EuroCommerce
THE RETAIL, WHOLESALE AND INTERNATIONAL TRADE REPRESENTATION TO THE EU

Draft EuroCommerce position on the European Commission proposal for a General Data Protection Regulation, COM(2012) 11

Draft Position paper

Date:	7 September 2012
Name:	Fatma Sahin, Adviser on Internal Market and Consumer Affairs
Contact:	T +32 2 737 05 96, sahin@eurocommerce.be

Interest Representative Register ID number: 84973761187-60

Introduction

EuroCommerce welcomes the Commission's efforts to provide a simplified and more harmonised framework for data protection while providing legal certainty for businesses and consumers. The current fragmented rules on data protection in the EU as a consequence of the Data Protection Directive (95/46/EC) created legal uncertainty for businesses and consumers. However, the proposal on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), published on the 25th of January 2012, introduces significant complexity and costs to businesses and industry.

Harmonisation of the data protection rules should increase competitiveness of business and facilitate cross-border activities. We welcome the territorial scope (Article 3) which will remove the possibility that businesses will set up in another Member State where the rules are more flexible and thereby put an end to forum shopping which has created competitive disadvantages for many businesses.

EuroCommerce supports the protection and free movement of personal data; however, any provision must be reasonable and proportionate to the aim pursued. We stress that where there is no evidence of need to change of what is currently applying well, it should not be changed. There are good provisions in the Data Protection Directive of 1995 and these should not be changed unnecessarily.

The draft Regulation will not only apply to the online world but it will also have serious implications for offline businesses. The proposal seems to focus mainly on social media and online networks without taking into consideration the negative side effects on businesses both offline and online. The main activity of a company is not data processing but retailing. The draft Regulation, as it currently stands, will hamper the daily business of companies. Many of the provisions are not practical and not necessary in order to provide a good protection of individual's personal data.

Regarding **delegated and implemented acts** (Article 86), EuroCommerce stresses that, in particularly taking into account the importance of harmonisation and legal certainty, there should be a clear distinction between technical content for which delegated acts can be justified and essential/fundamental content where it is necessary to regulate. Currently the number of delegated and implementing acts are too many; almost every provision allows the Commission to adopt delegated and implementing acts.

Delegated acts are regulated by Article 290 TFEU and shall only concern non-essential elements of the Regulation. The European Parliament and the Council will have the power to revoke delegated acts. This means that there is uncertainty on the exact content of many of the provisions and that the Commission can update provisions without having to review the Regulation.

Please find hereunder the main concerns of EuroCommerce members and our comments on the provisions which need to be revised in order the make the rules proportionate and practically possible for the whole society.

1. **Scope**

The scope of the draft Regulation is much broader than the current Directive. "**Personal data**" is being defined as any information relating to an identified/identifiable person (Article 4(2)). **Online identifiers** (IP addresses or cookies, identification numbers, location data etc.) are specifically mentioned as means reasonably likely to be used to identify an individual (Article 4 (1)). Online identifiers are, however, also mentioned as not necessarily being considered as personal data in all circumstances (Recital 24).

The current definitions do not provide a clear indication what could be considered as or how you can identify personal data. The definition should be clarified, in particular with the currently very high fines included in this proposal which are linked to any breach of data protection. Data should only be considered as personal data if the one processing it is reasonably likely to identify the data subject.

Therefore, EuroCommerce recommends to redefine "personal data" and "data subject", for example:

"Personal data" means data which relate to a living individual reasonably likely to be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller;

"Data subject" means an individual who is the subject of personal data; and "Data" means information held on computer or non-automated records structured in such a way which allows ready access to information about individuals.

EuroCommerce also recommends adding a definition for **"Anonymous data",** namely any data that has been rendered into a form which does not identify individuals. This includes data in the hands of a receiving party where they have no practical or legal means to access the 'key' held by the disclosing party.

