set). The GL7p must also be configured for the function (see section "5.4.4. Duration of Use "). There are two configuration modes for the function:

- Absolute duration of use ("Duration" function)
  In this mode, a usage period (depending on the "Time limit" parameter in minutes or hours, see "5.4.10 Configuration Settings Table") is configured. After locking a locker, the user must unlock the locker again within the defined period. The period begins from when the locker was first locked.
  Example:
  The time is set to 360 minutes. If the locker is locked at 17:00, it can be unlocked until 23:00. If the locker is locked at 21:00, it can be unlocked until 03:00 of the next day. The duration of use time is reset after the locker remains open for 60 minutes.

- Use up to a specific time after midnight ("Point of time" function)
  In this mode, a time is configured up to which the locker can be used every day. After locking a locker, the locker must be unlocked before the defined time. The usage period starts from the configured time after midnight.
  Example:
  The time is set to 120 minutes. As the calculation begins at midnight, the locker can be used until 02:00 the following day regardless of when the locker was locked. If the locker is locked, e.g., at 01:00, it can be unlocked until 02:00 of the following day. If the locker remains locked past this time, the data carrier can no longer unlock the locker. In this case, the user must release the data carrier at a central station.

Locking and unlocking lockers with a data carrier

► Close the locker door.

► Press the button of the GL7p in using a data carrier for approximately 1 second.

   o The information on the data carrier is read.

a) Valid data carrier: The LED flashes blue briefly and then green and the action (lock/unlock) is carried out. The time on the data carrier is checked and the current time written onto the data carrier.

b) Invalid data carrier: The LED flashes blue briefly and then red and the GL7p switches off without completing the locking action. Possible reasons for this include:

   - Another locker has already been locked using the data carrier. In this case, the first locker must be unlocked before the data carrier can be used with the new locker.

   - The duration of use period has been exceeded and the locker cannot be opened anymore. In this case, the data carrier must be reset at a central station.

► When locking the locker, check that it is locked by pulling the locker door.

6.3.2 Free Locker Universal Mode

The "Free locker universal" operating mode differs from the standard free locker mode in the following ways:
- Free locker universal mode allows the use of data carriers that are also used for other applications.
- No validity date with free locker universal mode.
- It is not possible to use a duration of use time with free locker universal mode.
- The following requirements for the data carriers apply:
   1. The locker segment must be unused and "empty", i.e., coded with all zeros.
   2. The Access Keys must be correct.

Locking and unlocking lockers with a data carrier

► Close the locker door.

► Press the button of the GL7p in using a data carrier for approximately 1 second.

   o The information on the data carrier is read.

a) Valid data carrier: The LED flashes blue briefly and then green and the action (lock/unlock) is carried out.

b) Invalid data carrier: The LED flashes blue briefly and then red and the GL7p switches off without completing the locking action.

► When locking the locker, check that it is locked by pulling the locker door.

Locking and unlocking lockers with a PIN code

► Close the locker door.

► Enter your PIN code.

   NOTE: The length of the PIN code can be defined in the configuration.

► Press the OK button (√) or the button of the GL7p to confirm the PIN code.

   o The PIN code is checked.

a) Valid PIN code: The LED flashes green briefly and the action (lock/unlock) is carried out.

b) Invalid PIN code: The LED flashes red briefly and the GL7p switches off without completing the locking action.

► When locking the locker, check that it is locked by pulling the locker door.

6.3.3 Free Locker Unique Number Mode

"Free locker unique number" operating mode differs from the standard free locker mode in the following ways:
- All MIFARE and ISO 15693 data carriers can operate with the lock.
- The data carrier can have a GANTNER locker segment, however the segment is not used for this mode.
- When a locker is locked with a data carrier, the locker number is not written onto the data carrier.
- Every data carrier can use (lock) any number of lockers at the same time.

Locking and unlocking lockers with a data carrier
► Close the locker door.
► Press the button of the GL7p in using a data carrier for approximately 1 second.
  o The information on the data carrier is read.
  a) Valid data carrier: The LED flashes blue briefly and then green and the action (lock/unlock) is carried out.
  b) Invalid data carrier: The LED flashes blue briefly and then red and the GL7p switches off without completing the locking action.
► When locking the locker, check that it is locked by pulling the locker door.

