Letter of Authorisation – regular tests

v2020.1

Engagement Reference Penetration test COVID-19
Engagement Date 17 April 2020

EL Title **Letter of Authorisation penetration COVID-19 app**

Type of testing activities

In signing this Letter of Authorisation, _____ (hereafter to be referred to as Client) authorises KPMG Advisory N.V. (also known as KPMG IT Advisory, hereafter to be referred to as KPMG) to perform (a selection of) the following tests:

Testing activities
☒ external (internet) penetration test
☒ internal network penetration test
☒ vulnerability scan
☒ webapplication test
☐ hardware hacking (e.g. stolen equipment test)
☐ war-drive test (wifi hacking)

Short description of testing activities
Penetration testing activities on the COVID-19 applications for iOS and Android (where applicable) and the backend server and software, including automated vulnerability scanning and manual exploitation.

Contact information of all involved parties

This section contains all relevant contact information related to the activities.

KPMG testing team

#	Name	Function	Phone number	Email
1	5.1.2e	Coordination of tests, first point of contact	+31 5.1.2e	5.1.2e @kpmg.nl
2	5.1.2e	Engagement partner who is responsible for the overall conduct of the project	+31 5.1.2e	5.1.2e @kpmg.nl

Client directly involved employees

During the execution of the assignment, a contact person should be available who is capable of providing specific information on the infrastructure and who can be contacted in the case of problems and when the operational activities commence and finish.

Name	Function	Phone number	Email

Third party (e.g. hosting provider) involved employees

☐ (A part of) the IT objects in scope are outsourced to a third party. The contact information is in the overview as per below:

Name	Function	Phone number	Email

Scoping and operational limitations

This section contains all relevant information regarding the scope and the operational limitations related to the activities.

Objects included in the scope

The list of target IP addresses, hostnames, SSIDs and/ or locations are as follows:

IP Ranges Backend	FQDN or URL	Description	Physical location of target systems

Client representative (and, if applicable, the Third party) declares that it is legal owner or holder of the above specified targets and therefore has the authorisation to permit KPMG to perform the above specified test on these objects.

Objects out of scope

Unless specifically authorised to do so by the undersigned Client representative (and, if applicable, the Third party), KPMG agrees NOT to include the following objects in the tests:

IP Ranges Backend	FQDN or URL	Description	Physical location of target systems

Timing of our activities

Testing is allowed in the period from 17 April to 18 April. Valid timeslots for testing during this period are:

☒ during business hours (08:00 – 18:00 GMT +1)
☒ outside business hours and weekends

Rules of engagement

During a security test, procedures and mechanisms can be used that might (temporarily) reduce your overall system security. The checked techniques below are ALLOWED during our security test:

☐ Capturing of user credentials (e.g. user ID and passwords) and other data
☐ Taking screenshots, audio and camera recordings on Client's end user systems
☐ sniffing on the target network after access has been achieved
☐ installing Backdoors on the targets
☐ sending Trojans via email (or similar services)
☐ the use of (hardware or software) password and/or keyboard loggers on the targets
☐ perform system reconfiguration on the targets (which are sometimes needed to perform special attack types)
☐ Denial-of-Service attacks
☐ Other:.....

Generic terms and conditions

In authorising KPMG to perform the specified tests against Client's objects and/or persons, Client (and, if applicable, the Third party) acknowledges the following:

- If the tests concern an internet penetration test, that this will be performed from KPMG's Technology Center, using the IP ranges 217.100.97.152/29.
- If the tests concern a wardrive / wireless or physical security test, that the tests will be performed in and around the buildings of Client.

Dutch law requirements

In order to comply to requirements in criminal and civil law in The Netherlands, Client (and, if applicable, the Third party) acknowledges that KPMG uses, among others, the following techniques, and that Client (and, if applicable, the Third party) does not object to this:

- Technical operations, false signals, keys or identity to gain access to the client's automated systems.
- Copy and store data encountered on the client's automated systems.
- A public telecommunication infrastructure or system to use computing capacity of the client's automated systems.
- Process, transfer or change the data encountered on the client's automated systems and append data to it.

Client (and, if applicable, the Third party)also acknowledges that in performing security testing, KPMG may gain access to Client (and, if applicable, the Third party) information or other Client (and, if applicable, the Third party) automated systems than specified in the above list of target IP

addresses and/or hostnames, as a result of a successful penetration. Client (and, if applicable, the Third party) agrees that this is acceptable.

Client (and, if applicable, the Third party) further declares it shall indemnify and hold harmless KPMG and any company owned by, or affiliated with KPMG and their respective principals, employees and affiliates, against any damage, demands, liabilities and claims for personal injuries and/or property damage that may be caused by or ensue from the execution of the security test.

We would like to stress the fact that a penetration test cannot demonstrate or prove that a system is secure. A penetration test can only show the weaknesses and vulnerabilities at the moment of testing.

Secured method of communication

The security testing team may be handling some sensitive data such as vulnerability details and the final report which we may need to email to the Client point of contact. This information will be communicated using encryption, preferably (but not exclusively) an encrypted PDF. Any passwords will be communicated separately.

On behalf of Client		On behalf of (third party)	_____
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Function:	_____	Function:	_____
Date:	___-___-___	Date:	___-___-___