2. **Personal data processing (Articles 5 and 6)**

Article 6 provides the conditions for lawful data processing. There is no reason why paragraph 4 of this provision does not include Article 6 (1)(f), "processing is necessary for the purposes of the legitimate interests pursued by a controller" while points (a) to (e) are included.

Therefore EuroCommerce calls for clarification of Article 6.

Some businesses collect data on other businesses which is to a large extent personal data. This holds true, for example, if the information includes data on individual owners or the management of businesses. Such data collection and processing requires a legal justification and today, such justification is provided by the so-called "**balance of interest clause**" in Article 7 (f) of the current Directive as implemented in national laws.

For example, credit information services collect data solely in the legitimate interest of third parties to whom the data are disclosed (their customers), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects. Credit reporting agencies do not have a contractual relationship to the person on whom they collect data. Much like the directory industry, the business of credit reporting agencies is based on the interests of the recipients of the collected data, i.e. on the interest of third parties.

The Proposal does not enable credit information services to rely on third party legitimate interests which are vital since it is in the benefit of their customers to receive information about the financial performance of their business partners. Without this, credit information services would only be able to rely on the legitimate interest which might not be sufficient to justify the data collection that is vital to perform their business. They would be unable to rely on other legal justifications such as consent as it would be impossible for them to collect the necessary consent declarations from all individuals involved. There is no clear justification to propose this major change to the balance of interest clause. Deleting the interests of third parties to whom the data are disclosed does not make the balance of interest clause more modern, flexible or business-friendly.

Therefore EuroCommerce recommends the following change in Article 6 (1) (f) of the Proposal:
"(f) processing is necessary for the purposes of the legitimate interests pursued by a controller or by a third party or third parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject […]"

Credit information services will store data for different purposes than that for which they were originally intended. Under the current Directive, a change of purpose requires a legal justification (Article 6 (1) (b) of the Directive). However Article 6 (4) of the draft Regulation explicitly excludes the balance of interest clause as a legitimate justification for a change of purpose. This means cases in which the change of purpose is legitimate and no overriding interest of the data subject applies, it will still be unlawful. There is no justification as to the reason behind this change. Credit information services must be able to rely on the balance of interest clause to legitimately collect data in order to function.

Therefore EuroCommerce recommends the following change in Article 6 (4) of the Proposal:
"4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis, at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract."

3. **"Consent"**

The draft Regulation introduces that businesses will need either to obtain the **explicit consent from consumers** or the **processing must be necessary** (Article 6(1). According to Article 4(8)) the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Highly significant is the tightening of the definition of consent which, where applicable, must be "explicit". This definition is narrowing down the possibility of rightful data processing and is different from the current Directive which requires an **unambiguous consent, which is more flexible. EuroCommerce recommends maintaining the current definition of consent.** Requiring an explicit consent for non-sensitive issues will result in a high administrative burden for businesses while it is not of interest to anyone. In cases of sensitive personal data (racial origin, political beliefs, religion, sexual orientation, etc.) we do support explicit consent.

It should be noted, that businesses since the 25th of May 2012 must comply with the Cookies/E-Privacy Directive (Directive 2009/136/EC), which states that data processing is only allowed on upon consent from subscriber or user concerned once they have been provided with clear and comprehensive information about the purposes of the processing, in line with the Data Protection Directive. Creating new requirements would force businesses to change their procedures and systems again creating extra cost and administrative burden. Therefore EuroCommerce calls for coherence with the Cookies/E-Privacy Directive in cases of cookies.

Mandating the use of explicit consent (opt-in) will have significant implications for e-commerce and online activities. For example, requiring an increased use of mechanisms on websites that indicate an individual has agreed to their data being processed.

Recital 25 helps as it states that consent can be given by a "statement or a clear affirmative action", including by ticking a box or by any other statement or conduct which clearly indicates the individual's acceptance. However, it also states that silence or inactivity should not constitute consent.

