EUROPE'S VIDEO GAMES INDUSTRY

ISFE position paper on the Data Act

1. ISFE supports the Data Act's overall objective of ensuring fairness in the allocation of economic value among actors of the data economy and creating a "well-functioning single market for data". Our sector understands how important data is for economic development. Without data, our industry would not exist. We fundamentally agree with the European Commission that removing the obstacles that hinder a better sharing of data can promote growth, encourage innovation, and foster digital transformation.

2. We have, however, identified a number of issues that may impact these objectives. These are related to the horizontal nature of this legislative instrument, its broad scope and the lack of clarity on how it aligns with the applicable legal framework. We have developed corresponding recommendations that aim to help ensure that the principles in this law can be translated into workable requirements which will deliver on the ultimate objective of establishing a flourishing data economy. We will highlight these following the order of the chapters in the proposal. Our key recommendations are:

    - The proposal should explicitly state that data protection law prevails in case of a conflict with the provisions of the proposal.
    - Video game consoles and peripherals should be explicitly excluded from the definition of a product.
    - The scope of the unfairness test should be clarified.
    - The scope of B2G data access requests should be clarified and defined much more narrowly.
    - Data covered by trade or professional secrecy must be exempt from the scope.

The proposal should explicitly state that data protection law "prevails" in case of a conflict with the provisions of the proposal

3. ISFE members support the joint opinion[1] of the European Data Protection Board and European Data Supervisor where it calls on the legislators to strengthen the wording of Article 1(3) by explicitly specifying that, in case of conflict with the provisions of the proposal data protection law "prevails", insofar as it concerns the processing of personal data.

4. Article 2(1) defines data as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording". This definition is extremely broad and does not distinguish

[1] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), §26.

between different types of data and includes both personal and non-personal data. It has raised the risk of overlapping and conflicting obligations with existing data and privacy protecting rules and principles at the level of the "data holder and "data user". A data holder may also be a data controller under the GDPR whereby corresponding obligations, such as data minimisation, purpose limitation, and privacy by design, may be in clear conflict with the interests of the data user who may, for instance, want to monetize his data and would therefore be more interested in receiving large datasets. Similarly, if the data holder and controller is also the manufacturer of the product, he would find that the privacy by design and privacy by default requirements in the GDPR would contradict with the obligation in Article 3.1 to make data generated by the use of products or related services accessible by default. Finally, the data holder may simply find it impossible to share data as it consists of personal data and lacks a legal basis to do so.

5. The proposal regularly refers to pseudonymisation and encryption as examples of technical and organisational measures that data sharing parties should implement to protect the fundamental rights of individuals. However, these techniques cannot help solve the issues resulting from conflicting legal obligations, as pseudonymised data (including encrypted data) do not fall outside the scope of data protection regulations because re-identification is still possible[2]. A legal basis under the GDPR is therefore necessary when pseudonymised personal data is subject of a data access request. Anonymisation represents a more effective privacy-preserving mechanism as it would require the data holder to take robust measures including by aggregating the data to a level where the individual events are no longer identifiable. The technique can however not always be applied, because the risk of the re-identification, for instance by singling out individuals, remains high in certain datasets[3].

6. ISFE members consider that the best way to address such conflicting competences is to explicitly state that the provisions of the data protection and privacy frameworks supersede those of the Data Act proposal. We welcome and support the current statements in Article 1(3) and recital 7 of the proposal, which aim to ensure that the application of existing data protection rules shall not be affected or undermined. However, we agree with the EDPB and EDPS that the legal order between the two frameworks need to be further clarified and that the wording of Article 1(3) should be strengthened by explicitly specifying that, in case of conflict the provisions of the data protection and privacy frameworks would prevail. This will allow for more legal certainty, thus enabling the industry to easily comply and reap the benefits of the new Regulation.

[2] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, p 10.
[3] 10 misunderstanding about anonymisation, AEPD/EDPS report, p 4

Video game consoles and peripherals should be explicitly excluded from the definition of a product.

7. ISFE calls on the legislators to explicitly exclude video games consoles and peripherals from the definition of a product by adding it to the list of excluded devices under recital 15.

8. A product is defined in the proposal as a "tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data." Recital 15 clarifies that "the Regulation should not cover certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps".

9. Video game consoles consist of home consoles and handheld devices with their integrated networks and associated peripherals that share similar characteristics, including: custom hardware and operating systems designed for game play; an integrated online network and marketplace unique to that platform supporting game play functions while also providing ancillary functions. The primary purpose of a console is to provide gameplay. While the integrated networks and associated peripherals are designed to supplement and enhance the device's game play purpose, other entertainment functions, such as downloading or streaming of movies and music, are additional, ancillary functions. This characterisation of the console's primary purpose is widely recognised[4].

