Dear all,

First of all, I would like to thank you for the invitation to brief you on some of the core provisions of the Regulation 2016/679, the General Data Protection Regulation (GDPR), which entered into force in May 2016 and shall be applied as of the 25th of May 2018. In addition, I will suggest some steps that the controllers such as WARGAMING should take, in order to be fully prepared to implement the GDPR, on day one.

The GDPR replaces Directive 95/46/EC, the main EU data protection legislation, which has served us well for more than 20 years. While the data protection principles stipulated in this Directive, remain strong, globalization, technological advancements and the increasing cross – border flow of personal data called for the need for a new legislation.

As a rule, Regulations have immediate effect and do not need any national legislative measures for their implementation. However, the GDPR allows Member States a degree of flexibility on how to apply certain Articles. Therefore, my Office undertook the task of preparing a draft bill for the better and effective implementation of certain provisions of the GDPR. In addition, the GDPR provides that the Commission shall further regulate certain Articles by implementing or delegates Acts. Therefore, you should bear in mind, that we have a long way to go before this legislation is finalized. Nonetheless, this should not prevent WARGAMING from taking all necessary steps to be fully prepared to implement the GDPR on day one.

The GDPR has a dual purpose. Its philosophy is reflected in its title, which explains that the GDPR aims to protect natural persons from the processing of their personal data but, at the same time, it aims to ensure the free movement of these data.

The GDPR strengthens existing rights and obligations and introduces new, it promotes the principles of accountability and transparency, it strengthens the cooperation of Data Protection Authorities, the DPAs, in cross-border cases, where a number of persons is affected across several Member States and it establishes the one stop shop. According to the principle of accountability, WARGAMING should be in a position to demonstrate its compliance to the GDPR. The one stop shop stipulates that WARGAMING and every person in the EU, has the right to deal with and bring their case before one DPA.

In cross border cases there may be competent and interested DPAs but one DPA may act as a lead authority. The lead DPA shall be determined by specific criteria, such as the Member state of the main or only establishment of the controller or Member State where the alleged infringement of the GDPR took place. In cases where the involved DPAs cannot reach a consensus on how to deal with a

particular cross border case, the consistency mechanism in Chapter VII of the GDPR, shall be activated to ensure a consistent enforcement actions. The GDPR, arms DPAs with quite stringent enforcement powers. In certain cases, imposed administrative fines may be up to 20 million euro or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

WARGAMING operates in many Member States. Therefore, one of the first things it should do is to decide the Member State of its main establishment. Consequently, this will determine, the DPA with which WARGAMING will have to deal with. Subsequently, WARGAMING should review all its processing activities and ensure that these are aligned with the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation integrity and confidentiality and accountability, stipulated in Article 6 of the GDPR.

As a matter of fact, Article 30 obliges WARGAMING to maintain a record of its processing activities and update it when necessary. This record contains the same information that, under the existing legislation, WARGAMING has a blanket obligation to notify to the Commissioner. The GDPR provides that WARGAMING shall make this record available to the Commissioner, on request. WARGAMING should also review its privacy policy and adjust it, if necessary, in simple terms, comprehensible to children.

Every processing should have a legal basis. I assume that WARGAMING will rely, at large, on consent or, on the performance of a contract to which the data is party or in order to take steps at the request of the data subject prior to entering into a contract, set out in Articles 6(1)(a) and (b) of the GDPR, respectively. If the processing is based on consent, WARGAMING should ensure that this is given freely. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Special categories of personal data that may lead to discriminations, afford a higher level of protection. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation should be based on one of the conditions of Article 9.

We can safely assume that WARGAMING is an information society service offered directly to adults and children. Article 8 provides that when an information society service is based on consent, the processing shall be lawful if the child is at least 16 years old. For children below the age of 16, consent should be given by the

person holding parental responsibility. Member States may provide, by virtue of national law for a lower age, but not lower than 13 years. The European Data Protection Board, which is an independent body with legal personality, established by GDPR Article 28, composed by the heads of the national DPAs and the European Data Protection Supervisor, may, in due course, issue guidelines for the modalities of implementing Article 8.

WARGAMING should have mechanisms in place for the exercise of the data subjects rights referred to in Articles 13 to 22 and 34 of the GDPR. Some of these rights such as the right to receive information and the rights of access and rectification, are already provided for by the current legislation, but the GDPR provides more detailed provisions for their exercise. The right to erasure is elevated to the right to be forgotten and is aligned with the 2014 milestone ruling of the Court of Justice of the European Union, the CJEU, in the famous Google Spain case. As a rule, what is uploaded on the web stays on the web. However, there are several technical ways for remedying this. For example, if it is not possible to delete publicly available information from its source, according to the Google Spain CJEU ruling, links to the source may be removed from search engines' lists of results. The right to be forgotten can be exercised only if certain grounds apply such as the withdrawal of consent, the exercise of objection and unlawful processing.