In context, failure to indicate objection should be part of the mechanism whereby a person indicates consent. For example, if a business provides a clear and prominent message, the fact that a person has not ticked a box should help establish that consent has been given. The crucial consideration is that individuals must fully appreciate that they are consenting and must fully appreciate what they are consenting to.

Furthermore, there are special concerns with Article 7 (4), in particular in the context of employment. It states that consent should not provide a valid legal ground for processing of personal data where there is a clear imbalance between the data subject and the controller. According to recital 34, this is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. It should be allowed to use collective agreements as a basis of employee data processing, to rely on employee consent to justify processing, or to modify some data subjects' right which would be difficult to comply with in the employment context such as the right to be forgotten.

Therefore, EuroCommerce recommends:

- Keep the current definition of the '95 Directive on consent and delete the word "explicit" in the definition of consent;
- Limit explicit consent only to sensitive issues such as religion, racial origin, sexual orientation, political beliefs, etc.;
- Coherence with the recently entered into force Cookies Directive;
- Collective agreements in the context of employment should be recognised as legal basis for data processing.

4. **Information to be given to consumers (Article 14)**

Businesses will have to provide consumers with more information than in the current Directive on data protection: the contact details of the business, the period of which the personal data will be stored, information on the right of erasure, information on the right to lodge a complaint and information on any intention of transfer to third countries. This information will be overwhelming for consumers.

With many more data subject interactions becoming electronic, slicker, faster, app-based, targeted towards small handheld devices, etc., this does not seem practical and will be very challenging to comply with.

Transparency is an important aspect of data protection. Over the years, however, the function of transparency has changed. In the early years of data protection laws, the information that data is processed electronically was important news for individuals. Today, it is common knowledge that data processing takes place in all aspects of commercial activities.

We recommend a general exemption with respect to transparency obligations in the B2B area.

Given that the most business relationships exist between companies and that the contact to the relevant individuals is often indirect, it is impossible to fulfil extensive transparency obligations vis-à-vis such individuals. In addition, anyone active in commercial activities has a relatively clear understanding of the data processing that happens. Since this relates to the business-related activities of the individuals, we do not see the justification for extensive transparency requirements.

EuroCommerce therefore recommends the following changes in Article 14 of the Proposal:

"5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject has already the information referred to in paragraphs 1, 2 and 3 or the information is commonly available or public knowledge; or

(e) the data is processed with respect to the professional role of the data subject in the context of commercial activities between businesses; or"

Furthermore, delegated acts could be useful in technical cases but not for setting up information requirements.

5. **The right to be forgotten and to erasure (Articles 17 and 19)**

In principle, we support the 'right to be forgotten' but it should be made subject to adequate safeguards for data controllers who have a legitimate business and/or legal reason to continue to process personal data.

Businesses are concerned about the obligation on data controllers to delete personal data on request of data subject in certain circumstances. The range of circumstances where the "right to be forgotten" arises is too wide and unnecessarily complex. In our view it **should only arise if the continued retention of the personal data would constitute a breach of the Regulation.**

For example, lenders rely on credit history data to assess a borrower's suitability. If the consumer has requested erasure of past data, then he/she will not qualify for a loan as the lender has nothing on which to base a credit decision. If he/she has used the right to be forgotten to conceal adverse but accurate data, then he/she may obtain credit which he/she is unable to support. **It is essential that Article 17 should not allow erasure of data processed for creditworthiness purposes.**

Furthermore, there is a direct conflict with other regulations. Less sharing of credit performance data conflicts with the requirement for organisations to lend responsibly under the Consumer Credit Directive, the future Directive on credit agreements relating to residential property and the Capital Requirement Directive. This would also impact regulated organisations attempting to comply with the customer due diligence requirements under the Money Laundering Regulations and impact other fraud prevention activities.

