December 2012

ISFE Position
on the proposed Data Protection Regulation

Introduction

ISFE, the Interactive Software Federation of Europe represents the European videogame industry which produces entertainment and educational software for use on personal computers, game consoles, portable devices and mobile phones. The videogame industry is the fastest growing 'content' sector in Europe and is a major employer within the EU. ISFE member publishers distribute videogames for consumer enjoyment both on and off line and the European videogame market is now estimated to be worth approximately € 20 billion annually.

The online games sector is the fastest growing part of our industry. More and more consumers are playing games online thereby engaging in international and multi-lingual communication on a constant basis. The scale of such online communication is a good example of how much the growth of our online industry relies on an efficient transfer of data between territories. Unfortunately, the inconsistent Member State implementation of the Data Protection Directive has created a fragmented digital single market in which such cross border data flows are greatly hindered.

We therefore welcome the Commission's initiative to modernize the European Data Protection framework and to try to establish greater harmonisation of various national frameworks. The proposed Regulation would deliver uniformity and therefore increased legal certainty to the data protection regimes that apply at national level to the benefit of businesses and consumers alike. We also approve of the focus on the issues of globalization and international data transfer, as well as on the reduction of the administrative and costs burden through harmonisation and simplification of the current notification system.

Furthermore, we applaud the references to support for self-regulatory initiatives which would contribute to better enforcement of data protection rules. Self-regulation has the unique ability to quickly develop detailed sector-specific rules based on the industry's expertise in a rapidly changing digital environment and forms the best complement to the existing, more general legal framework. The videogame industry already has extremely robust measures in place to protect consumers' data and to ensure safe, transparent and efficient communication when data is being gathered. We welcome any approach that enshrines these best practices which are applied to protect our consumers.

We do however have concerns that the wide ranging nature and scope of the Regulation and the inflexibility and lack of definition of a number of key concepts defined therein may both make implementation more difficult and also increase the cost of compliance for companies of all sizes, so contributing to an increase in the uncertainty that the Regulation is designed to eliminate.

I. General ISFE Concerns

ISFE has concerns that some key provisions in the Regulation, particularly those which concern the 'Right to be Forgotten', Data Breaches and Data Portability, will be difficult to implement in practice without further specific guidance (and accurate definitions) on the scope of how the recommendations are to be applied. Many of the proposals introduce new concepts and seem to be dealing with issues that relate mainly to social networks. There is concern that the wider effects of these proposals on other sectors and business models have not been properly considered. This could make implementation extremely difficult, prohibitively expensive and could also create legal uncertainty.

Costs of implementation could indeed be very high as existing data systems may have to be re-built to ensure compliance. In the videogame industry the management of data and the development of tools required to so do can vary greatly depending on the specific platform used to deliver a game. The methodology required is best understood and implemented by the industry and therefore does not lend itself easily to third party regulation.

Further, many stipulations in the Regulation are subject to 'Delegated' or 'Implementing' acts through which the Commission can specify criteria, conditions and requirements. Although leaving certain issues to Delegated Acts may be necessary, many provisions of the Regulation cannot in fact be applied without the corresponding act being in place from the outset. As the adoption of such delegated acts in relation to a large number of articles may take several years, substantial legal uncertainty is bound to follow. Such uncertainty will not be conducive to business or therefore to the growth of this industry.

II. Specific ISFE Concerns

(a) Consent (Art. 4 and Art. 7)

The regulation currently calls for a single form of "freely given, specific, informed and explicit consent" to be given by consumers before data controllers can gather and process any form of personal data in cases where none of the other conditions in Article 6 apply. As the legitimate interests condition in Article 6(1)(f) appears to have been restricted to a degree, particularly in respect of children (which as defined means anyone under the age of 18), the circumstances in which industry will need to obtain the consent will increase. Whilst the video game industry fully recognizes the need for consumers to have transparency regarding where their data is being gathered, we are also concerned about the potential impact of this requirement on the user-friendliness, speed and financial cost of the services offered to our consumers (particularly for gameplay services which are often offered to children under 18).