10. Video games as interactive experiences that involve sequences of events individually created and controlled by players each time they play. On-screen action in a video game entirely consists of the processing of data by software operation which is essentially dependant on human input from the player, and in the case of multiplayer games, the input of multiple users. No game is experienced the same way twice and many have no pre-defined end.

11. Consequently, video game consoles are very clearly excluded from the definition of a product and we call on the legislators to include them in the list of examples in Recital

[4] It was for instance also used and adopted in the context of the "Games Consoles Voluntary Agreement, a self-regulatory initiative set up under the terms of EU Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products.

15. In this context, ISFE members also agree with the joint EDPB and EDPS Opinion[5] which considers that the proposal "defines a product in such (broad) terms that it might be necessary to amend this definition of product so as to clearly exclude products listed in recital 15, including also in the enacting terms of the proposal."

The scope of the unfairness test should be clarified.

12. ISFE calls for clarity on the lists of terms set out in Articles 13(3) and (4). The text should clarify that the contract terms listed in Article 13(3), which are very general in nature, only apply where they expressly relate to access or use of data and data-related obligations. Terms in Article 13(3) and (4) such as "grossly", "inappropriate", "significantly detrimental", "proportionate" or "unreasonable" are open to wide interpretation and should be avoided or more clearly defined to provide certainty.

13. ISFE appreciates the objective of Article 13 is to protect SMEs in cases where they have been unable to influence changes to unfair contract terms. However, it is not practical to put the burden of proof on the data provider in these cases, not least because it could lead to a large number of spurious claims. We recommend that the burden of proof should be on the data recipient.

14. ISFE does not favour an extension of the test to negotiated data-related terms. This idea, which was assessed as part of policy option 3 in the impact assessment report[6], would have a disproportionate impact on the principle of freedom of contract and was rejected by the researchers. As a matter of principle, the contractual parties should remain free to negotiate the terms and conditions of the contract, even if they result in a situation where one party is able to obtain a better deal than the other. Contractual agreements between commercial actors can differ substantially depending on the objective of the data sharing and the potential risks to which the data can be exposed. Companies should therefore always be able to freely enter into data sharing agreements after careful consideration of all the implications.

The scope of B2G data access requests should be defined much more narrowly.

15. ISFE members recommend limiting the scope of B2G access requests to what is strictly necessary and proportionate, while clearly stating that public sector bodies must demonstrate that the data could not be obtained alternatively, or that the request would substantively reduce the administrative burden.

[5] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), §42.
[6] Commission Staf Working Document, Impact Assessment Report, p 36.

16. Chapter V of the proposal provides for an obligation to make privately held data available to public sector bodies that demonstrate an exceptional need to use the requested data. Article 15 states that such exceptional need may occur to respond to (or prevent) public emergencies or in situations where the lack of available data prevents the public sector bodies from fulfilling a specific task in the public interest that has been explicitly provided by law or the data cannot be obtained by alternative means (including by purchasing on the market or through existing or new legislation), or obtaining these data would "substantively reduce the administrative burden for data holders or enterprises".

17. ISFE members agree with the statement in recital 61 that, "in cases of exceptional need, a proportionate, limited and predictable framework at Union level is necessary for the making available of data to public sector bodies, both to ensure legal certainty and to minimise the administrative burdens placed on businesses". We welcome in Article 17.2 that B2G access requests must be clear and proportionate in terms of their scope of content and their granularity, and that their purpose and intended use must be specific and clearly explained. However, we are concerned that the scope of the legal basis for such access requests is not very precise and overly broad which flouts basic legal principles of legal clarity and proportionality in EU law.

18. The definition of public emergencies provided under Article 2(10) appears overly broad and goes well beyond classical examples, such as natural and public health disasters. It also covers situations negatively affecting an individual member state, or part of it, with the risk of serious repercussions on living conditions, such as disruptions in production chains and cybersecurity incidents. The notions of public interest and exceptional need are not defined although recital 58 mentions as example of the latter "the timely compilation of official statistics".

19. ISFE members recommend defining much more narrowly the concepts of public emergencies and exceptional need to ensure that access to data by public authorities remains limited to what is strictly necessary and proportionate. The obligation to provide data to "assist the recovery from a public emergency" would give public bodies extremely wide discretion potentially going beyond the concept of "exceptional need". Furthermore, it should be clarified in Article 15(c) that public sector bodies must prove that they "have been unable to obtain such data by alternative means" or that obtaining the data would "substantively reduce the administrative burden for data holders or enterprises". If not, such provisions may be misused to circumvent legislative action to invoke access to data in a disproportionate way.