Credit granters would need to redevelop their credit decision models and procedures, with the significant costs. Also, credit decisions would be weakened, leading to further bad debt across the industry and/or less affordable credit to consumers and small businesses ,

We are also concerned that, in certain circumstances, a burden of proof falls on the data controller to demonstrate compelling legitimate grounds overriding data subject's interests, failing which they must delete the data. In our view the relevant test should be whether data controller ***has*** **compelling legitimate interests**, and not whether the data controller *can demonstrate* such interests.

There is an important exemption where the retention of data by the data controller is necessary ***"for compliance with a legal obligation to retain personal data",*** but we think that this is framed too narrowly. **It should be expanded to apply where such retention is necessary "for compliance with a legal obligation"** so as to cover situations where there is no express obligation to retain data but retention is implicitly required by, or ancillary for compliance with, any legal obligation.

The wider context here is that businesses routinely retain customer transaction and communications data in order to deal with regulatory investigations and /or legal claims which only arise in a small minority of

cases. The Regulation should not create a situation where it is unclear whether this practice is permissible if a customer complains and the retailer cannot clearly demonstrate an overriding justification for retention of the data for that particular individual.

Moreover, when a consumer requests to have his or her personal data erased, the business will be obliged to inform third parties to whom the data have been disclosed and will be considered **responsible for their publication afterwards** (Article 17(2). **This liability should be limited to data that businesses can control. Businesses should not be responsible for publication of data of which they have no control over (published by third parties).**

Therefor EuroCommerce calls for:

- **Adequate safeguards** regarding the "right to be forgotten";
- The "right to be forgotten" **should only arise if the continued retention of the personal data would constitute a breach of the Regulation.**
- Regarding **the burden of proof** that the relevant test should be **whether data controller *has* compelling legitimate interests**, and not whether the data controller *can demonstrate* such interests;
- "*for compliance with a legal obligation to retain personal data*", it should be expanded to apply where such retention is necessary "for compliance with a legal obligation;
- Businesses should not be responsible for publication of data of which they have no control over (published by third parties).

6. **Right to data portability (Article 18)**

Information is a powerful tool in empowering customers and driving competition. EuroCommerce fully supports helping consumers to make relevant and informed choices about the products and services they buy. However, we do not believe there is a case for regulatory intervention. Competition is strong and already delivering for customers, including by providing them with access to information to enable them to make informed choices. This makes regulation unnecessary, and the costs associated with it unjustified. Furthermore, unlike other sectors there is not a uniform approach to the holding of data, which means regulation of this sort would not be appropriate. We believe that this right would be better pursued through voluntary means.

The right to data portability is designed to allow individuals to change online services more easily by giving them the right to obtain a copy of their data from the service provider. For example, social networks and photo sharing websites allow people to store hundreds of photos, but if a user wishes to move these photos to a new service provider, the original company must comply where technically possible. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and, in particular, the copyright protecting the software (Recital 51).

This provision will have severe consequences on businesses and in particular for the offline world. It is uncertain whether the right of portability will mean that businesses will have to make all data available, including business generated data such as shopping history, customer behaviour and preferences etc. Will businesses be allowed to **decouple data** (dividing data which identifies a person from anonymous data, for example customer behaviour and shopping history) if it has been possible to identify the consumer, as for example with loyalty cards?

Not all data is collected by businesses in the same format or processed in the same way. An obvious consequence of this provision would be the work and cost involved in setting up such a service, particularly if required to provide transaction and derived data. According to Article 18 (3) the Commission may specify the electronic format as well as technical standards, modalities and procedures for the transmission of personal data by implementing acts. This would mean that businesses have to change the systems they have already invested in. Any unnecessary burden and costs should be prevented.

Given these considerations it is questionable whether this proposal really has a place in a piece of data protection legislation and is not, more readily, a competition issue. Applying a rule such as this would be a **huge disincentive to invest for companies** who aim to make better use of customer data to tailor products to individual needs. For example, a retailer running a loyalty card scheme to offer discounts and special offers. A competitor could potentially gain access to the IP and data processing capabilities that underpin such a scheme.

