INFORMATION ON THREATS

This Information ("Information") on particular threats related to the use of services provided electronically by a limited liability company operating under Splentum limited liability company with registered office in Rzeszów, ul. Solarza 6/18, entered in the register of enterprises of the National Court Register (KRS) run by the District Court in Rzeszów, XII Economic Division, under KRS number 0000594413, NIP (Tax Identification Number) 8133710147, REGON (National Business Register Number) 362933748, e-mail address: kontakt@splentum.pl, ("Splentum"):

a. concerns all Internet portals ("Portals"), whose operator is Splentum, especially MRSO.PL portal, available at: www.mrso.pl and Splentum portal available at: www.splentum.pl;
b. is published by Splentum in line with the provision of Article 6 point 1 of the Act of 18th July 2002 on Providing Services Electronically (that is Journal of Laws from 2013, item 1422) in order to provide the Users an updated source of data on particular threats related to the use of services provided electronically by Splentum.

The information concerns threats considered to be potential threats by Splentum, therefore, they should be taken into account in Splentum opinion, in spite of the fact that Splentum uses systems protecting its infrastructure against unlawful influence of third persons.

Splentum lists the following potential threats:

1. the possibility of infringing the intellectual property rights, especially royalties, by their unauthorized use (including: copying) without the knowledge and/or consent of the authorized entity;
2. the possibility of installing software for using services provided through portals from sources other than those authorized by Splentum, which, in spite of attempts made by Splentum aimed at minimizing the possibility of providing software versions modified by third parties, may contain malicious software;
3. the possibility of obtaining unsolicited commercial information (spam) sent electronically;
4. the possibility of being exposed to harmful software (such as malware, Internet worms) in the net environment, spread by code replication;
5. the possibility of breaking security measures in order to obtain personal and confidential information and to steal one's identity, by sending false e-mail messages resembling authentic e-mail messages;
6. the possibility of finding weaknesses in the cryptographic system, thus enabling its breaking or passing by and, as a result, the possibility of obtaining personal and confidential information in order to steal one's identity;
7. the possibility of phishing by sending false e-mail messages, looking exactly the same as the authentic messages and, as a result, obtaining personal and confidential information about the User;
8. the possibility of illegal tapping consisting in using a computer software whose task is to intercept and analyze data flowing in the network (spyware).