Locking and unlocking lockers with a PIN code
► Close the locker door.
► Enter your PIN code.
  NOTE: The length of the PIN code can be defined in the configuration.
► Press the OK button (✓) or the button of the GL7p to confirm the PIN code.
  o The PIN code is checked.
  a) Valid PIN code: The LED flashes green briefly and the action (lock/unlock) is carried out.
  b) Invalid PIN code: The LED flashes red briefly and the GL7p switches off without completing the locking action.
► When locking the locker, check that it is locked by pulling the locker door.

6.3.4 Personal Locker Programming Card Mode

For lockers operating in "personal locker programming card" mode, up to 32 data carriers and/or 32 PIN codes per GL7p can be authorized for use. These 32 data carriers and/or 32 PIN codes can be used with the locker as often as required and share the same authorization access, e.g., for use as family cards.
The data carriers are authorized for use with the personal locker using the PROGRAM data carrier (included in the GAT ECO.Basic Set, see section "6.4 GAT ECO.Basic Set FD").

Authorizing data carriers

► Close the locker door.

► Press the button of the GL7p in using the PROGRAM data carrier for approximately 1 second.

    o   The information on the data carrier is read and the LED flashes green briefly.

► The GL7p enters into programming mode.

    o   The LED flashes red until the PROGRAM data carrier is removed. As soon as the PROGRAM data carrier has been removed, the LED flashes red/green and the lock is ready to program data carriers.

► Within 5 seconds, hold the data carrier being authorized in front of the GL7p button (the button does not need to be pressed).

   a) Successful authorization: The LED flashes green for approximately 3 seconds. When the data carrier is removed, the LED flashes red/green alternately again and another data carrier can be authorized in the same way. Repeat this process until all the data carriers are authorized.

   b) Unsuccessful authorization: The LED flashes red and the GL7p switches off. Possible reasons for this include:

    - The maximum of 32 data carriers are already authorized in the GL7p.

    - The data carrier could not be read correctly, e.g., because the data carrier is damaged.

► You can repeat the last step using different data carriers to program these data carriers successively. To do this, each data carrier being authorized must be held in front of the GL7p button within 5 seconds after removing the previous data carrier. If you wait longer than 5 seconds, the reading process is terminated, and the read data carriers are saved in the lock.

Authorizing PIN codes

► Close the locker door.

► Press the button of the GL7p in using the PROGRAM data carrier for approximately 1 second.

    o   The information on the data carrier is read and the LED flashes green briefly.

► The GL7p enters into programming mode.

    o   The LED flashes red until the PROGRAM data carrier is removed. As soon as the PROGRAM data carrier has been removed, the LED flashes red/green and the lock is ready to program data carriers.

► Within 5 seconds, enter the PIN code being authorized and confirm with the OK key (✓) or by pressing the push button.

   a) Successful authorization: The LED flashes green for approximately 3 seconds. When the data carrier is removed, the LED flashes red/green alternately again and another PIN code can be authorized in the same way. Repeat this process until all the PIN codes are authorized.

   b) Unsuccessful authorization: The LED flashes red 3 times and the GL7p switches off. Possible reasons for this include:

    - The maximum of 32 PIN codes are already authorized in the GL7p.

    - The PIN code was not correctly entered, e.g., the PIN code was too short or too long or an invalid PIN code was entered.

Gantner

► You can repeat the last step using different PIN codes to program these successively. To do this, the PIN code must be entered within 5 seconds after confirming the previous PIN code. If you wait longer than 5 seconds, the reading process is terminated, and the PIN codes are saved in the lock.

Deleting data carriers or PIN codes (= removing authorization)

It is only possible to delete all authorizations in the GL7p at once.
► Close the locker door and hold it shut.
► Press the button of the GL7p in using the PROGAM data carrier for approximately 1 second.
  o The information on the data carrier is read and the LED flashes green briefly.
► The GL7p enters into programming mode.
  o The LED flashes red until the PROGRAM data carrier is removed. As soon as the PROGRAM data carrier has been removed, the LED flashes red/green and the lock is ready for the next step.
► Within 5 seconds, press the button of the GL7p in using the PROGRAM data carrier for approximately 1 second.
► When the action is successful, the LED flashes red 3 times and 2 beeps are emitted. The GL7p then switches off.
  o All data carriers and PIN codes are now deleted from the GL7p and no longer have the authorization to use the locker.