EuroCommerce calls for:

- Removal of this provision, failing which:
- Greater clarity on the scope of personal data covered (or excluded) by this provision;
- Limiting the application of this provision to the personal data detained by the social networks or to user generated data only and not operated data – data that has been provided voluntary.

7. **Measures based on profiling (Article 20)**

"Profiling" as used in the draft Regulation would seem to cover many routine data processing operations that may also benefit the individuals concerned. For example, operations to evaluate customers shopping behaviour and habits e.g. loyalty schemes, in order to provide the consumer a better service which is adjusted to his or her special needs.

It then places restrictions on the way that such profiling may be conducted, which will likely cause many companies to re-evaluate their data processing practices. Much of the terminology used in this article is unclear and likely to be difficult to implement in practice.

In general it is not clear what problems these restrictions are aimed at? If the key focus is social network websites, then the draft Regulation should reflect this, rather than impose? In particular it would be extremely helpful to understand whether the right to object to profiling is intended to apply to internet 'banner advertising'.

Moreover, this provision does not distinguish between data processing that identifies an individual and data processing that does not. Article 20 refers to every natural person rather than data subject. This broadens the application of the draft Regulation beyond its aim and therefore it needs to be adjusted in order to make it coherent with the proposal and with the current directive on data protection which refers to "data subjects".

Furthermore, the draft Regulation does not fit in the legitimate activity of credit reporting agencies within the range of credit examination. In this area it is usual and indispensable to represent the creditworthiness of a person or a company e.g. in a numerical value in order to give to the information user a first and fast to seize overview of the creditworthiness classification.

To allow this procedure also in future, however, the permission regulation in paragraph 2 (a) applying only for the conclusion or the fulfilment of a contract is perceived to be too narrow, because the customers of credit reporting agencies perform credit ratings also outside of existing or intended contractual relations. This provision must be extended so that the function of the credit reporting agencies remains possible.

EuroCommerce calls for:

- Change Article 20 (1) by replacing "every natural person" by "data subject";
- Clarification of what is meant by that the right to object only applies in respect of a "measure" which (1) produces legal effects to or (2) significantly affects the person in question;
- Clarification that certain profiling techniques and technologies used to manage, improve or customise services for similar customers are not prohibited by this Regulation;
- Clarification that the restrictions on 'profiling' apply only when processing of personal data is involved. We would assume this to be the case but it should be clarified, otherwise it would appear to go beyond the proper scope of the Regulation.
- Extension of the scope of Article 20 (2) (a) in order to include the normal functioning of credit reporting agencies.

8. **Notification of data breach to regulator & data subjects (Articles 31 and 32)**

The draft Regulation contains a general breach notification requirement applicable to all data controllers. Notification is to be given to the lead Data Protection Authority "without undue delay and, where feasible, not later than 24 hours after having become aware of it". Moreover, data controllers must also notify affected data subjects of a breach, but only when the breach is "likely to adversely affect the protection of the personal data or privacy of the data subject", and after having notified the Data Protection Authority, and then without "undue delay". Notification is not required if the data controller had implemented "appropriate technological protection measures" prior to the data breach.

The Commission's impact assessment suggests that the requirement to notify should begin to apply at "the moment when the data controller records in its files that an event that triggered a first investigation has been identified as a personal data breach" (Annex 5 at 84). Notice within 24 hours need not be given when the data controller provides a "reasoned justification to the Data Protection Authority as to why this time period could not be upheld".

The 24 hour requirement is unreasonable from a policy point of view and impossible to comply with in practice. Excessive notification of data security breaches has become a serious problem in other jurisdictions such as the US. The 24 hour requirement only creates incentives for companies to over notify, rather than properly assessing situations and working with regulators to minimise the damage.