The increased requirements for consent in Article 7 also present challenges for this industry, especially in an online context. In particular, it is not clear what is expected of controllers in order to prove that they have obtained consent in an online context. Also, if data controllers must obtain

consent for each data privacy matter separately from other matters this could lead to registration pages for online services with multiple 'opt-ins' or consent statements. Further, it is unclear if the reservation that consent cannot be obtained where there is a significant imbalance between the data subject and the data controller applies to commercial situations. It would be extremely difficult for games companies, particularly those operating online, to assess on a case by case basis whether or not such an imbalance exists.

Requiring numerous opt-in mechanisms for all categories of personal information will frustrate many users (particularly children). It will increase the potential for consent fatigue ('click fatigue') and may lead consumers to automatically consent to everything and to not pay proper attention to critical notifications, such as those regarding sensitive data. This will eventually drastically lessen the impact and undermine the principle of consent. It may also stifle the uptake of European services by consumers may become unnecessarily frustrated by long 'registration pages' and processes..

(b) Parental Consent (Art. 8)

According to the draft proposal, the collection and processing of personal data of a child below the age of 13 years by providers of information services directed to children shall only be lawful if consent is given or authorised by the child's parent or custodian. Our industry welcomes a European wide agreement on the age of parental consent which is consistent on both sides of the Atlantic, and has always been a keen supporter of the enhancement of parental involvement in children's online activities.

ISFE has already engaged in self-regulatory initiatives to empower parents and to strengthen data and minor protection in the online gameplay environment. In 2003 the industry adopted a pan-European Age rating system PEGI which is now the industry standard (and is backed by a rigorous Code of Conduct for PEGI signatories). PEGI provides parents with intelligible, objective information and advice about the suitability of video game content for their children. In 2009 ISFE also launched PEGI Online, a European Commission funded labelling system that indicates if PEGI rated online game services ensure both user privacy and protect minors against unsuitable online content.

As said before, we very much welcome the recognition and support in the Regulation for the implementation of codes of conduct in order to contribute to a better application and enforcement of data protection rules. However, the details of the standard form for methods to obtain valid parental consent have been left for the Commission to develop after the adoption of the Regulation.

Ideally, mechanisms for obtaining verifiable parental consent should be flexible and scalable, leverage existing technologies, minimize the burden on parents and service providers and work on different technological platforms. We would therefore recommend allowing the industry to adopt user-friendly, effective and enforceable standards in consultation with the European Commission which will avoid regulatory uncertainty and compliance challenges. PEGI and PEGI Online are very good examples of how effective such standards can be.

(c) the Definition of Personal Data (Art. 4)

Parental consent need to rely on a pragmatic definition of 'personal data.' The definition proposed in the Regulation is very broad and encompasses any type of information, from sensitive data to pseudonymised and anonymised data used to facilitate website browsing. It does not take into account the different categories of data in terms of their risk and the feasibility of enabling the identification of a specific individual. Nor does it allow the development of a sliding scale of varying levels of safeguards that each of the categories must ensure in order to best protect a child's personal data. Instead, under the present definition, virtually any web activity of children under 13 will require a child to obtain parental consent. This may impede our industry's ability to maintain and develop the current range of online entertainment services directed to children under 13.

Historically in the US, anonymised or pseudonymised data such as screen names and user names have been recognized as a valid way to avoid collection of personal information of children under 13, while at the same time enabling interactivity and user customization in the design of the online services directed to children. A recent FTC amendment to COPPA (the 'Children's Online Privacy Protection Act') has clarified that a screen name or user name is to be regarded as personal information only '…where it functions in the same manner as online contact information…' The FTC also recognized that such data is typically used to support the internal operations of an online service 'in place of individually identifiable information, including use for content personalization, filtered chat, for public display on a website or online service, or for operator-to-user communication via the screen or user name.' It is also essential to user authentication, maintaining user preferences, protecting against fraud or theft, and using analytics to improve site navigation or service offerings.

Video game publishers and console and handheld manufacturers often limit themselves to the collection of user names alone, specifically to avoid the collection of more sensitive types of personal information, such as children's full names or e-mail addresses. A single screen name can allow a player to engage in online gameplay, aggregate achievements and maintain user settings and preferences across different gameplay platforms. It can also serve as a security function to activate, access, or use an authenticated copy of the game software.

If the processing of such anonymised or pseudonymised data is to be submitted to a Parental Consent rule, the operator will need to collect additional, more sensitive, personal information from the child, including the parent's online contact information and the name of the child or parent. Investments to implement the consent mechanism will substantially increase costs on all types of games and will make the business model of some smaller games unworkable. Publishers might also choose to limit the interactive features of games which will affect all users and will stifle innovation. We therefore recommend that the use of anonymised and pseudonymised data in practices which do not implicate privacy concerns should be exempt from the parental consent requirement, or, at least, should only trigger a low level of protection.