6.3.5 Personal Locker Expiry Date Mode

During check-in, the user receives a data carrier encoded with GANTNER data blocks. The FID is written onto the "general" data block and the user's personal locker number together with the expiry date ("valid from" and "valid to") are written onto the "locker" data block of the data carrier. Furthermore, an index value is written onto the "locker" data block. The "valid from" date must always be valid, i.e., newer or equal to the data set in the GL7p.

This mode is only possible with RFID data carriers and not with PIN code entry, since the PIN codes cannot be used to save a validity date.

Upon first use of a locker, the expiry date ("valid to" date) and the current index value of the data carrier are stored in the lock. The guest can lock and unlock the locker as required, starting from the "valid from" date and for as long as the expiry date is not reached or exceeded.

NOTE! The GL7p does not adjust to daylight saving time automatically. This must be considered when evaluating events and authorizing data carriers with an expiry date.

An unlimited number of data carriers (users) can use the same locker. The following conditions apply to the data carriers in this mode:

- The same locker number must be stored on the data carriers.
- The same expiry date must be stored on the data carriers.
- The same index value must be stored on the data carriers.

When one of the data carriers assigned to a user is used at the locker for the first time, the expiry date and the index value of the data carrier are transferred to the GL7p.

Locking and unlocking lockers

► Close the locker door.

► Press the button of the GL7p in using the data carrier for approximately 1 second.

   o The information on the data carrier is read. The locker number on the data carrier must correspond with the locker number in the lock.

► The following situations are possible. The data carrier ...

   1) … is the first data carrier used at the locker:
      o The index value and the "valid to" date of the data carrier are saved in the lock. The data carrier can lock and unlock the locker until the end of the validity period.

   2) …has the same index value and "valid to" date as stored in the lock:
      o The data carrier is now authorized to lock and unlock the locker like the previously authorized data carriers.

   3) …has a higher index value than in the lock:
      o The new index value and the "valid to" date of the data carrier are saved in the lock. The data carriers previously authorized in the lock lose their validity, i.e., they are no longer authorized to use the locker.

   4) …has the same index value and a newer "valid to" date than in the lock:
      o The index value and the new "valid to" date of the data carrier are saved in the lock. The data carriers previously authorized in the lock lose their validity, i.e., they are no longer authorized to use the locker.

NOTE! Situation 2) is possible when the locker is locked or unlocked. Situations 3) and 4) are possible with a locked or unlocked locker except when the "PersonalLockerSecureFlag" option is set (see "5.4.10 Configuration Settings Table"). With this option set, the procedure is only possible with an open (unlocked) locker.

► Release the locker door.

   a) Valid data carriers: The locker state will switch, i.e., the locker will open when it was locked or will lock when it was open.

   b) Invalid data carriers: The LED flashes red briefly and the GL7p switches off without carrying out an action.

There is also no unlimited usage period for the locker, i.e., the expiry date must be a valid date (not "0"). If the "valid to" date is exceeded, the locker can no longer be opened using the data carrier except when the "LastOpenAtExpiredDate" option is set (see "5.4.10 Configuration Settings Table"). With this option set, the locker can be opened one more time using the data carrier.

6.4 GAT ECO.Basic Set FD

The following items are included in the GAT ECO.Basic Set FD (Part No. 1100550).

System data carriers:
- MASTER data carrier (3 pieces, red)
- DELETE MASTER data carrier (orange)
- PROGRAM data carrier (black)
- BATTERY data carrier (blue)
- SERVICE data carrier (yellow)
- APP KEY data carrier (purple)

Additional items:
- 3 m USB programming cable
- GANTNER USB stick with configuration software
- GANTNER lanyard
- Battery compartment key "GL7p Battery CoverKey"

Additional items (not required for the GL7p):
- Battery compartment key "GAT ECO.Lock 7000 - Battery Key GEA" (only for the GAT ECO.Lock 7xxx)
- Emergency power adapter "GAT ECO.EPS 7000" (only for the GAT ECO.Lock 7xxx and GAT Side.Lock 7xxx)

Optional data carriers:
- OPEN MASTER data carrier
- BLOCKING data carrier

6.5 Summary of System Data Carriers

The data carriers included in the GAT ECO.Basic Set are required to configure and maintain a GL7p equipped locker system.