In practice it takes several days or weeks to conclude even the preliminary investigation required to understand properly whether such an incident has occurred. We do not see the benefit of requiring businesses to rush this process to meet an arbitrary 24 hour deadline. It would often lead to incomplete and inaccurate information being provided to the relevant supervisory authority. This 24 hour deadline would also disrupt business operations and incur additional costs without real justification. **In our view the Regulation should be amended to make it clear that no obligation to notify the regulator arises until the data controller has had reasonable time to conduct an initial investigation and determine conclusively that a security incident had occurred**. This is because the necessary timing required will vary from case to case depending on the nature and severity of the breach. At that stage the data controller should be under an obligation to inform the supervisory authority without undue delay. We would prefer the legislation not to include any specified time limit but if this was unavoidable it should be more reflective of the genuine process involved, which would require longer than 24 hours for a meaningful (for consumer and business) investigation.

In addition, there is currently no threshold requirement and consequently the draft Regulation can be read as requiring notification for any personal data breach however small or trivial. This is unreasonable and disproportionate, and would involve data controllers in unnecessary costs. **A 'substantiality' or 'materiality' requirement is therefore needed by amending the definition of "personal data breach" to include such a requirement.** For example the UK Information Commissioner's Office (ICO) guidance on data security breach management makes it clear that notification is not an end in itself and that notification should have a clear purpose. Where a minor or trivial data breach occurs (e.g. copying in one person to an email in error) and consequences are not serious in nature, then it is unlikely that notification will serve any real purpose.

Therefore, EuroCommerce calls for:

- Removal of the '24 hours' requirement to notify the lead Data Protection Authority. Notification deadlines should be reasonable and proportionate to the gravity of the violation. "Without undue delay" is sufficient;
- Introduction of a 'substantiality' or 'materiality' threshold which will trigger notification to the lead Data Protection Authority.

9. **Impact assessments (Article 33)**

The draft Regulation introduces the **obligation for businesses to carry out an impact assessment** before processing operations that present specific risks. Under the current Directive it is left for the Member States to decide when a processing operation presents a specific risk. It is unclear what is considered as a specific risk to the rights and freedoms of data subjects. In general, this obligation could become very onerous, taking a great deal of time and incurring significant costs. It could also simply become a box checking exercise which is of very limited benefit to data controllers.

We are concerned about the obligation on data controllers to seek the views of data subjects (or their representatives). This is not reasonable, would be commercially impractical and it is also unnecessary. **EuroCommerce** recommends the removal of this requirement altogether.

Clarity should be provided on the circumstances in which a duty to conduct a Data Protection Impact Assessment arises. The Regulation currently says that such an Assessment is required where the processing proposed presents "specific risks to rights and freedoms" of data subjects, and then goes on to identify particular cases in Art 33(1). We are concerned that the first scenario (Art 33(2)(a)) is unclear and the third scenario (Art 33(2)(c)) would appear to require a new Data Protection Impact Assessment every time a new CCTV (security cameras) system is installed. The first should be clarified and the latter deleted.

10. **Data Protection Officer (Article 35)**

EuroCommerce welcomes the establishment of the Data Protection Officer (DPO) role on a formal statutory basis, but we have some concerns.

Further **clarity is needed regarding the requirement of data controllers to appoint a DPO who is (i) independent and (ii) reports "directly to the management"**. What does this mean in practice for a large company, and in particular how can an employee or contractor who will be subject to an obligation to act in the best interests of the data controller be genuinely 'independent'. **The independence obligation should be amended or removed.**

The provision that a DPO does not "**receive any instructions**" is unclear and seemingly at odds with the normal role of a data protection specialist who will advise on law and risk but leave the decisions to management of the business. We recommend that **this provision be removed and replaced with a requirement that a DPO expresses her honest advice / analysis and is not swayed by pressure from management in so doing**.

The **requirement to appoint a DPO for a period of two years, and the restrictions on termination of their employment, constitute an unnecessary interference with employment relationship** (with various employee rights enshrined in law).

