

KEEP EUROPE GROWING

10 July 2015

Keep Europe open to international data transfers – the Digital Single Market is not enough to ensure global competitiveness!

Dear GDPR trialogue stakeholders of European Institutions,

The European Data Coalition acknowledges and respects the need to protect EU citizens' data when transferring data outside the EU. International data transfers are not meant to circumvent EU data protection standards, rather it is possible to reconcile economic interests with the fundamental right to privacy. Open international data transfers are critical for the growth of and continued investments in EU-based data processing businesses. Simply promoting the Digital Single Market (DSM) is not enough in order for European companies to achieve and/or maintain global competitiveness leadership.

This position paper reflects on Chapter V of the proposed Regulation. It is our intention to identify concerns but also suggest solutions that would guarantee the right conditions for continued investments in EU-based data processing, while preserving the right of EU companies to benefit from global value chains, enhancing trust and maintaining or even improving privacy standards.

1. International Data Transfers

Under the proposed Regulation, there will be three categories of lawful transfers: 1) transfers with an adequacy decision (Art. 41/1); 2) transfers by way of appropriate safeguards (Art. 42/1) and c) exceptional transfers as laid down in Art. 44 (see below).

In this context, we would like to address the following concerns:

1.1. Adequacy decisions & Appropriate Safeguards (incl. BCRs)

The Coalition encourages the European Commission to continue to **promote and expand mutual recognition through adequacy assessments** of third countries' privacy regulations. This will limit the need for a competent authority to approve cross-border data flows, as well as the need for controllers or processors to rely on specific legal transfer mechanisms. Furthermore, adequacy decisions should impose reciprocal obligations, to keep the third countries' personal data flows open into the EU and improve the business conditions for EU based data processing.

When international harmonization of privacy regulations cannot be realistically achieved, or is expected to take a long time, the Coalition supports the ambition of EU Institutions to foster the **use of effective legal transfer mechanisms** such as the U.S. [Safe-Harbor Company Certification](#), [Binding Corporate Rules](#) (BCRs) for both controllers and processors or [Standard Contractual Clauses](#) to facilitate trans-border data flows.

1.2. Sunset Clauses

Cross-border data flows have become the backbone of international commerce and services. The internet economy alone has accounted for 21% of European economic growth during the past five years¹. Many European SMEs create jobs in Europe by exploiting the benefits of the digital ecosystem. Data is critical to SME's across all sectors to compete fairly in the global economy.

We are very concerned that the European Parliament proposed the introduction of sunset clauses to existing adequacy decisions and to existing authorizations for BCRs or Standard Contractual Clauses. The Parliament text also retains the power for the Commission to adopt inadequacy decisions. Accordingly, the Commission would have to reissue adequacy decisions within five years of the entry into force of the Regulation, or within two years in case of appropriate safeguards authorisations. Compliance with well-established and trusted data transfer arrangements under Directive 95/45/EC already implied a significant investment by European businesses. Suspending these transfer mechanisms would result in unacceptable regulatory uncertainty and make it prohibitively costly for private companies to invest in these transfer mechanisms, with unnecessary harmful consequences for the relationship with trade partners and users.

The Commission's proposal and the Council's version follow a more adequate approach to existing transfer mechanisms, allowing them to continue until amended, replaced or repealed by the Commission. The European Data Coalition supports this approach as it safeguards investment and international trade.

1.3. Specific Authorisation

References to "specific authorisation" in Arts. 41/1 and 42/3 are introduced, instead of "further authorisation" as proposed by the Commission, when an adequacy decision or safeguard authorisations have been adopted. **The essence of these measures is that once they are approved, no other (or "further") notification is required. If we impose additional ("specific") requirements, it defeats the purpose of these instruments, as it will create uncertainty and could undermine the system in place.** Therefore, the Commission's original proposal ("such transfer shall not require any "further" authorization) seems to be more in line with the purpose of the law, as stated in Recital 80, Art. 41/1 and Art. 42/2(a).

