

DATA ACT/ AFEP proposals

- Scope and definitions, including the data covered: to be specified

Amendment 1

Commission's proposal	AFEP proposals
Article 2: Definitions (1) 'data' means 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;	Article 2: Definitions (1) data' means <i>IoT data as</i> 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 <i>communicated by a product or related service via a publicly available electronic communication service;</i>
	New recital <i>(14a new) Connected products generate a wide variety of IoT data, differing in their volumes, natures or levels of processing. Possible market failures, incentives for innovation and the competitive situation within and outside the Union differ greatly depending on the situation considered. Specific needs and sectoral details should therefore be left to the flexibility of contractual freedoms to allow for more tailored definitions of shareable data.</i>

Justification

This clarifies that data covered by the scope should only be **data emanating from products or related services as defined by this Regulation**. Moreover, flexibility should be left in the recitals to allow for **differentiated approaches and tailored definitions** to take into account the nature, volume and processes of data resulting from the use of a connected product, which is by no means homogenous.

Amendment 2

Commission's proposal	AFEP proposals
Article 2: Definitions	Article 2: Definitions <i>(1a) 'accessible data' means data that the data holder can request and obtain, via a publicly available electronic communication service, in a digital, machine-readable format, from the product, onto an existing interface.</i>

Justification

This Regulation should not assume that all data is already easily accessible and shareable provided that the obligation is introduced into law. Sectoral realities show that companies are engaged in **continuous efforts to extract, collect, format and process data** in order to make it usable. Both the product design and architecture need to allow for such access. Moreover, some data is not available to the data holder and is considered intermediate or “circulating data” before being stored in a final format, with only the latter being accessible. **No obligation to store additional data should be introduced**, as this would generate significant constraints for the data holder (change of product specification and significant additional costs). This accessible data should be granted to both the manufacturer and the user alike to ensure a level playing field. It will also ensure that privacy by design and by default is complied with.

Amendment 3

Commission's proposal	AFEP proposals
Article 2: Definitions (3) 'related service' means a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions;	Article 2: Definitions (3) 'related service' means a digital service, including software, which is incorporated in or directly inter-connected with a product at the time of its sale, rent or lease in such a way that its absence would prevent the product from performing one of its functions;
Recitals (16) It is necessary to lay down rules applying to connected products that incorporate or are interconnected with a service in such a way that the absence of the service would prevent the product from performing its functions. Such related services can be part of the sale, rent or lease agreement, or such services are normally provided for products of the same type and the user could reasonably expect them to be provided given the nature of the product and taking into account any public statement made by or on behalf of the seller, renter, lessor or other persons in previous links of the chain of transactions, including the manufacturer. These related services may themselves generate data of value to the user independently of the data collection capabilities of the product with which they are interconnected. This Regulation should also apply to a related service that is not supplied by the seller, renter or lessor itself, but is supplied, under the sales, rental or lease contract, by a third party. In the event of doubt as to whether the supply of service forms part of the sale, rent or lease contract, this Regulation should apply	Recitals (16) It is necessary to lay down rules applying to connected products that incorporate or are interconnected with a service in such a way that the absence of the service would prevent the product from performing its functions. Such related services can be part of the sale, rent or lease agreement, or such services are normally provided for products of the same type and the user could reasonably expect them to be provided given the nature of the product and taking into account any public statement made by or on behalf of the seller, renter, lessor or other persons in previous links of the chain of transactions, including the manufacturer. These related services may themselves generate data of value to the user independently of the data collection capabilities of the product with which they are interconnected. This Regulation should also apply to a related service that is not supplied by the seller, renter or lessor itself, but is supplied, under the sales, rental or lease contract, by a third party. In the event of doubt as to whether the supply of service forms part of the sale, rent or lease contract, this Regulation should apply. <i>These related services do not include the Electronic Communication Service that provides the interconnection.</i>

Justification

The proposed definition is too broad and could potentially include all processing services, IoT and AI software as well as other market participants, whereas the data sharing obligation is focused on manufacturers of a product and the services offered with it.