The draft Regulation states that a DPO shall be designated for a period of at least two years and during their term of office may only be dismissed if they no longer fulfil the conditions required for the performance of their duties. It is not entirely clear what is meant by 'no longer fulfilling the conditions required' but, given that the proposal states the requirement for professional qualities and expert knowledge, it could be interpreted as meaning these.

What then if the DPO commits an unrelated offence, for example, is found to have behaved in a seriously dishonest way which would ordinarily lead to a decision to dismiss any employee? What if that DPO shows themselves to be very unreliable in attendance? What if they are injured such that they cannot attend work anymore; or mentally unwell to the extent that they cannot carry out their responsibilities without additional professional full-time support? Should the employer be barred from exercising its normal rights to address matters concerning conduct, performance or ill health?

This does not seem right and would not serve the purpose of protecting the data subjects. **EuroCommerce, recommends that Article 35 should be amended to be clear that an employer should only dismiss an employee with good cause, as permitted by Member State law.**

We are also concerned about the potential negative practical and privacy consequences of the DPO being required to publish their name and, to a lesser extent contact details. Unfortunately all large companies experience a handful of vexatious and unmeritorious consumer complaints. If the DPO has to disclose his/her name to the public the risk of distress or even physical harm being suffered by him/her in such cases is increased. **The draft Regulation should be amended to remove the requirement to provide the DPO's name and limited to provision of a single contact mechanism** (which could, for example, be a generic email address).

In addition, we have concerns about the 'right' of data subjects to "contact" the DPO on all issues related to processing of their data. If this right is intended to permit any disgruntled customer, employee or other third party to speak directly to the DPO then for large companies that hold data on millions of data subjects this will impose a huge administrative burden and will prevent the DPO from doing his or her 'day job'. Data subjects already have a wide range of rights under the draft Regulation and data controllers have obligations to establish mechanisms to comply and to provide contact details of DPO. **In light of this EuroCommerce recommends that this additional right "to contact" be removed altogether as it is unnecessary.**

11. **Data transfers to third countries**

There are three categories of mechanisms that may legitimise international data transfers:

- A Commission adequacy decision (Article 41);
- the use of "appropriate safeguards" (Article 42), including Binding Corporate Rules (BCRs) (Article 43); or
- the application of a derogation (Article 44).

The fact that adequacy decisions may no longer be subject to any kind of authorisation will reduce the administrative burden for data controllers in some Member States that currently require them.

Unfortunately, the draft Regulation does not discuss how adequacy decisions are to be issued, a process which is in need of reform.

Explicit legal recognition of BCRs is welcome, and the fact that Data Protection Authorities may no longer require authorisation of transfers using the EU standard contract clauses will be important for data controllers.

However, it is disappointing that transfers based on contract clauses will require further authorisation by the Data Protection Authority, which is bureaucratic and burdensome and likely to lead to unnecessary delays in business. A system of allowing self-assessment for international data transfers should be supported.

Furthermore, for international companies, easy and cross-border exchange of (personal) data within the organisation is of major importance. Today's organisational and working structures are very often cross-company. Virtual teams, consisting of members of several subsidiaries, are absolutely common in retail and various other industries. Therefore, it has to be ensured that it is possible to run a central storage of data in one subsidiary, to which the other subsidiaries – even from different countries – have access.

In Articles 40 and 41 and the following, the draft Regulation introduces a number of burdens for the internal use of data within an international cooperation and its subsidiaries. It seems as if the exchange of data within one company is treated like the data-transfer to third parties. The Proposed Regulation would burden the daily work of businesses with complex conditions, corporate directives and approval processes.

Therefore **EuroCommerce recommends** the inclusion of an intra-group exemption, making the data exchange within a company and its subsidiaries less burdensome and complex.