(d) Right to be Forgotten and to Erasure (art.17)

The proposed Regulation states that individuals have a 'Right to be Forgotten'. Where an individual makes such a request and the personal data has been made public, data controllers are responsible for taking all reasonable steps to inform any third parties that the data subject wishes them to erase their data and any subsequent links to them.

First, the Regulation should recognize the difficulties companies may face removing all trace of data relating to a single individual from their systems "without delay". Data can be stored in backup tapes for instance and it can be difficult, time consuming and costly to remove individual items of data from such tapes while retaining the rest. In the context of a company's own infrastructure, it is not as simple as it might appear to delete all information about a user because of the nature of commonly adopted backup systems. Data cannot be manually deleted from some backup systems, data controllers have no choice but to wait until the system automatically deletes data (such deletions are carried out periodically). Data can be manually deleted from other backup systems, but this can be impractical, time consuming and therefore expensive. The cost to data controllers of deleting data from backup systems manually rather than waiting for the next scheduled auto delete needs to be balanced against the likelihood of consumer harm if data is retained on the backup system until the next auto delete. In our view, the risk of consumer harm is low here and does not justify the potential cost (if the data can be permanently (?) deleted manually at all).

Second, by stating that data subjects have the "right to obtain from the controller the erasure of personal data relating to them" the Regulation suggests that companies are expected to be able to delete all data for a given individual.

The Regulation over-estimates the ability of a business to have oversight of the entire internet and the information available on it. Publicly available data is transmitted extensively across the internet which makes it difficult if not impossible to remove all traces of an individual's data. The proposals do not take into account how data is or has been transferred (e.g. by third parties), and under which types or formats. Storage of personal data is necessary for various reasons both legal and commercial associated with security, financial accounting, tax compliance, service improvement, customer service and user protection, but also increasingly to combat fraud and piracy. There is a growing concern that the Right to be Forgotten could be used to conceal an illegal act, and/or to prevent detection of copyright infringements. Piracy is an increasing problem for our industry which is endeavouring to develop and grow, especially online where piracy can thrive at great speed. It is not clear that all of these commercial reasons for retention are clearly permitted in paragraphs 1 and/or 3 of Article 17 and they should, therefore, be explicitly acknowledged in the text.

Much of the data stored about individuals, however, poses no threat to consumers should a data breach occur. We therefore consider the proposal of removing all data relating to a consumer, regardless of any assessment of its effect on them, as simply too broad.

As already stated, whilst this proposal, in general, seems to be dealing with issues that relate mainly to social networks, its wider effects on other sectors and on business models such as those of our member companies should be properly considered. We therefore would like to see the Regulation

provide more clarity on exactly what is expected of companies and third parties with regards to the Right to be Forgotten, particularly with respect to paragraph 2 of Article 17. The Regulation should encourage companies to be responsible for deleting data that is within their control, should also ensure that any expected measures are within the bounds of what is technically possible and should be more focused on the specific issue and sector that the Commission is seeking to address.

(e) Right to Data Portability (art. 18)

The Regulation also provides data subjects with a Right to Data Portability i.e. a right to obtain their data in a structured, commonly used electronic format which can be used across different platforms and services. As the range of digital businesses currently using data is increasing all the time, establishing just one single data format would be extremely difficult and expensive.

Of added concern is the proposal for the Commission to set formats, technical standards and procedures for data transfer should industry not be able to comply with the requirements introduced under the Regulation. Imposing a single format for the transfer of data will stifle innovation and again be extremely costly for business. Furthermore, requiring the use of a "commonly used" format is potentially dangerous – commonly used formats are arguably less secure as they are better understood. The best way to ensure data security and confidentiality is to use a format which is not commonly used. It should therefore be left to industry to define the format and technical details of how data should be transferred in a secure, but easy and consumer-friendly way.