20. The need to define much narrower what qualifies as a 'public emergency' and 'exceptional need' is even higher in cases where the data consists of personal data, as was clearly established by the joint EDPB-EDPS opinion. It clearly stated that "any limitation on the right to personal data, such as an obligation to share personal data with a public sector body, must be based on a legal basis of which the scope is clearly defined

and accompanied by sufficient safeguards to protect individuals against arbitrary interference "[7].

The proposal should exclude data covered by trade or professional secrecy from its scope.

21. ISFE members recommend excluding all business sensitive information, including trade secrets, from all data sharing obligations under this proposal.

22. Article 21 states that public sector bodies that have received data in the context of the provisions of chapter V are entitled to share that data with third parties in view of carrying out scientific research or analytics, or to national statistics bodies and to Eurostat, but only to the extent that the research is compatible with the purpose for which the data was requested and that the third parties act on a not-for-profit basis or in the context of a public-interest mission recognised in Union or Member State law. The proposal however does not provide sufficient safeguards for the legal protection of data when data is shared to a third party in this context.

23. Art. 17 specifies that data access requests from public sector bodies shall respect "the legitimate aims of the data holder, *taking into account the protection of trade secrets* and the cost and effort required to make the data available and that they shall concern, *insofar as possible*, non-personal data". Further on, Art. 19 specifies that disclosure of trade secrets or alleged trade secrets to a public sector body shall only be required to the extent that it is strictly necessary to achieve the purpose of the request and that, in such a case, the public sector body shall take *appropriate measures* to preserve the confidentiality of those trade secrets.

24. These provisions are very vague and do not provide any definition of the "appropriate measures" that the public sector body is expected to take, nor do they provide any indication as to how compliance will be monitored and enforced. Furthermore, it is unclear how the public sector body can be able to determine whether disclosure of trade secrets is necessary to achieve the purpose of the request when the essence of a trade secret is that it excludes others from confidential business information.

25. The proposal lacks necessary guarantees to ensure full legal protection of the requested data which can create serious security concerns for the video games sector. The data processed within a video game is usually based on a unique code format which only has relevance in the context of that specific game and is protected under the EU Computer Programs Directive as well as subject to non-disclosure agreements under the licensing agreements allowing gameplay. Revealing the code would weaken the protection measures put in place to prevent piracy and keep players safe from hackers and would allow other companies to copy the game.

[7] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), § 77.

26. Private sector data is often the result of investments and usually entails commercially sensitive information that allow a company to have a competitive advantage. The protection of this confidential business data and trade secrets is paramount to a well-functioning competitive market. We are concerned that the provisions in this proposal may undermine the protection regime afforded by the Trade Secrets Directive. Rather than focussing on weak confidentiality safeguards, the proposal should clearly exempt trade secrets from its scope.

About ISFE

1. The Interactive Software Federation of Europe (ISFE) comprises national trade associations covering 18 countries throughout Europe which represent in turn hundreds of games companies at national level. ISFE also has as direct members the leading European and international publishers, many of which have studios with a strong European footprint, that produce and publish interactive entertainment and educational software for use on personal computers, game consoles, portable devices, mobile phones and the Internet.
   Transparency Register Identification Number: 20586492362-11

2. The video games industry represents one of Europe's most compelling economic success stories, relying on a strong IP framework, and is a rapidly growing segment of the creative industries. The European digital single market area is the third-largest market for video games globally. All in all, there are around 5,000 game developer studios and publishers in Europe, employing over 98,000 people. In 2021, Europe's video games industry was worth €23,3bn[8].

[8] ISFE Key Facts from 2021 from GameTrack Data by Ipsos MORI and commissioned by ISFE.

Suggested amendments

Text proposed by the Commission	*Amendments*
Article 1.3 Union law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect the applicability of Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC, including the powers and competences of supervisory authorities. Insofar as the rights laid down in Chapter II of this Regulation are concerned, and where users are the data subjects of personal data subject to the rights and obligations under that Chapter, the provisions of this Regulation shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679.	Article 1.3 Union law **and national law** on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment shall apply to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation ~~shall not affect the applicability of Union law on the protection of personal data~~ **is without prejudice to**, in particular Regulation**s** (EU) 2016/679 **and (EU) 2018/1725** and Directive**s** 2002/58/EC, **(EU) 2016/680 and (EU) 2016/943** including **with regard to** the powers and competences of supervisory authorities. Insofar as **data subjects are concerned,** the rights laid down in Chapter II of this ~~Regulation are concerned, and where users are the data subjects of personal data subject to the rights and obligations under that Chapter, the provisions of this Regulation~~ shall complement the right of data portability under Article 20 of Regulation (EU) 2016/679 **and shall not adversely affect data protection rights of others.**
Justification *The wording of Article 1(3) should be strengthened by explicitly specifying that, in case of conflict, the provisions of the data protection and privacy frameworks would prevail, insofar as it concerns the processing of personal data. Similarly, the Trade Secret Directive has been added to the list of laws that would prevail in case of conflict.*	