> **i** *The system data carriers are coded to function with specific installations and will only function with the respective system.*

6.5.1 MASTER Data Carrier

With a MASTER data carrier, all locks in a system can be unlocked and locked. If a user's data carrier is lost, an emergency opening of the corresponding locker can be carried out using a MASTER data carrier. Three MASTER data carriers are included in the basic set and they are only valid for the respective system.

NOTE! The system operator must ensure that the MASTER data carriers are stored in a safe and secure location.

If a MASTER data carrier is lost, a new MASTER data carrier can be ordered from GANTNER Electronic GmbH. Before the new MASTER data carrier is used, the original MASTER data carriers must be deleted from the GL7p (the number of a MASTER data carrier is stored in the lock the first time the MASTER data carrier is used). This is carried out using the DELETE MASTER data carrier. Complete the following procedure:

► Press the locker door shut.

► Press the button of the GL7p in using the DELETE MASTER data carrier for approximately 1 second.

    o The information on the data carrier is read and the LED flashes red until the DELETE MASTER data carrier is removed.

► Remove the DELETE MASTER data carrier from the button.

    o All MASTER data carriers are now deleted from the lock. Next, the LED flashes green and red alternately and the new MASTER data carriers can be programmed.

► Within 5 seconds, press the button of the GL7p in using the first MASTER data carrier for approximately 1 second.

    o When the data carrier is read correctly, the LED flashes green for 2 seconds.

► Remove the MASTER data carrier from the button.

    o The LED flashes green and red alternately. The second MASTER data carrier can now be programmed.

► Repeat the process until all MASTER data carriers are programmed.

► If no action occurs after 5 seconds during programming of the MASTER data carriers, the GL7p automatically returns to the normal operating mode and the new MASTER data carriers are saved in the lock.

6.5.2 OPEN MASTER Data Carrier (Optional Accessory)

The OPEN MASTER data carriers can unlock any GL7p in a system. If a user's data carrier is lost, an emergency opening of the corresponding locker can be carried out using an OPEN MASTER data carrier. Compared to the MASTER data carrier, the OPEN MASTER data carrier cannot lock the locker after it has been opened.
The OPEN MASTER data carrier is not included in the Basic Set and must be ordered separately as required. This data carrier is only valid for the respective system.

NOTE! The system operator must ensure that the OPEN MASTER data carriers are stored in a safe location that is secured against unauthorized access.

An OPEN MASTER data carrier can be used instead of an original MASTER data carrier. To program the OPEN MASTER data carrier into a lock, read the data carrier at the lock. If already the max. amount of MASTER data carriers (10) are programmed into the lock, the MASTER data carriers must first be deleted and the OPEN MASTER data carrier must be programmed together with the required MASTER data carriers (max. total amount of 10).

6.5.3 DELETE MASTER Data Carrier

The DELETE MASTER data carrier is used to delete all the MASTER data carriers stored in the GL7p. See section "6.5.1. MASTER Data Carrier".

6.5.4 PROGRAM Data Carrier

For locks operating in personal locker mode, the PROGRAM data carrier is used to authorize data carriers so that they can be used with the locker. The PROGRAM data carrier is also used to delete the existing authorizations of personal lockers. See section "6.3.4 Personal Locker Programming Card Mode".

6.5.5   BATTERY Data Carrier

After the batteries are replaced in the GL7p, the lock must be set back to the normal operating mode using the BATTERY data carrier. The internal action counter is reset to zero when the BATTERY data carrier is used. See section "4.2.3. Replacing the Battery" for more information.

i *After replacing the battery of a GL7p in personal locker mode, all settings stored in the lock remain as previously configured.*

6.5.6   SERVICE Data Carrier

The SERVICE data carrier is used to put the GL7p into configuration mode after the lock is connected to a computer via USB (see section "4.3 USB Connection"). The settings of the GL7p are configured using GAT Config Manager while the lock is in configuration mode (see "6. CONFIGURATION").