Amendment 4

Commission's proposal	AFEP proposals
Article 2: Definitions (5) 'user' means a natural or legal person that owns, rents or leases a product or receives a services ;	Article 2: Definitions (5) 'user' means a natural or legal person that owns, rents or leases a product or makes use of a contractual service;

Justification

To add clarification in accordance with Recital 18, where the user is defined through contractual relationship ("which has purchased, rented or leased the product. Depending on the legal title under which he uses it (...)").

Amendment 5

Commission's proposal	AFEP proposals
Article 2: Definitions (6) 'data holder' means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services , the ability to make available certain data;	Article 2: Definitions (6) 'data holder' means a legal or natural person who holds the data and has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, the ability to make available certain data that it holds ;

Justification

This amendment will help clarify who actually holds the data generated by the use of the product and will hence be expected to make the data available to the user. Indeed, in some sectors, the **entity that holds the data might be a separate entity from the manufacturer and may not have control of the design of the product and related services**. Similarly, the user can also act as a data holder. It will be necessary for certain sectors to have to clarify the attribution of rights and obligations in situations where the configurations of production, hold of data, use and ownership of the device are more complex than the manufacturer-user relationship.

■ Articulation with the GDPR: to be improved

Amendment 6

Commission's proposal	AFEP proposals
<p>Article 3: Obligation to make data generated by the use of products or related services accessible</p> <p>1. Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user.</p>	<p>Article 3: Obligation to make data generated by the use of products or related services accessible</p> <p>1. Products shall be designed and manufactured, and related services shall be provided, in such a manner that accessible data generated by their use are, by default, easily, safely, securely and, where relevant and appropriate, directly accessible to the user. <i>This should be done without endangering their functionality nor going against data security requirements from Regulation 2016/679, product regulations or technical standardisation.</i></p>

Justification

As some products and services may process different categories of personal data, **their sharing must be carried out in accordance with the GDPR and appropriate protection must be ensured**. Privacy by design should not be put into question. As underlined by the EDPB and EDPS in their [joint opinion](#), “co-legislator (shall) explicitly specify that **data protection prevails in case of conflict with the provisions of the Proposal** insofar as the processing of personal data is concerned”. In addition to preserving this fundamental right, this would also ensure that there is no confusion during the implementation of texts by companies and that these provisions do not go against their efforts and investments to strengthen the data security and cybersecurity of their products.

Amendment 7

Commission's proposal	AFEP proposals
<p>Article 6: Obligations of third parties receiving data at the request of the user</p> <p>(b) use the data it receives for the profiling of natural persons within the meaning of Article 4(4) of Regulation (EU) 2016/679, unless it is necessary to provide the service requested by the user;</p> <p>(c) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user;</p>	<p>Article 6: Obligations of third parties receiving data at the request of the user</p> <p>(b) use the data it receives for the profiling of natural persons within the meaning of Article 4(4) of <i>under conditions that do not comply with Regulation</i> (EU) 2016/679, unless it is necessary to provide the service requested by the user;</p> <p>(c) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user <i>or this provision strictly complies with Regulation (EU) 2016/679</i>;</p>

Justification

The prohibition on using data received by a third party for profiling purposes (Article 6-2-b) appears **contrary to Article 6 of the GDPR** which defines the legal bases (processing made necessary for the execution of the contract, consent of the individual, public interest, compliance with a legal obligation or legitimate interest of the controller) allowing controllers to process personal data. The EDPB also developed guidelines.

It is also **contrary to the objective of innovation** of the Data Act, as profiling, when respectful of the GDPR, allows a multiplicity of European economic actors to better understand the needs of users and develop new services.

Article 6-2-c is also contrary to the GDPR which also already very strictly regulates the sharing of data between economic operators and the reuse of personal data, to which are added the rights of data subjects guaranteed by the GDPR.

Thus, this amendment recalls the **necessary consistency with Regulation (EU) 2016/679** to promote the sharing of data between the different actors in the digital economy and European innovation.