The Right to Data Portability also requires a copy to be provided of all personal data that is undergoing processing by the data controller. However, it is unlikely that the data subject would require a copy of all data classified as personal data being processed, given the breadth of the definition of personal data, in order to move to a different service. If the Right to Data Portability is to be retained, it should be narrowed to cover the data that the data subject actually needs in order to change providers. The right should also be focused on the industries upon which the Commission seems to be focused i.e. social networks, otherwise it could have unintended consequences for other data controllers which do not offer a social network service. For instance, does the proposal mean that games companies with online gameplay networks must offer portability for all gameplay statistics, forum posts, etc if a user wishes to move to another gameplay network? This would appear not to be the case because an uncommon format is likely to be used in these instances. The position is not clear in the text.

Finally, all the above points expose the fact that the Right to Data Portability is not actually a question of Data Protection and Privacy, and is rather a question of Consumer Rights and Barriers to Market Entry as they apply to social networks, and should not be present at all in a general framework Regulation for Data Protection law.

(f) Measures Based on Profiling (Art. 20)

Like many digital businesses, some games industry business models rely on Profiling to offer consumers a better service. Profiling is merely the aggregation and sorting of data into patterns. It can have many benefits and allows web services to retain key information and improve the service that they offer individuals (for example linking suitably matched players to each other in online games). There is nothing inherently wrong with Profiling, although it can sometimes be applied in less beneficial ways.

It therefore makes sense for the Regulation to focus on limiting how harmful Profiling can be prevented, rather than limiting the beneficial use of it to improve legitimate online businesses. We also would like to request more clarity concerning the methods and circumstances under which adults can waive their right to be profiled.

(g) Privacy by Design and by Default (Art. 23) and Transparent Communication (Art.11)

The video game industry is global by nature. Most retail games now allow for online play between gamers from around the world and a large part of the revenue streams are derived from such online play. It is therefore of vital importance that the technical standards and requirements which must ensure that the principles of 'Privacy by Design' and 'Privacy by Default' are implemented will not affect the ability of the users to easily interact with each other and obtain the best possible gameplay experience. While it is a good idea to ensure that data protection is inherent in the design of systems and services that store personal data, we are against imposing strict design mandates or overly prescriptive procedures as they would stifle innovation, hinder technological development and could have a huge negative impact on the user experience and consequently the financial revenue of our sector.

We also would like to caution that the provision to provide privacy policies in an intelligible form, using clear and plain language, in particular for any information addressed specifically to a child, should not be overly prescriptive. There is no single language that can be equally plain and clear for all the various age and user groups. Such a requirement may impair the necessary flexibility and legal certainty required to deal with the many different types of data interactions involving our members companies.

(h) Documentation (art. 28)

We feel that the requirement to maintain documentation of all internal processing operations places an unnecessary burden on industry with no real added value for the data subjects. Such provisions, as with a number of the issues raised above, seem to contradict the initial objective of the Data Protection Framework Review i.e. to reduce administrative burdens on industry.

(i) Data Breach Notification (art. 31)

The proposal requires all data controllers, in all sectors, to notify their Data Protection Authorities about all breaches – regardless of the risk that they pose or the harm that they might cause. Reporting must be within 24 hours and applies broadly to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to any personal data.

Whilst it is accepted that data breach notification is important as a principle, it will be very difficult to comply in practice with the scope of the current proposals. It will not, for example, be possible to notify large scale data breaches with any accuracy within the 24 hour timescale stipulated in the Regulation. Data controllers will need time to assess the impact of data breaches as there are likely to be many cases where internal and external parties will need to provide intelligence on the nature and extent of the breach.

Increasing the time available to make a notification would mean the accuracy and usefulness of the notification to both regulators and consumers would be likely to increase, making implementation of the Regulation more of a reality. Therefore, rather than specifying a time period within which to notify, we would suggest using a more realistic standard i.e. that data controllers are required to notify within a reasonable time once they are on notice of a data breach. This will allow data controllers sufficient time to fully investigate and therefore accurately report on the breach.

It is also significant that there is no mechanism in place to determine or filter out data breaches with a high level or low level of risk or severity. Imposing the requirement to notify all breaches within 24 hours, regardless of severity, will likely lead to Data Protection Authorities being overwhelmed by data breach notifications and to high level breaches going undetected. In order to facilitate effective implementation of the Regulation, the notification requirement should only apply to breaches over a specified level of severity or risk, for example where there is a reasonable likelihood of the breach resulting in consumer harm, and the timescale for notification should take account of the severity or complexity of the breach involved.