When the GL7p reads the SERVICE data carrier without being connected to a PC via USB cable, an antenna calibration is performed, which locks the lock for a few seconds. After locking, the LED flashes red and the SERVICE data carrier must be removed. The antenna is calibrated and the LED flashes green. Finally, a green LED and a beep are emitted to indicate that the antenna calibration has been completed successfully. The locker is then unlocked if it was locked before the calibration.

NOTE! The SERVICE data carrier must be available for service employees who are required to configure the locker system. Without the SERVICE data carrier, system configuration is not possible!

6.5.7   APP KEY Data Carrier

The APP KEY data carrier is required to configure the GL7p using the MoLA app. This app can be installed on mobile devices with an Android operating system. When the lock is in factory mode and configured for the first time, the APP KEY is not needed. For subsequent configuration changes however the APP KEY data carrier is required (see also "5.3. Configuration with the MoLA App").

i *To configure the GL7p with GAT Config Manager, the APP KEY data carrier is not required.*

6.5.8   BLOCKING Data Carrier (Optional Accessory)

This data carrier is used to block a locker which is locked by a user. After using the BLOCKING data carrier at the locker, the user cannot open the locker anymore. To open the locker, a MASTER data carrier must be used. The automatic open function will be disabled after the BLOCKING data carrier is used until the lock is opened with a MASTER or OPEN MASTER data carrier.

The BLOCKING data carrier is not included in the scope of supply but can be ordered as an accessory.

6.6 Summary of GL7p Signalization

The electronics of the GL7p are activated when the lock button is pressed in. The activation is signaled by the LED at the top of the GL7p (LED flashes blue). Immediately thereafter, the following lock states are signaled via the same LED and the integrated beeper.

LED	Beeper	Meaning
Blue flash	-	Lock ready to read a data carrier
Red flash	-	- No authorization - Error
Green flash	-	- Data carrier accepted - Operation successful
Green flash	Ascending beeps	Battery replacement successfully completed; lock operating in normal operating mode again
Flashing red/green	-	Only in configuration mode; lock waiting to read a data carrier
5 x red flashes	5 x beeps	Battery change required
1 x brief white flash	1 x beep	Pressing of a PIN code key has been detected

Table 6.2 - *Summary of the LED and sound signals*

7 CLEANING AND MAINTENANCE

This chapter contains information for the cleaning personnel and service technicians responsible for the cleaning and maintenance of the GL7p locks and lockers.

ATTENTION! The instructions described in this chapter may only be carried out by suitably trained personnel. The warnings in this chapter must be observed and followed during functional testing, cleaning, and maintenance.

7.1 Cleaning

Regular cleaning of the locker components ensures that the locker system remains in good condition and the correct working order is maintained.

NOTE! Do not use cleaning benzene, diluents, or other abrasive detergents. In addition, the components must not be cleaned using a high-pressure or steam cleaner otherwise damage can occur!

Complete the following steps to clean the locker:
- ► Wipe off dirt and dust using a soft, lint-free, dry cloth.
- ► For extreme dirt, clean the locker components using a slightly moistened cloth. Do not allow any moisture to enter the inner parts of the GL7p.

7.2 Maintenance

The GL7p system components are maintenance-free, i.e., maintenance of the mechanical parts is not required. Should a malfunction be detected during functional testing that cannot be remedied, the corresponding faulty part(s) must be replaced.

7.3 Functional Testing

To ensure that the locker locks are functioning correctly, periodically test the functionality of the locker doors and lock components.

Frequency
- After every 1000 locking operations, or,
- If the locking function of a locker door is impaired.

Instructions
- ► Close the locker door.
    - o The door must close shut without increased effort. Readjust the door (see below) if this does not happen.
- ► Lock the door. Depending on the type of lock (data carrier or PIN code), press the GL7p button in with a valid data carrier or enter a valid PIN code when the door is closed.
    - o The locker door must lock. If it does not, check that the data carrier authorization is valid.

► Unlock the door. Depending on the type of lock (data carrier or PIN code), press the GL7p button in with a valid data carrier or enter a valid PIN code when the door is locked.

  o The locker door unlocks and must open without resistance. If the door or latch jams, re-adjust the door or latch (see below).

  o If the data carrier was not read, the RFID reading field may be misaligned and the range too small. In this case, recalibrate the reading field by reading the SERVICE data carrier (see "6.5.6. SERVICE Data Carrier").