Particular attention should also be given to novel rights such as data portability, the data subject's right not to be subject to a decision based solely on automated processing, including profiling and data breach notification. Article 23 provides that Member States may restrict, by virtue of national laws, the exercise of the above mentioned rights and obligations. We have included some restrictions into the draft bill for the better and effective implementation of the GDPR, but we wish to discuss them with the Commission before we consult with interested stakeholders, both in the public and the private sector.

Chapter IV of the GDPR is devoted to the obligations of controllers and processors. Particular attention should be given to data protection by default and by design, set out in Article 25, which obliges WARGAMING to implement appropriate technical and organisational measures, such as pseudonymisation, and data minimisation, both at the time of the determination of the means for processing and at the time of the processing itself, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons. If addition, if WARGAMING assigns or outsources some processing activities to external contractors, the processors, particular attention, should be devoted to Article 28, which governs the relation between WARGAMING and contractors, in their respective capacity as controller and processors.

Other Articles of Chapter IV of the GDPR, oblige WARGAMING to keep the records of processing activities, already mentioned, to cooperate with the supervisory authority, to carry out data protection impact assessments, in particular when considering new technologies and to consult the Commissioner when an impact assessment indicates that the processing would result in a high risk in the absence of measures taken by WARGAMING to mitigate the risks for the data subjects. DPAs shall adopt and publish a list of processing operations that require an impact assessment and may adopt and publish a list of operations that do not require one.

If the core activities of WARGAMING consist of processing operations which, by virtue of their nature, scope and/ or purpose, require regular and systematic monitoring of its customers on a large scale, according to Article 37, WAGAMING is obliged to designate a Data Protection Officer, the DPO. The position and tasks of the DPO are regulated by Articles 38 and 39, respectively. It should be noted that the role of the DPO is advisory and he acts as a liaison with data subjects and the supervisory authority. It should also be noted that all the legal responsibilities stemming from the GDPR burden the controller, in this case WARGAMING as a controller and not the DPO.

The Article 29 Working Party, which shall be replaced by the European Data Protection Board, has already issued guidelines for data portability, data protection impact assessments, data protection officers and lead authorities and soon will issue additional guidelines for consent, profiling and data breach notifications. You are strongly advised to thoroughly study these guidelines and to regularly check my Office's website for updates. All the guidelines will be reviewed soon after the establishment of the European Data Protection Board, which shall replace the Article 29 Working Party.

Article 40 and 41 regulate the codes of conduct and their monitoring. Adherence to a code of conduct may not be mandatory but they can be adhered to by controllers or processors established in third countries that are not subject to the GDPR in order to provide appropriate safeguards for the transfer of personal data from the EU to them, in line with Article 46(2)(e). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects. The same applies to certifications, data protection seals and marks. Adherence to such certifications seals and marks is voluntary but they can be used as toolkit for demonstrating compliance with the GDPR or for the transfer of data to third countries, in line with GDPR Article 46(2)(f).

If WARGAMING transfers data to controllers or processors established in third countries, particular attention should be given to Chapter V of the GDPR. Such transfers can be carried out on the basis of an adequacy decision where the Commission that a country, a territory or a sector therein ensures an adequate

level of protection. Such a transfer does not require a prior authorization. In the absence of an adequacy decision, transfers can be carried out on the basis of appropriate safeguards such as standard contractual clauses approved by the Commission or the DPA, binding corporate rules, approved codes of conduct or approved certification mechanisms with enforceable commitments. Alternatively, for specific situations, transfers may be carried out on the basis of the derogations set out in Article 49 of the GDPR that may rely, inter alia, on consent, performance or conclusion of a contract and the exercise of legal claims.

As I have explained at the beginning of my speech, we have a long way to go before this legislation is finalized since there is an ample number of Articles that allows MS to implement national legislative measures and an additional number of Articles shall by further regulated by the Commission by means of implementing or delegated Acts. I hope that with this brief presentation, I have managed to convey to you some core provisions of the GDPR and how WARGAMING should prepare to implement it and demonstrate its compliance.

I was also asked to comment on how my Office prepares to enforce the GDPR on day one. At EU level, we closely monitor all discussions in the frame of the Article 29 Working Party and we contribute, to the extent of our resources, to the drafting of Guidelines and we liaise with other DPAs in tackling cases of common concern. At national level, we have carried out an internal training of our staff to ensure that everyone has a common understanding of the provisions of the GDPR and I have given a great number of presentations, such as this one, to organizations both in the public and the private sector. In cooperation with the Academy of Public Administration we run a number of 2-day workshops designed for the training of data protection officers in the public sector, and a similar series of 2-day workshops will be organized in autumn, for the private sector.

Ladies and gentlemen, again I would like to thank you for inviting me to deliver this speech and I hope that I have met your expectations.