■ Sharing of data : free of charge for B to C/ fair compensation in both B to B and B to G

- Free of charge for non-professional users

Amendment 8

Commission's proposal	AFEP proposals
<p>Article 4: The right of users to access and use data generated by the use of products or related services</p> <p>1. Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.</p>	<p>Article 4: The right of users to access and use data generated by the use of products or related services</p> <p>1. Where data cannot <i>be accessed</i> by the <i>user on</i> the product, the data holder shall make available to the user the <i>accessible</i> data <i>directly</i> generated by its use of a product or related service without undue delay, free of charge <i>for non-professional users</i> and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible</p>

Justification

The operational costs involved in the collection, storage, management, and dissemination via electronic means of data generated by products can be substantial for the data holder. In this respect, **preserving the incentive for industrial players** to develop the volume of data available must be fully taken into account, as an essential condition for the further development of the sharing of this data –**except when the user is a non-professional one**. The volume of data required by a commercial company is typically higher than for individual consumers and will likely increase exponentially as the EU data economy continues to develop. Such costs may become unsustainable for individual manufacturers and will severely undermine investment incentives.

The rest of the amendment is in line with previous amendments on accessible data (Art. 2 – amendment 2).

Amendment 9

Commission's proposal	AFEP proposals
<p>Article 5: Right to share data with third parties</p> <p>1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the user of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time</p>	<p>Article 5: Right to share data with third parties</p> <p>1. Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the accessible data directly generated by the user of a product or related service to a third party, without undue delay, free of charge to the non-professional user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time</p>

Justification

Similar to the previous amendment: The operational costs involved in the collection, storage, management, and dissemination via electronic means of data generated by products can be substantial for the data holder. In this respect, preserving the incentive for industrial players to develop the volume of data available must be fully taken into account, as an essential condition for the further development of the sharing of this data - **except when the user is a non-professional one**. The volume of data required by a commercial company is typically higher than for individual consumers and will likely increase exponentially as the EU data economy continues to develop. Such costs may become unsustainable for individual manufacturers and will severely undermine the investment incentives.

The rest of the amendment is in line with previous additions on accessible data (Art. 2 - amendment 2).

- Professional users: fair compensation taking into account the value of data

Amendment 10

Commission's proposal	AFEP proposals
<p>Article 9: Compensation for making data available</p> <p>1. Any compensation agreed between a data holder and a data recipient for making data available shall be reasonable.</p> <p>2. Where the data recipient is a micro, small or medium enterprise, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request. Article 8(3) shall apply accordingly.</p> <p>3. This Article shall not preclude other Union law or national legislation implementing Union law from excluding compensation for making data available or providing for lower compensation.</p>	<p>Article 9: Compensation for making data available</p> <p>1. Any compensation <i>contractually</i> agreed between a data holder and a data recipient for making data available shall <i>take into account the value of this data and the cost of making it available</i>.</p> <p>2. Where the data recipient is a micro, small or medium enterprise, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, any compensation agreed shall not exceed the costs directly related to making the data available to the data recipient and which are attributable to the request. Article 8(3) shall apply accordingly.</p>

Justification

The “reasonable” nature of the compensation agreed upon between a holder and a recipient of data must be:

- decided between data holder and recipient **through a fair contract**,
- specified in order to better take into account the **real value of this data** and the cost of making it available, and
- thus, national or **European provisions likely to call into question this principle of compensation should be removed**.

- Fair contractual terms for all parties

Amendment 11

Commission's proposal	AFEP proposals
<p>Article 13: Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise</p> <p>1. A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise as defined in Article 2 of the Annex to Recommendation 2003/361/EC shall not be binding on the latter enterprise if it is unfair.</p>	<p>Article 13: Unfair contractual terms unilaterally imposed on <i>one of the parties</i></p> <p>1. A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise on <i>one of the parties shall</i> not be binding on the latter enterprise if it is unfair.</p>

Justification

This approach seems to be unsuitable in the digital world where **any structure can be economically powerful regardless of its size** and where unfair terms might also exist between larger companies.

As such, it is proposed **to target “parties”** instead of micro, small or medium-sized enterprises.

- B2G data sharing: limit a too broad and unclear scope

Amendment 12

Commission's proposal	AFEP proposals
Article 2: Definitions (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 substantial degradation of economic assets in the Union or the relevant Member State(s);	Article 2: Definitions (10) 'public emergency' means an exceptional situation negatively, <i>suddenly and unpredictably</i> affecting the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on living conditions, economic stability, <i>and</i> substantial degradation of economic assets in the Union or the relevant Member State(s);

Justification

Companies recognize the need to respond to a public emergency and therefore share their data to help the community. However, the definition of "public emergency" as proposed remains very broad and could prove disproportionate and unviable for data holders, especially for long-term emergency situations.