► Check that the latch is firmly seated on the mounting thread.

Adjusting the locker door and door latch

If a problem, as described previously in "Instructions", occurs while opening or closing the locker door during functional testing:

► Adjust the position of the locker door using the dimensions in sections "3.8 Installation of the GL7p" and "8.9 Dimensions".

► If the door does not adjust properly, mount it in a different position.

► If the door is damaged, replace the door with a new door.

► Ensure that the correct latch is installed so that it sits exactly against the stop on the locker wall when the door closed and keeps the door closed without any play. See sections "3.8 Installation of the GL7p" and "8.9 Dimensions".

► If the supplied standard latch does not suit the locker wall (e.g., when retrofitting), a corresponding offset latch can be ordered. The standard latch must not be bent or modified in any way.

► If the latch is damaged, it must be replaced.

7.4 Disposal

- Do not dispose of the GL7p and the associated components with the normal household waste, but rather at your local electronic waste recycling facility in accordance with European Directive 2002/96/EC.

- Recycle defective or used batteries according to European Directive 2006/66/EC.

- Observe local regulations for the separate disposal of batteries.

- Recycle packaging in an environmentally friendly manner.

8 TECHNICAL DATA

8.1 Power Supply

Power supply:	1 x 3.6 V lithium battery, type AA, capacity 2.4 Ah
GANTNER approved battery:	- Tadiran SL-860/S - Tadiran TL-4903/S (alternative)
Battery lifespan:	Up to 10 years* with 10 operations per day and +20 °C * depending on usage, configuration and ambient conditions

8.2 Reading Field

Reader type:	MIFARE® supported types:
	  - MIFARE® Classic (1k and 4k)
	  - MIFARE Ultralight®
	  - DESFire EV1® and EV2®
	  - NFC (HCE)
	 - ISO 15693
	 - HID iCLASS UID (13.56 MHz)
	
	Note: It is recommended to have customer-specific data carriers approved by GANTNER before use.

Reading field frequency:	- RFID: 13.56 MHz - Wireless interface: 2.4 GHz
Maximum transmission power:	- RFID: < 500 mW - Wireless interface: 3.7 dBm (2.344 mW)
Reading field range:	5 to 35 mm* (0.2´´ to 1.38´´)* * depending on the installation and data carrier

8.3 Memory and Time Management

Data storage:	EEPROM with capacity for 150 bookings, data retained during battery change
Internal clock:	Quartz-controlled, real-time clock

8.4 Control and Display Elements

Control element: Button

Display element: - LED (multi-colored) to display the different operational states
- Beeper

