**INFORMATION ABOUT SPECIAL THREATS**

**CONNECTED WITH THE USE OF SERVICES**

**SUPPLIED ELECTRONICALLY**

**BY QZ SOLUTIONS SP. Z O.O.**

**VIA THE ZILLIN WEBSITE**

QZ Solutions Sp. z o.o., as a supplier of services supplied electronically via the Zillin Website, to fulfil its obligation under Art. 6.1 of the Electronically Supplied Services Act of 18 July 2002 (Journal of No 2002.144.1204, as amended), hereby informs you about special threats connected with the use of electronically supplied services by users.

This information applies to threats that can occur only potentially.

Major threats connected with the use of the Internet are among others:

* Malware, including: computer viruses, i.e. specific software which, once executed, can infect files so that they reproduce, making copies of themselves, usually without discovery by the user; viruses can cause varying degrees of damage to the host operating system and, at the very least, result in resources being wasted in terms of RAM, CPU and hard disk space.
* various types of applications or scripts that have a harmful, criminal or malicious impact on the user’s ICT system, like viruses, worms, trojans; the presence and operation of worms, i.e. self propagating malware; an email worm is a disruptive network attack that collects all email addresses from a local software and then sends hundreds of emails to those email addresses with the worm programme itself as an attachment;
* Spyware, which means software programmes that track a user's Internet surfing, which install themselves without informing the user and without their knowledge, authorisation or control;
* Spams: unsolicited and undesired electronic messages sent simultaneously to many recipients, often with advertising content;
* Phishing, i.e. gaining access to personal and confidential data (e.g. passwords) under false pretences by means of impersonating a respectful person or institution;
* Sniffing: forbidden tapping where a sniffer, i.e. a computer program, is used to catch and analyse data in the network. Such computer programs specialise in data collecting and analysing. A sniffer is a program used to tap and, if located in a proper place in the LAN network, it enables to monitor activities made in such a network. In this way, a hacker can access all private data;
* Hacking into the user’s ICT system by the use of hacker tools;
* Cryptoanalysis: ability to find weaknesses of a cryptographic system to hack in or pass it by.

To avoid the above threats, the user should install an antivirus program and a firewall in its computer and other electronic devices with Internet access. Such programs should be updated on an ongoing basis.