Thus, this definition should be amended **to refer exclusively to situations affecting the Union or Member States**

1. **suddenly and unpredictably**
2. and to provide for **cumulative conditions**.

Amendment 13

Commission's proposal	AFEP proposals
<p>Article 15: Exceptional need to use data</p> <p>(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</p> <p>(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; or¹²</p> <p>(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</p>	<p>Article 15: Exceptional need to use data</p> <p><i>Deleted</i></p>

Justification

AFEP regrets the lack of impact assessment that would have identified potential market failures that would justify such an obligation. Data sharing with public authorities work satisfactorily, but the **Article 15- c) provision appears particularly disproportionate and outside of the concept of exceptional need**. Sharing obligations towards public sector bodies (B2G) **should be duly justified** (no intervention when the current situation is satisfactory) in order to **avoid extensive national interpretations**.

Amendment 14

Commission's proposal	AFEP proposals
<p>Article 20: Compensation in cases of exceptional need</p> <p>2. Where the data holder claims compensation for making data available in compliance with a request made pursuant to Article 15, points (b) or (c), such compensation shall not exceed the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation and of technical adaptation, plus a reasonable margin. Upon request of the public sector body or the Union institution, agency or body requesting the data, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin</p>	<p>Article 20: Compensation in cases of exceptional need</p> <p>2. Where the data holder claims compensation for making data available in compliance with a request made pursuant to Article 15, points (b), such compensation shall not exceed the technical and organisational costs incurred to comply with the request including, where necessary, the costs of anonymisation and of technical adaptation, plus a reasonable margin. Upon request of the public sector body or the Union institution, agency or body requesting the data, the data holder shall provide information on the basis for the calculation of the costs and the reasonable margin</p>

Justification

In line with the amendment to Article 15 (amendment 13), deletion of (c).

Amendment 15

Commission's proposal	AFEP proposals
Article 17: Requests for data to be made available	Article 17: Requests for data to be made available
2. A request for data made pursuant to paragraph 1 of this Article shall:	2. A request for data made pursuant to paragraph 1 of this Article shall:
(a) be expressed in clear, concise and plain language understandable to the data holder;	(a) be expressed in clear, concise and plain language understandable to the data holder;
be proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested;	(b) be proportionate to the exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested and be limited to data necessary to carry out the task carried out; (bbis) mention the purpose of this processing

Justification

The current version of this chapter contains undetermined obligations to transfer data, which could include personal data, phrased in a way that suggests exemption from GDPR (e.g., (45) GDPR : " ... *where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law (...)* It should also be for Union or Member State law to determine the purpose of processing").

With B2G obligations, the **purpose of processing should be explained** at the time of the request and the **data requested be clearly limited**.

Amendment 16

Commission's proposal	AFEP proposals
<p>Article 17: Requests for data to be made available</p> <p>4. Paragraph 3 does not preclude a public sector body or a Union institution, agency or body to exchange data obtained pursuant to this Chapter with another public sector body, Union institution, agency or body, in view of completing the tasks in Article 15 or to make the data available to a third party in cases where it has outsourced, by means of a publicly available agreement, technical inspections or other functions to this third party. The obligations on public sector bodies, Union institutions, agencies or bodies pursuant to Article 19 apply.</p>	<p>Article 17: Requests for data to be made available</p> <p>4. Paragraph 3 does not preclude a public sector body or a Union institution, agency or body to exchange within the Union data obtained pursuant to this Chapter with another public sector body, Union institution, agency or body in view of completing the tasks in Article 15 or to make the data available to a third party in cases where it has outsourced, by means of a publicly available agreement, technical inspections or other functions to this third party. The obligations on public sector bodies, Union institutions, agencies or bodies pursuant to Article 19 apply.</p>

Justification

Regarding Article 17-4, these exchanges can potentially go beyond the strict European framework and therefore undermine the competitiveness of European companies without conditions of reciprocity.

To avoid such an economic inconvenience, this amendment **precise the scope of this exchange** between other public sectors or third parties.