8.5 Mechanical

Locking: Mechanical with motorized latch lock

Break-in resistance: DIN 4547-2

8.6 Interface

Interface type: USB 2.0

Interface connection: USB type Micro-B

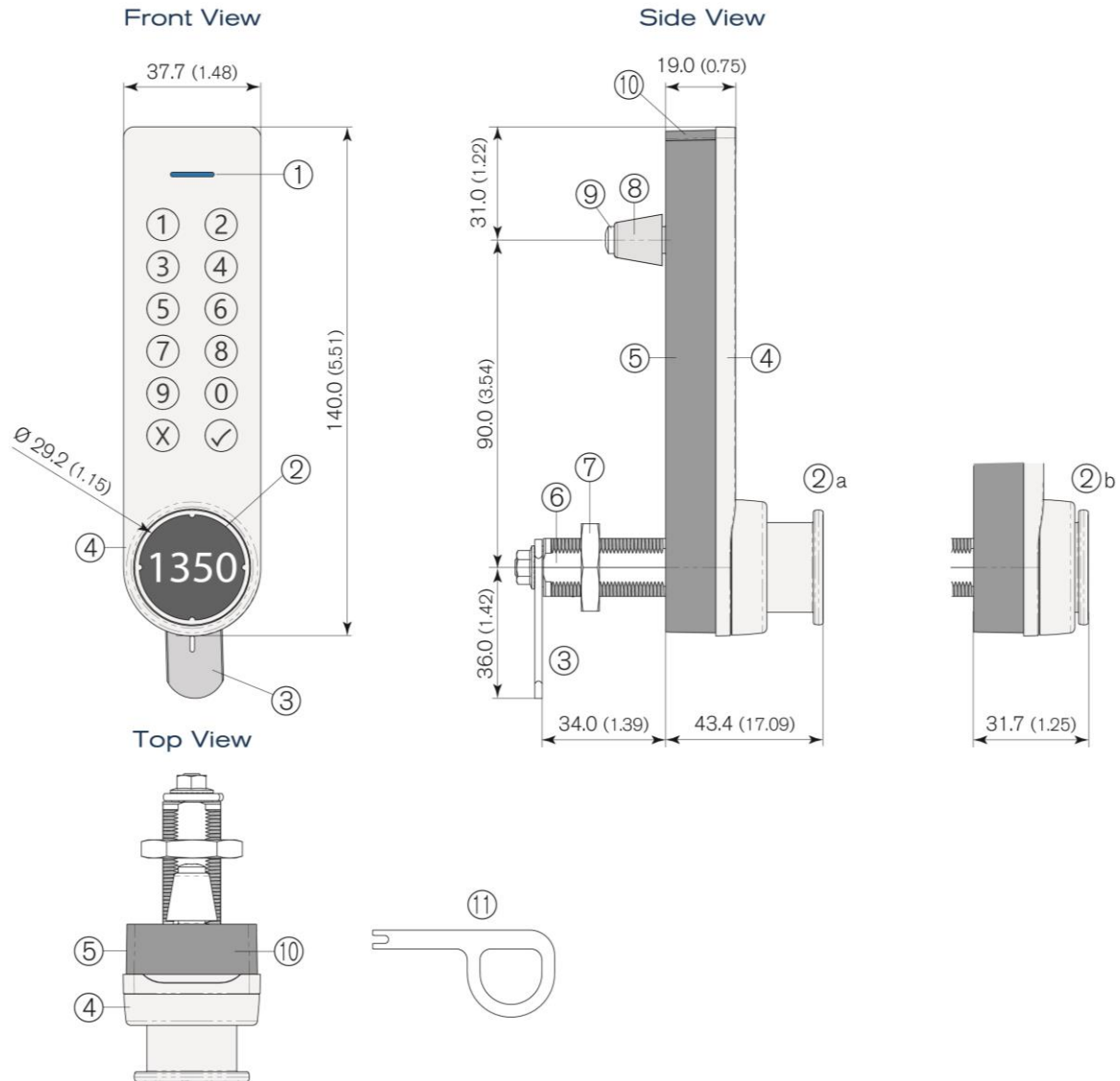**Wireless interface:** - NFC (13.56 MHz)
- Wireless (2.4 GHz)

8.7 Housing

Material: Plastic (PC), halogen-free, V0

Latch: Steel

Mounting thread: Die-cast zinc

Color: - Front part: white
- Rear part: dark gray

Weight: Approx. 250 g (8.82 oz.)

8.8 Environmental Conditions

Permitted ambient temperature: -20 to +60 °C (-4 to +140 °F)

Protection type: IP 42 (when installed)

Environment class (VdS 2110) II (conditions in indoor areas)