Text proposed by the Commission	*Amendments*
Article 2 (2) 'product' means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data;	Article 2 (2) 'product' means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data **nor is it primarily designed to display or play content, or to record and transmit content**;

Recital 15: In contrast, certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.	Recital 15: In contrast, certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, **consoles and peripherals**, cameras, webcams, sound recording systems and text scanners. They require human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps.
Justification *Video game consoles and peripherals should be explicitly excluded from the definition of a product by adding it to the list of excluded devices under recital 15 while the definition of a product should be amended to better exclude them.*	

Text proposed by the Commission	*Amendments*
Article 13.5 A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that supplied a contractual term bears the burden of proving that that term has not been unilaterally imposed.	Article 13.5 A contractual term shall be considered to be unilaterally imposed within the meaning of this Article if it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it. The contracting party that **claims that a contractual term has been unilaterally imposed,** bears the burden of **proof** ~~proving that that term has not been unilaterally imposed.~~
Justification *Putting the burden of proof on the supplier of a contractual term in cases when this term is contested as being unfair would lead to a large number of spurious claims.*	

Text proposed by the Commission	*Amendments*
Article 2(10) 'public emergency' means an exceptional situation negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the substantial degradation of economic assets in the Union or the relevant Member State(s);	Article 2(10) 'public emergency' means **public health emergencies, emergencies resulting from natural disasters, as well as human-induced major disasters, such as major cybersecurity incidents,** ~~an exceptional situation~~ negatively affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions or economic stability, or the

	substantial degradation of economic assets in the Union or the relevant Member State(s);
Article 15 An exceptional need to use data within the meaning of this Chapter shall be deemed to exist in any of the following circumstances: (a) where the data requested is necessary to respond to a public emergency; (b) where the data request is limited in time and scope and necessary to prevent a public emergency or to assist the recovery from a public emergency; (c) where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law; and (1) the public sector body or Union institution, agency or body has been unable to obtain such data by alternative means, including by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data; or (2) obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises.	Article 15 An exceptional need to use data within the meaning of this Chapter shall be **limited in time and scope and** deemed to exist **only** in ~~any of~~ the following circumstances: (a) where the data requested is **strictly** necessary to respond to a public emergency; (b) where the data request is ~~limited in time and scope and~~ **strictly** necessary to prevent a public emergency ~~or to assist the recovery from a public emergency~~; (c) where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law; and (1) the public sector body or Union institution, agency or body **can clearly demonstrate that it** has been unable to obtain such data ~~by alternative means, including~~ by purchasing the data on the market at market rates or by relying on existing obligations to make data available, and the adoption of new legislative measures cannot ensure the timely availability of the data; or (2) **it can demonstrate that** obtaining the data in line with the procedure laid down in this Chapter would substantively reduce the administrative burden for data holders or other enterprises.
Justification *The scope of the concepts of public emergency and exceptional need must be narrowed to what is strictly necessary and proportionate.*	

Text proposed by the Commission	*Amendments*
Article 4.3 Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.	Article 4.3 ~~Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties.~~ The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.
Article 5.8 Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed	Article 5.8 ***Deleted***

between the user and the third party and all specific necessary measures agreed between the data holder and the third party are taken by the third party to preserve the confidentiality of the trade secret. In such a case, the nature of the data as trade secrets and the measures for preserving the confidentiality shall be specified in the agreement between the data holder and the third party.	
Article 8.6 Unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.	Article 8.6 Unless otherwise provided by Union law~~, including Article 6 of this Regulation,~~ or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943.
Article 19.2 Disclosure of trade secrets or alleged trade secrets to a public sector body or to a Union institution, agency or body shall only be required to the extent that it is strictly necessary to achieve the purpose of the request. In such a case, the public sector body or the Union institution, agency or body shall take appropriate measures to preserve the confidentiality of those trade secrets.	Article 19.2 ***Deleted***
Justification *Trade secrets should be excluded from all data sharing obligations under this proposal.*	

ISFE Secretariat, October 2022