ARTICLE 41 Transfers with an Adequacy Decision			
European Commission	European Parliament	Council	European Data Coalition
1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of	1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an	1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of	1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of

¹ McKinsey Global Institute, The great transformer: The impact of the Internet on economic growth and prosperity, October 2011 (available at http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_transformer)

<p>protection. Such transfer shall not require any further authorisation.</p> <p>(...)</p> <p>5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).</p> <p>(...)</p> <p>8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission.</p> <p>(...)</p>	<p>adequate level of protection. Such transfer shall not require any further specific authorisation.</p> <p>(...)</p> <p>5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 to decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).</p> <p>(...)</p> <p>8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission in accordance</p>	<p>protection. Such transfer shall not require any further specific authorisation.</p> <p>(...)</p> <p>3a. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a the Decision adopted in accordance with paragraph 3 or 5.</p> <p>(...)</p> <p>5. The Commission may decide that a third country, or a territory or a processing specified sector within that third country, or an international organisation does not no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).</p> <p>5a. The Commission shall enter into consultations with the third country or</p>	<p>protection. Such transfer shall not require any further authorisation.</p> <p>(...)</p> <p>3a. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a the Decision adopted in accordance with paragraph 3 or 5.</p> <p>(...)</p> <p>5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).</p> <p>5a. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the before taking a Decision made pursuant to paragraph 5. The</p>
--	---	--	---

	with paragraph 3 or 5 before the end of this period.	international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5. (...) 8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission.	Commission shall ensure appropriate publicity for this consultation.
--	--	---	--

ARTICLE 42 Transfers by way of Appropriate Safeguards			
European Commission	European Parliament	Council	European Data Coalition
(...)	(...)	(...)	(...)
3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) or paragraph 2 shall not require any further authorization.	2. The appropriate safeguards referred to in paragraph 1 may shall be provided for (...), without requiring any specific authorization from a supervisory authority , by:	2. The appropriate safeguards referred to in paragraph 1 may be provided for (...), without requiring any specific authorization from a supervisory authority , by:	3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) or paragraph 2 shall not require any further authorization.
(...)	(...)	(...)	(...)
5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in	5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall	5b. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency	5b. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in

Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.	apply the consistency mechanism referred to in Article 57 Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until two years after the entry into force of this Regulation unless amended, replaced or repealed by that supervisory authority before the end of this period.	mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by a that supervisory authority Commission Decision in accordance with paragraph 2.	Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by a that supervisory authority Commission Decision in accordance with paragraph 2.
--	---	---	---

2. Prohibition on data disclosure to third-country administrative or judicial authorities

Article 43a is clearly a reaction to the National Security Administration’s (NSA) PRISM program. EU Institutions are rightly trying to limit access of national security agencies to EU personal data. However the access of the EU member states’ national security agencies to EU personal data goes unaddressed. Art. 43a would ultimately force European companies operating in the US and Europe to choose which legislation to break when they receive a Foreign Intelligence Surveillance Act (FISA) order from the US government. It also sets a poor example for other jurisdictions: the would-be EU approach promotes extra-territorial conflict of law and places European companies in the middle of an unsolvable dilemma. Article 43a introduces severe legal uncertainty for European companies operating in the EU and US territories, with serious practical implications on their operations.

Our Coalition is in favour of reviewing the access to commercially processed data by national security and law enforcement agencies. Compliance with national security and law enforcement requests should neither require private companies to violate the privacy and data protection laws of other countries, nor their reasonable privacy commitments to individuals, employees, and customers. But we must stress that **the proposed Art. 43a is an untenable solution as it puts European companies in the middle of an extra-territorial conflict of law. Furthermore Art. 43a does not offer a genuine legal redress for EU citizens, as it does not create competencies over EU or non-EU national security and law enforcement agencies.**

The Coalition recommends deleting Article 43a. Any concerns with law-enforcement access to commercial data processing should be dealt with the relevant frameworks, and not in the context of commercial data processing.

ARTICLE 43 (new)			
Transfers or Disclosures not Authorised by Union Law			
European Commission	European Parliament	Council	European Data Coalition
	1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international		1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual

	<p>agreement in force between the requesting third country and the Union or a Member State.</p> <p>2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority.</p> <p>3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with points (d) and (e) of Article 44(1) and Article 44(5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57.</p> <p>4. The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1).</p>		<p>legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.</p> <p>2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority.</p> <p>3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with points (d) and (e) of Article 44(1) and Article 44(5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57.</p> <p>The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1).</p>
--	---	--	--

3. Not all international data transfers are created equal

It is important to remark that not all data transfers are equal and they do not imply the same level of risk. Art. 44 (“derogation”) proposes a gamut of exceptions to the general requirements for lawful international transfers set down in Articles 41-43. The proposed text is similar to that of Art. 26 of the 95 Directive, except for (h). This paragraph caters to needs to transfer personal data where such needs arise infrequently and where the transfer is not massive. The Coalition agrees that this derogation should not cover mass transfers or frequent small-scale transfers of end-user data. Its fundamental objective is to address business-to-business situations when a **temporary or non-bulk or non-frequent data transfer of personal data is necessary for completion of a support function, troubleshooting action or routine control**. Typically in these circumstances the personal data is incidental and not the object or purpose of the transfer.