(j) Extended Impact Assessments (Art. 33)

The Regulation stipulates that the processing of children's' personal data in large scale filing systems present specific risks to the rights and freedoms of data subjects. The controller must carry out an impact assessment of these envisaged processing operations which includes a consultation of the data subject(s). It can be questioned here as well whether data protection authorities will be able to cope with high volumes of impact assessments and whether data subjects being inundated with consultation requests will be able to deal with them effectively. Further, the lack of a clear definition of "large scale filing systems" and the fact that the Commission still needs to specify the criteria and conditions for the processing operations that present such risks will create considerable uncertainty. Finally, a requirement for such a level of impact assessments would necessitate a disproportionate level of expense.

(k) Fines (Art. 79)

A similar "one-size-fits-all" approach is applied where the Regulation proposes to fine companies up to 2% of their turnover in the event of a breach of the Regulation, including data breaches. There does not seem to be any connection between the impact of a particular breach and the size of the fine. As the maximum levels of these fines are disproportionate, small and medium sized businesses will be less likely or indeed unable to engage in business in the EU. Larger enterprises may scale back or review existing or planned operations.

We are also concerned about the risk of discriminatory application of the fines as a result of there being no objective criteria on how regulators should levy the penalties. We therefore ask for the introduction of a fine structure which is proportionate to the impact that a particular breach has for example the impact of a data breach on consumers, and which takes account of the difference between situations where companies intentionally or negligently violate the rules, and situations where they cannot reasonably be held culpable for the breach. Data security is of course of utmost importance to our industry but no system is infallible and in data breach cases data controllers are often the victims of others acting illegally. A proportionate fine structure should take into account the culpability of the data controller as well as the impact of the breach.

(l) Intellectual Property Protection.

The proposals contained in both the draft Regulation and the draft Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences, should not prevent the effective implementation of IP enforcement measures.

The concerns that have long been raised by rightsholders concerning the interface between data protection and the enforcement of intellectual property rights have not been resolved in the draft Regulation. Uncertainty regarding the relationship between the Enforcement Directive and the Data Protection Regulation will, as things stand, unfortunately, remain. The draft Regulation includes no specific reference to the right to property. While the Explanatory Memorandum does refer to the right to property, there is no corresponding reference in the Regulation itself. In the light of recent CJEU case law, we regard the Regulation's silence on the need to balance the fundamental right to privacy with the fundamental right to property as a serious cause for concern.

The current broad definition of "personal data" also triggers concerns as to how it will affect the transfer of data relating to IPR enforcement. While Recital (24) of the draft Regulation states that "identification numbers, location data, online identifiers … as such need not necessarily be considered as personal data in all circumstances", this statement being in a Recital is of lesser legal significance. The relevant wording contained in Recital 24 is also vague.

In particular, we question whether IP addresses collated by third party internet scanners should be regarded as "personal data" when the addresses will not be used to identify individuals and when such third party scanners have no means to link them to individuals.

Conditions for the lawfulness of Data Processing in Article 6 of the draft Regulation have been tightened in comparison to those in the current Directive. Article 6(1)(f) (which provides that data processing shall be lawful if "necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child") will become more demanding in nature with the adoption of "delegated acts", and its "balancing test" will be subject to even more restrictions than Article 7(f) of the current Directive 95/46/EC.

Article 21 ("Restrictions") of the draft Regulation is equivalent to Article 13 of the current Directive which constitutes an important legal basis for rightsholders in the context of copyright enforcement activities. Article 13 includes the well-known reference to the "rights and freedoms of others". Article 21 of the Draft Regulation provides for the possibility that EU or national law may restrict, by way of a legislative measure, the rights and obligations set forth in Article 5(a) to (e) (principles relating to data processing), Articles 11 to 20 (right of the data subject), and Article 32 (communication of a personal data breach to the data subject), when such restriction constitutes a necessary and proportionate measure in a democratic society and when it is intended to safeguard in particular: public security; the prevention, investigation, detection and prosecution of criminal offences; other public interests of the Union or of a Member State (in particular an important economic or financial interest); the protection of the data subject or the rights and freedoms of others. Although subject to strict conditions, this provision could still be used, we believe, as a tool to help deal with the interface between privacy and the right to property. However, it is unclear why it appears to serve only as a derogation to Article 5, but not also to Article 6 (on lawfulness of processing).