Compliances: CE, FCC, IC

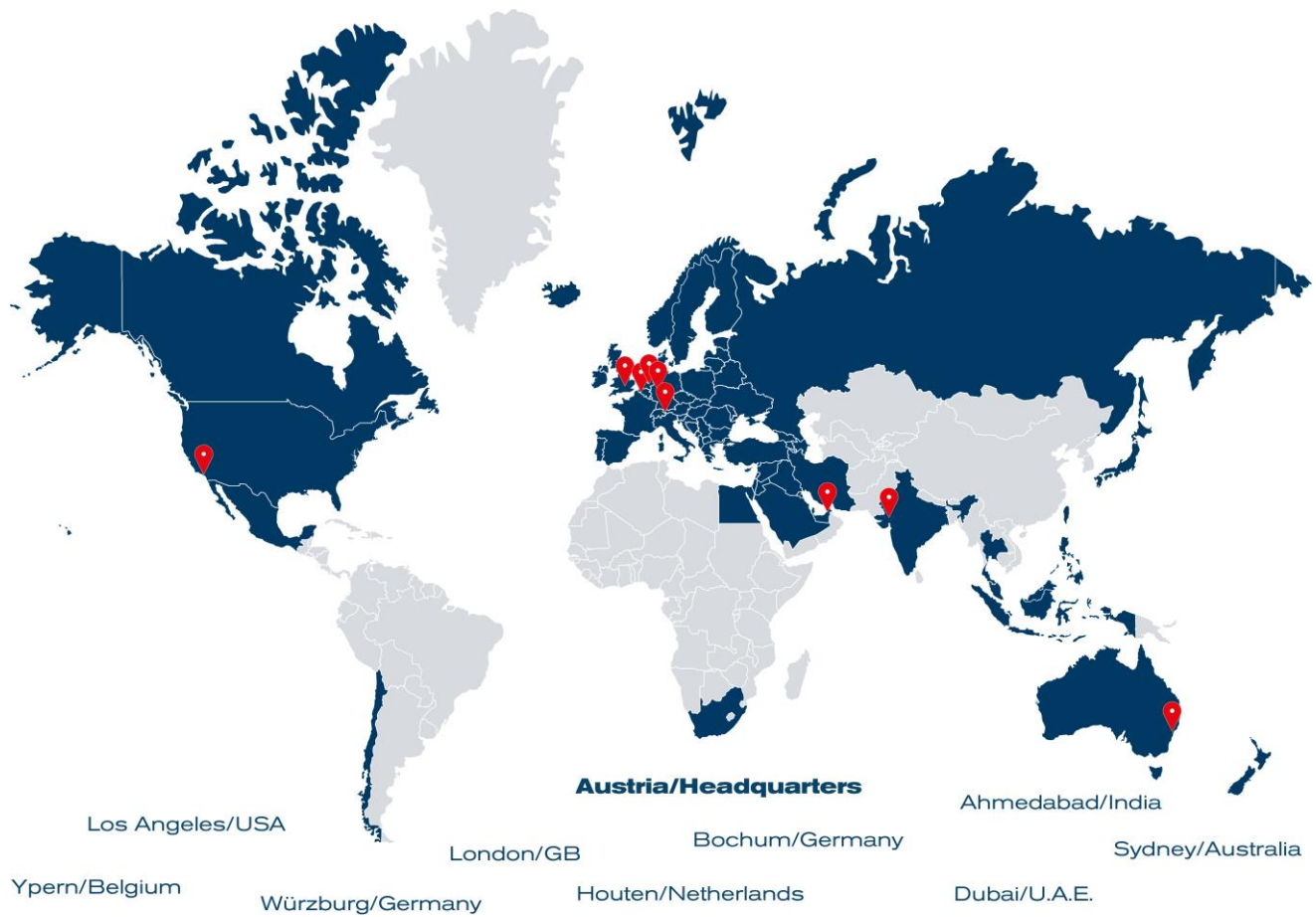**Availability:** The GL7p is not available in North America (United States, Canada)

Gantner

8.9 Dimensions

1. LED status indicator
2. Button (a = "unlocked", b = "locked")
3. Latch
4. Front part
5. Rear part
6. Mounting thread (M19x1)

7. Fixing nut
8. Spacer sleeve
9. Screw for anti-rotation protection
10. Battery compartment cover
11. Battery compartment key

Note:
This manual is valid as of 25th August 2020. It is subject to change.
Amendments can be made without prior notice at any time!

Los Angeles/USA
Ypern/Belgium
London/GB
Würzburg/Germany
Austria/Headquarters
Bochum/Germany
Houten/Netherlands
Ahmedabad/India
Dubai/U.A.E.
Sydney/Australia

GANTNER operates in over 60 countries worldwide. **Please visit www.gantner.com**

Nüziders, Austria
info@gantner.com

London, United Kingdom
info-uk@gantner.com

Ypern, Belgium
info@gantner.be

Houten, the Netherlands
info@gantner.nl

Bochum, Germany
info-de@gantner.com

Dubai, UAE
info-me@gantner.com

Sydney, Australia
info-aus@gantner.com

Los Angeles, USA
info-us@gantner.com

Ahmedabad, India
info@gantnerticketing.com

Current contact information: www.gantner.com/locations

www.gantner.com