Amendment 17

Article 18: Compliance with requests for data	Article 18: Compliance with requests for data
	<p><i>5bis. The public sector body, Union institution, agency or body making the request for a dataset is solely responsible for the proportionality and adequacy of the request and processing. The data holder may not be held liable nor fall under claims, damages and expenses in relation to alleged GDPR violations ensuing from the transfer and processing, where the data holder has abided by a request and provisions under this Regulation.</i></p> <p><i>The data holder, whether complying with the request or not, may refer the request and alleged processing to the relevant national supervisory authority.</i></p>

Justification

The current Regulation proposal makes the data holder sole responsible for controlling the proportionality of the request in terms of volume and granularity (see Articles 18(2) b. and 17 (2) b.), whereas the public sector is requesting data for special purposes known to him alone. This thus puts at risk the data holder:

- the data holder may be scared or induced into communicating data to public authorities without any control at all, notably bearing in mind that (i) the data holder may regard itself as unable or illegitimate to take decisions over a matter of public interest, which only the public authority is legitimate in determining and (ii) dismissing the request may be an administrative offence,
- data holders may be also at risk of litigation from the data subjects (user) or supervisory authorities for not adequately preserving personal data (Article .32 & 33 of the proposal), or for impeding or delaying public administration's action.

The public sector body, Union institution, agency or body making the request for a dataset should therefore be **solely responsible for the proportionality and adequacy of the request and processing** and the **data holder should not be held responsible for potential breaches** ensuing from the transfer and processing by the public sector body, Union institution, agency or body.

Amendment 18

Commission's proposal	AFEP proposals
<p>Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs</p> <p>4. Where a public sector body or a Union institution or body transmits or makes data available under paragraph 1, it shall notify the data holder from whom the data was received.</p>	<p>Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs</p> <p>4. Where a public sector body or a Union institution or body <i>intends to transmit or make</i> data available under paragraph 1, it shall <i>first inform</i> the data holder from whom the data was received <i>and provide all necessary information regarding the identity of the data recipient and the activities that will be carried out by the data recipient based on the data received pursuant to paragraph 1.</i></p>

Justification

The guarantees regarding the confidentiality of the data and trade secrets provided under this provision fall short of offering **the legal protection and certainty** that private stakeholders that share data to serve the public interest should be afforded.

Data shared with a public sector body under Article 14 should **not be passed on** without prior agreement of the data holder.

Amendment 20

Commission's proposal	AFEP proposals
Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs	<p>Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs</p> <p><i>5. (new) 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, provided that all specific necessary measures required by the trade secret holder are taken to preserve the confidentiality of trade secrets, in particular with respect to the third parties. The data holder and the public sector body, or the Union institution, agency or body can contractually agree on measures to preserve the confidentiality of the shared data, in particular in relation to third parties. The data holder should have the possibility to refuse this sharing, when these guarantees are not ensured or respected ex-ante.</i></p>

Justification

See the justification above for Article 19.

The Data Governance Act moreover provides that confidential information (e.g. trade secrets) can be disclosed for re-use only with the **data holder's permission** whose rights or interests may be affected by the re-use.

- Intellectual property rights and trade secrets: ensure an appropriate protection

Amendment 21

Commission's proposal	AFEP proposals
Article 1: Subject matter and scope	Article 1: Subject matter and scope <i>5(new). This Regulation shall not affect Union Treaties, Union and national legal acts providing for the protection of commercially sensitive data, including the protection of trade secrets as defined by Directive 2016/943 of the European Parliament and of the Council, and intellectual property rights</i>

Justification

Respect for intellectual property rights and trade secrets is framed by several European and national texts that should be recalled in the Data Act. This respect is essential in order to **avoid distortions of competition for companies holding data** and to **maintain sufficient incentives** for them to invest and innovate. Without sufficient safeguards, the Regulation could lead to weak protection of these rights and secrets and to **leaks of European innovation to third countries**. The text should also expressly exclude data of a technical nature which could be subject to either or both trade secrets and IP rights protection, in accordance with Recitals 14 and 17, in particular derivative data.

