Information security incident and event management

Annex 103-B to EasyGo Security Framework

This copy of the document was published on www.easygo.com and is for information purposes only. It may change without further notice.

Document: 103-B
Version: 1.0
Date: 16 June 2020

Table of contents

Document Revision History

Version	Date	Author	Main changes
1.0	16.06.2020	ESC	Approved by ESC on 16 June 2020

1 Scope

1.1 General

This public EasyGo security document covers the classification and handling of security incidents and security events and as such enhances the management aspects of information security in EasyGo.

1.2 Objectives

The aim of this document is to give the entities connected to the EasyGo HUB a rulebook, on whom to inform, if an information security incident occurs in their system.

This document does not deal with any public relations related measures or describes any detailed measures for the entity on how to react to an information security element. The handling of an information security incident is in the full responsibility of the entity, where it occurred.

1.3 Document contents

This document provides a list of information security incidents to consider and a description on whom to inform, if a listed information security incidents occurs.

The responsibility for the content of the document lies with the EasyGo security group. It may be updated, if new information security incidents are detected other information security incidents or no longer relevant.

2 Information security incidents

There are multitudes of information security incidents, which can occur in an IT system. An information security incident is basically categorized by the fact, that it is not a planned event.

There are multitudes of other incidents that can occur in an IT system, but are of an operational nature (e.g. outages). These operational incidents are not considered as information security incidents and are not covered by this document.

As the severity of information security incidents vary from a mere security nuisance to a legal issue, especially under the rules of the GDPR, or even a complete system outage connected to an information security incident, these incidents need to be clustered and categorized.

The EasyGo security group monitors the handling of information security incidents by all entities connected to the EasyGo HUB.

2.1 Class 1 information security incidents

Class 1 information security incidents affect all entities connected to the EasyGo HUB.

The following list describes the defined class 1 information security incidents:

- Data breach in EasyGo HUB – data made available to an non-intended entity
- Processing error in EasyGo HUB – processing of data in an abnormal way

2.2 Class 2 information security incidents

Class 2 information security incidents affect several entities connected to the EasyGo HUB.

The following list describes the defined class 2 information security incidents:

- Data breach in AutoPass HUB – data made available to an non-intended entity
- Processing error in AutoPass HUB – processing of data in an abnormal way
- Data breach at a TC – data made available to an non-intended entity
  - e.g. unwanted disclosure of personal data provided as contacts in the ACT
  - e.g. personal data (license plate, OBE) provided in the TIF belongs to another TSP
  - e.g. IT data breach by an external (hacker)
- Data breach at a TSP – data made available to an non-intended entity
  - e.g. unwanted disclosure of personal data provided as contacts in the ACT
  - e.g. personal data (license plate, OBE) provided in the NAT, HGV belongs to another TC
  - e.g. IT data breach by an external (hacker)
- Compromise of security keys at a TC or TSP

3 Information security events

There are multitudes of information security events, which can occur in an IT system. An information security event is basically categorized by the fact, that it can be planned in advance, which is the main difference from information security incidents. An information security event in the meaning of this document affects the EasyGo security documents.

There are multitudes of other events that can occur in an IT system, but are of an operational nature (e.g. maintenance windows). These operational events are not considered as information security events and are not covered by this document.

There is no legal responsibility under the GDPR to report information security events. But all entities connected to the EasyGo HUB are required to report all events, which may require a change to the EasyGo security documents to the EasyGo security group.

3.1 Class 1 information security events

Class 1 information security events may initiate a review of the EasyGo security documents in a broader sense, which could affect all entities connected to the EasyGo HUB.

The following list describes the defined class 1 information security event:

- Change of European legislation (e.g. GDPR, EETS directive …)
- Change of national legislation (e.g. national tolling regulations, change of tolling laws …)
- Change of security policy in EasyGo

3.2 Class 2 information security events

Class 2 information security event affect at least one security requirement/security measure combination listed in document 103-C, which requires a renewal of the EasyGo security compliance statement 103-C by the affected entity.

The following list describes the defined class 2 information security events:

- Planned update of EasyGo HUB
- Planned update of Autopass HUB
- Planned update of central system at a TC
- Planned update of central system at a TSP
- Planned exchange of RSE at a TC
- Planned introduction of new OBE at a TSP
- Connection of a new a TC
- Connection of a new a TSP

4 Handling of information security incidents

The handling of any information security incident lies at all times in the responsibility of the entity, where it occurred. All steps needed to limit the effects of an information security incident shall be taken by the affected entity in a way that the possible consequences or damages to other entities connected to the EasyGo HUB are kept to a minimum.

4.1 Initial information

If a **class 1 information security incident** occurs, the IT support contact of **all entities** contained in the actor table (ACT) and the EasyGo security group **shall be informed** by the entity, where it occurred, **within 24 hours of its detection**.

If a **class 2 information security incident** occurs, the IT support contact of **all affected entities** contained in the actor table (ACT) and the EasyGo security group **shall be informed** by the entity, where it occurred, **within 24 hours of its detection**.

These strict timelines are required, to allow possible other affected entities to keep their legal reporting obligation of 72 hours according to the GDPR.

The EasyGo security group will keep a record of all information security incidents that occurred.

4.2 Periodic updates

The entity, where an information security incident occurred, shall send a periodical **status update to each affected entity** and the EasyGo security group **at least every 48 hours** until it is solved.

4.3 Summary

The entity, where an information security incident occurred, **shall provide a summary** to each affected entity and the EasyGo security group containing at least:

- the reason for the information security incident
- the measures taken to minimize the effects and consequences for the affected entities
- a description of the affects to each connected entity (if any) and how to remove them
- a plan on how to prevent further information security events in the future

latest 5 working days after an information security event is solved.

4.4 Optimisation of the EasyGo documents

The EasyGo security group will analyse the provided information to identify any suitable optimisations to the EasyGo security framework or technical documents. It will deliver a report to the EasyGo steering committee and update the EasyGo security framework accordingly. The update of other EasyGo documents will be handled by EasyGo management.

5 Handling of information security events

The handling of any information security event lies at all times in the responsibility of the entity, where it is planned.

5.1 Advance information

Each entity shall inform the EasyGo security group as soon, as a decision is taken, which will lead to an information security event. The advance information should contain a description of the possible consequences for the EasyGo security framework.

5.2 Update of the EasyGo security compliance statement

If an information security event affects a security requirement or security measure, a new EasyGo security compliance statement shall be sent to the EasyGo security group indicating the changed security requirement or security measure before a planned change is implemented.

The entity shall provide suitable measures to rectify any non-conformance which possibly arises from the information security event in the updated EasyGo security compliance statement.

6 References

For dated references, subsequent amendments to or revisions of any of these publications apply only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

6.1 *Standards and external documents*

Reference	Document Ref	Date / Version	Document title

6.2 *European directives, decisions and regulations (legislative acts)*

Reference	Document Ref	Date / Version	Document title

6.3 *EasyGo documents)*

Reference	Document Ref	Date / Version	Document title
[EasyGo-103]	103		EasyGo security policy (public)
[EasyGo-103-C]	103-C		EasyGo security compliance statement (strictly confidential)