EuroCommerce calls for:
- Greater clarity on how adequacy decisions are issued;
- Removal of requirement to obtain authorisation from the Data Protection Authority where transfers take place on the data controller's own standard contract clauses;
- Inclusion of an intra-group exemption for internal use of data within international companies.

12. **Redress**

Organisations which aim to protect citizens' rights and interests will have the right to represent one or more citizens in a complaint with a supervisory authority (Article 73(2)). This provision **introduces a representative group action while no safeguards are provided**. **EuroCommerce strongly recommends** the deletion of this provision or to provide for safeguards and conditions under which this action would be allowed and lawful. Moreover, the representative entity should be identified.

Furthermore, enforcement is the task of the DPO and therefore it should not be allowed that anybody else can go to court on behalf of the DPO.

13. **Administrative sanctions/Fines (Article 79)**

Highly significant is the proposal for penalties and administrative fines, which elevates the significance of data protection so that it is on a par with other corporate compliance topics such as competition law, anti-bribery, and money laundering requirements.

The sanctions that may be imposed on data controllers under the draft Regulation are hugely increased over what was previously possible, and arguably disproportionate in relation to the breaches. They are to be imposed mandatorily for any intentional or negligent breaches of certain provisions of the draft Regulation, and are divided into three categories, ranging from up to 0.5%, 1% or 2% of a company's annual worldwide turnover respectively.

The Commission has suggested publicly that there is an exemption for a company's first violation, but in fact the text only gives Data Protection Authorities the power to abstain from a fine in cases where the breach is committed by a natural person processing data without a commercial interest, or by an organisation with fewer than 250 employees that processes personal data "only as an activity ancillary to its main activities". So in the vast majority of cases such exemption will not apply.

The wording in Article 79(1) that sanctions may be imposed by "each supervisory authority" suggests that in theory a company could be sanctioned separately by 27 different Data Protection Authorities for

the same breach if it occurred within each jurisdiction. Some of the grounds for which penalties can be imposed seem overly burdensome or unclear. For example, the fact that a sanction may be imposed for not "timely or completely notifying" a data breach to a supervisory authority or to data subjects seems unreasonable given that what constitutes "complete notification" is likely to be a matter of opinion. The text of Article 79 also obliges Data Protection Authorities to impose administrative penalties ("shall impose a fine") whereas it would be more appropriate to allow them to do so ("may impose a fine").

Whilst there is some contingency within the proposal to reflect the seriousness of the breach with the scale of the fine, linking this to the company's worldwide turnover seems disproportionate. It would seem fairer to link it to the turnover of the country or business unit where the breach occurred. Moreover, EuroCommerce would like to stress that retail and several other industries only achieve very low operating profit (EBIT) margins. In general, many companies have to work with between 1 to 4 % of their turnover. For this reason EU sanctions ranging up to 2 % of the global turnover would be completely disproportionate and would endanger the survival of numerous businesses.

Therefore, EuroCommerce calls for:

- More proportionate levels for fines (e.g. UK = £500.000 max);
- Making fines discretionary; not mandatory;
- Greater clarity on when fines may be imposed by a Data Protection Authority;
- Greater clarity on which Data Protection Authority can sanction a fine;
- Removal of sanctions for not "timely or completely notifying" a data breach.

EuroCommerce and the commerce sector

EuroCommerce represents the retail, wholesale and international trade sectors in Europe.
Its membership includes commerce federations and companies in 31 European countries.

Commerce plays a unique role in the European economy, acting as the link between manufacturers and the nearly 500 million consumers across Europe over a billion times a day. It is a dynamic and labour-intensive sector, generating 11% of the EU's GDP. One company out of three in Europe is active in the commerce sector. Over 95% of the 6 million companies in commerce are small and medium-sized enterprises. It also includes some of Europe's most successful companies. The sector is a major source of employment creation: 31 million Europeans work in commerce, which is one of the few remaining job-creating activities in Europe. It also supports millions of dependent jobs throughout the supply chain from small local suppliers to international businesses.