- In B2B and with third parties

Amendment 22

Commission's proposal	AFEP proposals
<p>Article 4: The right of users to access and use data generated by the use of products or related services</p> <p>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.</p>	<p>Article 4: The right of users to access and use data generated by the use of products or related services</p> <p>3. Trade secrets shall only be disclosed <i>upon agreement of the data holder and</i> 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.</p>

Justification

Compliance with Article 39 §2 of TRIPS (Agreement on Trade-Related Aspects of Intellectual Property Rights), Directive 2016/943 and the Data Governance Act where **consent of the trade secret owner is key** for the protection of such trade secret, needs to be reflected in this provision. In addition to inconsistency with these texts, the lack of reference to the consent of trade secrets' owners when disclosing their assets would be a major competitive disadvantage for non-EU companies and a discouragement to investing in R&D for EU corporations.

Amendment 23

Commission's proposal	AFEP proposals
<p>Article 4: The right of users to access and use data generated by the use of products or related services</p> <p>6. The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active.</p>	<p>Article 4: The right of users to access and use data generated by the use of products or related services</p> <p>6. The data holder and the user shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement. The data holder shall not use such data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active.</p>

Justification

One clarification is added to specify that **both data holders and users have to use non-personal data on the basis of a contractual agreement**. The provisions as written in the proposal may provide a user with the means to bypass the data holder, by passing-on data obtained pursuant to Article 3 directly to third parties.

This would nullify all protections afforded to the data holder and trade secrets holder under Article 5. The protection of confidential business data and trade secrets is paramount to a well-functioning internal market.

Amendment 24

Commission's proposal	AFEP proposals
<p data-bbox="376 395 954 427">Article 5: Right to share data with third parties</p> <p data-bbox="215 472 1115 767">8. Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed 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.</p>	<p data-bbox="1290 395 1868 427">Article 5: Right to share data with third parties</p> <p data-bbox="1137 472 2024 879">8. Trade secrets shall only be disclosed to third parties <i>upon agreement of data holder and</i> to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party and <i>provided that</i> 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 <i>contractually</i> in the agreement between the data holder and the third party. <i>The data holder should have the possibility to refuse this sharing, when these guarantees are not ensured or respected ex-ante.</i></p>

Justification

The fragile safeguards envisaged are likely to slow down investments in innovation due to a lack of protection against potential breaches of business secrecy and distortions of competition. The proposal also leaves open the **question of possible guarantees for the data holder** if he fails in reaching an agreement with the data recipients on the protection measures. The text, which moreover does not distinguish between EU users and non-EU users or third parties should not force the data holder to disclose data constituting a trade secret. **Prior consent and sufficient protection measures** agreed between the parties are therefore required.

Amendment 25

Commission's proposal	AFEP proposals
<p>Article 35: Databases containing certain data</p> <p>In order not to hinder the exercise of the right of the users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the sui generis right provided in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service.</p>	<p>Article 35: Databases containing certain data</p> <p>In order not to hinder the exercise of the right of the users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the <i>subject of the</i> sui generis right provided in Article 7 of Directive 96/9/EC <i>shall not invoke this sui generis right to deny to the user access to the</i> data generated by <i>its</i> use of a product or a related service.</p>

Justification

The exception introduced by the proposed Regulation to the Sui Generis right could **jeopardize the intellectual property of database producers** as the entire database could remain unprotected in the future. The creation of databases indeed requires considerable human, technical and financial resources. This derogation could jeopardize their future investments, which would have a significant impact on the innovation capacity of European economic players. A less restrictive approach should therefore be adopted, **protecting both the user's right of access and the data holder's investment.**

- In B2G

Amendment 26

Commission's proposal	AFEP proposals
<p>Article 14: Obligation to make data available based on exceptional need</p> <p>1. Upon request, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested.</p> <p>2. This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.</p>	<p>Article 14: Obligation to make data available based on exceptional need</p> <p>1. Upon request, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested, <i>subject always to the provisions in Article 19 regarding trade secrets and subject to compensation in Article 20.</i></p> <p>2. This Chapter shall not apply to small and micro enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC.</p>

Justification

Respect for intellectual property rights and trade secrets is essential in order to **avoid distortions of competition for companies holding data** and to **maintain sufficient incentives** for them to invest and innovate.