This derogation is of economic relevance, as it allows EU companies greater flexibility in accessing global expertise and will contribute to increased job creation and stimulate EU-based investment. In today’s economy, products and applications are based on systems constructed in both EU and non-EU countries. As developers and support personnel are located in various countries, allowing them to perform their work remotely is not only necessary, but also a reality of today’s global distribution value chains. Open cross-border data flows must not conflict with the protection of data subjects, if openness is underwritten by accountability, suitable verification and non-circumvention. Furthermore, transfers that are infrequent, not massive and necessary to fulfill lawful interests by the controller or processor should be acknowledged under a reciprocity condition before the conclusion of an adequacy assessment of a third country. In the light of the above, the Coalition applauds the Council’s expansion of 41/1(h) to allow controllers and processors to transfer non-bulk or non-frequent data. We recommend that this clause also include a time-related element (“temporary”).

ARTICLE 44 Derogations			
European Commission	European Parliament	Council	European Data Coalition
<p>1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p style="text-align: center;">(...)</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on</p>	<p>1. 1. In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p style="text-align: center;">(...)</p> <p>(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation</p>	<p>1. In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules, a transfer or a set category of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p style="text-align: center;">(...)</p> <p>(h) the transfer, which is not large or frequent, is necessary for the purposes of the legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject or the processor, which cannot be qualified</p>	<p>1. In the absence of an adequacy decision pursuant to Article 41, or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:</p> <p style="text-align: center;">(...)</p> <p>(h) the transfer, which is temporary, not large or frequent, is necessary for the purposes of the legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject which cannot be qualified as frequent or massive, and where the controller or processor has assessed all</p>

<p>this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p>	<p>or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.</p>	<p>as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate suitable safeguards with respect to the protection of personal data, where necessary.</p>	<p>the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data.</p>
---	--	---	--

Recital 86			
European Commission	European Parliament	Council	European Data Coalition
<p>Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.</p>	<p>Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his explicit consent, where the transfer is necessary occasional in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.</p>	<p>Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his explicit consent, where the transfer is necessary occasional in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.</p>	<p>Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his explicit consent, where the transfer is necessary occasional in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients. When a controller in a third country needs to transfer back the personal data from an EU-based processor, such controller shall have the right to transfer back the personal data without restrictions.</p>

Conclusion

In conclusion, the Coalition recognises the necessity to protect EU citizen's data in international data transfers. Our argument in favour of flexible data flows is not, in any way, an attempt to defraud EU data protection standards, but rather to show that it is possible to advance privacy rights together with a regulatory text that promotes innovation and economic growth. Indeed, a progressive data protection regulation framework must recognize the significance of today's global value chains and the increasing role of international data transfers for European businesses.

The Coalition's proposal in this document offers concrete suggestions to triologue stakeholders to protect the fundamental right while at the same time make significant qualitative improvements to GDPR hereby allowing European companies to Keep Europe Growing!



Rene Summer

Coalition Spokesperson

ABOUT THE COALITION

Our Coalition is made up of twenty European companies, from SMEs to Global Multinationals and non-profit organisations operating in a variety of sectors on a national, regional and global scale. With an aggregate turnover (2013) of over € 158 billion and some 752,000 employees worldwide, our footprint allows us to bring growth, progress and jobs to the EU's economy. Our membership includes...

... a global leader in power and automation solutions...
... the leading Central and Eastern European e-commerce company...
... a productivity solutions provider of compressors, vacuum solutions, construction and mining equipment...
... a non-profit organisation dedicated to collecting money to prevent and combat child cancer diseases...
... a global leader in household appliances...
... two providers of communications technology and services...
... a designer, engineer, manufacturer and distributor of outdoor power products...
... an investment company...
... a SME provider of online marketing through search engine marketing, conversion and lead generation...
... an e-commerce company providing payment services for online storefronts...
... an engineering group in tooling, materials technology, mining and construction ...
... an enterprise software corporation...
... a global provider of heavy trucks and buses, engines and services...
... a provider of assured, secure cloud services to the UK public sector...
... a global provider of renewable solutions in packaging, biomaterials, wood and paper...
... the leading university in technology and digital arts programmes...
... a provider of business software and services to more than 340 000 business in the Nordics...
... a producer and distributor of trucks, buses and construction equipment...
... the leading company in advanced mobile services...

Our businesses are profoundly different but deeply united by the need for clear roles and responsibilities, open cross-border data flows, balanced codified sanction guide lines, effective one stop shop and absence of overly prescriptive rules as fundamental conditions for long-term growth, competitiveness and prosperity, for both us and the economies in which we operate.

For further information please visit us www.europeandatacoalition.eu or contact us at info@europeandatacoalition.eu