Amendment 27

Commission's proposal	AFEP proposals
<p>Article 19</p> <p>Obligations of public sector bodies and Union institutions, agencies and bodies</p> <p>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.</p>	<p>Article 19</p> <p>Obligations of public sector bodies and Union institutions, agencies and bodies</p> <p>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, <i>provided that all specific necessary measures required by the trade secret holder are taken to preserve the confidentiality of trade secrets, in particular with respect to the third parties. The data holder and the public sector body, or the Union institution, agency or body can contractually agree on measures to preserve the confidentiality of the shared data, in particular in relation to third parties. The data holder should have the possibility to refuse this sharing, when these guarantees are not ensured or respected ex-ante.</i></p>

Justification

Similarly to B2C and B2B sharing, it must be ensured that data is protected against access by unauthorised third parties or cyber-attacks and it is therefore essential to ensure that appropriate technical and organizational measures are adopted by public sector bodies to **ensure the confidentiality and integrity of the data shared**. Trade secrets should only be disclosed **where the data holder agrees to it**, and where **all specific measures agreed upon** between the data holder and the public sector body are taken by the latter to preserve the confidentiality of the trade secrets.

The Data Governance Act provides that confidential information (e.g. trade secrets) can be disclosed for re-use only with the data holder's permission whose rights or interests may be affected by the re-use.

- Non-personal data safeguards in an internal context: refrain from creating additional burdens for European companies

Amendment 28

Commission's proposal	AFEP proposals
<p data-bbox="389 536 936 564">Article 27: International access and transfer</p> <p data-bbox="199 612 1128 890">3. In the absence of such an international agreement, where a provider of data processing services is the addressee of a decision of a court or a tribunal or a decision of an administrative authority of a third country to transfer from or give access to nonpersonal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only:</p> <p data-bbox="199 898 1128 1066">(a) where the third-country system requires the reasons and proportionality of the decision or judgement to be set out, and it requires such decision or judgement, as the case may be, to be specific in character, for instance by establishing a sufficient link to certain suspected persons, or infringements;</p> <p data-bbox="199 1074 1128 1137">(b) the reasoned objection of the addressee is subject to a review by a competent court or tribunal in the third-country; and</p> <p data-bbox="199 1145 1128 1313">(c) the competent court or tribunal issuing the decision or judgment or reviewing the decision of an administrative authority is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protect by Union law or national law of the relevant Member State.</p> <p data-bbox="199 1321 1088 1385">The addressee of the decision may ask the opinion of the relevant competent bodies or authorities, pursuant to this Regulation, in order to</p>	<p data-bbox="1303 536 1850 564">Article 27: International access and transfer</p> <p data-bbox="1532 612 1621 641"><i>Deleted</i></p>

determine whether these conditions are met, notably when it considers that the decision may relate to commercially sensitive data, or may impinge on national security or defence interests of the Union or its Member States.	
--	--

Justification

This paragraph attends to mirror the GDPR and imposes a level of protection on non-personal data only required to protect personal data and fundamental rights. AFEP recalls the importance of data flows from and to the EU for European companies and calls for avoiding new barriers and uncertainties in the market. As such, the **burden on the data processing service provider** to prevent international transfers appears disproportionate in view of the reality of these flows. Because EU companies already struggle to assess the adequacy of non-EU laws with EU privacy laws, they question the possibility to perform similar assessments regarding confidentiality, trade secrets, patents, and intellectual property rights.

About AFEP

Since 1982, AFEP brings together large companies operating in France. The Association, based in Paris and Brussels, aims to foster a business-friendly environment and to present the company members' vision to French public authorities, European institutions and international organizations. Restoring business competitiveness to achieve growth and sustainable employment in Europe and tackle the challenges of globalization is AFEP's core priority.

AFEP has 114 members. More than 8 million people are employed by AFEP companies and their annual combined turnover amounts to €2,600 billion.

AFEP is involved in drafting cross-sectoral legislation, at French and European level, in the following areas: economy, taxation, company law and corporate governance, corporate finance and financial markets, competition, intellectual property, digital, labour law and social protection, environment and energy, corporate social responsibility and trade.

Contact:

Emmanuelle Flament-Mascaret, Director for Economic Law / concurrence@afep.com

Alix Fontaine, European Affairs Advisor / a.fontaine@afep.com