INSURANCE EUROPE MEMBERS' CONCERNS - EC PROPOSED GENERAL DATA PROTECTION REGULATION

I. Introduction

The following table is a compilation of the feedback received by members on concerns regarding the EC official proposed General Data Protection Regulation of 25 January 2012 and its impact on insurers. It includes analysis, suggestions and questions raised by members and occasionally divergent views on some issues.

This table is an internal document and it gives an overall perspective of different angles of the EC official proposed Regulation and its potential consequences for insurers. It is a basis for exchange of concerns within CEA members.

The table is divided in:

a) general remarks:

- Meeting conclusions were adopted
- Data sharing and fraud prevention
- Right to transmit personal data / transfer of data
- Direct marketing
- Anti-money laundering
- Joint data controllers
- Tightening the criteria for the adequacy of existing data for purposes of processing and
- Data processing in groups of companies and involving service providers

b) an analysis of specific articles, following the numbering in the official EC proposed Regulation.

Areas of concern	Members' analysis/ arguments/ suggestions/ questions
Data sharing and fraud prevention	There is a concern that changes to the EU data protection legislative framework may impact on the ability of insurers to share information to prevent fraud and other financial crime. Irrespective of the need to ensure appropriate consumer protection, which is understandable and welcomed, it is vital that the legislative framework recognises the need for organisations to share information for such purposes. Detecting and combating fraud protects honest consumers and it is in the overriding interests of society. It is therefore important that efforts to combat fraud are supported and explicitly recognised in the development and application of the law rather than being restricted. To be able to combat fraud, the insurance industry needs a legal ground for processing data concerning criminal convictions. The Regulation should also not prevent insurers from sharing / processing data relating to criminal convictions for the purposes of fraud prevention and / or detection as it is also an important part of the underwriting process. Premiums are calculated on the basis of risk and evidence shows that unspent convictions can indicate the likelihood of making a future claim. Restricting insurers' ability to use this information will impact on lower risk consumers. It should also be indicated here the need for a clear legitimacy for insurers to process personal data without any additional special restrictions, if such processing is connected with the protection of their legal interests, or the legal interests of third parties (including customers being data subjects). **In FIN** Under the current directive-based system, the Finnish insurers are able to maintain special shared registers for the identification of fraudulent claims as well as on known perpetrators of insurance fraud. The proposed regulation could possibly impose restrictions that will make it impossible to maintain the current regime. **In the UK** Reducing and deterring insurance fraud is a priority for the insurance industry. In 2010 UK general insurers detected 133,000 cases of fraud with a value of £919 million. But around £2 billion in insurance fraud goes undetected each year, adding, on average, an extra £50 a year to the insurance bill paid by every UK policyholder. This is why the UK insurance industry is investing around £200 million a year in tackling the problem and has a zero tolerance attitude towards insurance fraud. Insurers subscribe to a number of databases to detect fraudulent activity and ensure that the premiums paid by honest policyholders are commensurate with the risk. But, in return, policyholders have to accept that they must forego some privacy by

	allowing insurers to share information. For non-sensitive data, Clause 1(f), Article 5 'processing is necessary for the purposes of the legitimate interests pursued by the controller' may be intended to include data sharing for fraud purposes. We must ensure that this provision does allow us to share data for this purpose. However, the Regulation does not (outside of explicit consent) provide a similar right for sensitive data. CEA Members' suggestion There should be a specific exemption where processing is necessary for the purposes of preventing fraud or a particular kind of fraud. This exemption currently exists for in UK Data Protection legislation (schedule 3 7A).
Right to transmit personal data / transfer of data	Since personal data shall mean any information relating to a data subject, there might be a risk that even the undertakings' assessments of the clients is included in the definition of personal data. Moreover, the provisions on transfer of data might also present difficulties for the conclusion of the reinsurance contracts. CEA Members' suggestion It should be stated in the provision on the right to transmit data that data can be transferred only by the data subject.
Direct marketing	The possibility of direct marketing should be retained. It is therefore important to find a way to strike a good balance between data subjects' protection and economic interests. Notably, direct marketing of own products and services should be explicitly specified in the Regulation, as the legitimate legal basis for personal data processing. CEA Members' suggestion The formulation of German Data Protection Act (BDSG) in Section 28 par.3 may serve as an example.
Anti-Money laundering (AML) issues	**In PL** Currently, it is only life insurers that have to comply with the anti-money laundering and counter terrorism Act. Any additional requirements in connection with the processing of personal data in terms of ensuring compliance with the AML should not result in extending the obligations to non-life insurers. Such a change might lead to inconsistencies and additional costs for insurance companies.
Joint data controllers	CEA Members' suggestion A legal ground for the processing of data by joint controllers has to be introduced.
Tightening the criteria for the adequacy of existing data for purposes of processing	This is ordained in a way that results in the gathering of minimizing data ranges – and such request is inconsistent with the needs of insurance risk assessment, detection of fraudulent claims, and the requirements of the law on preventing money laundering and terrorism. Although it concerns mainly the data collection of potential customers in the form of detailed surveys, not only for insurance but also for other entities of corporate group (eg for a bank), which may result in restrictions to business insurance, and impairing the ability of adapting the offer to the actual customer's needs.

	The adequacy of the tightening of criteria should be widely consulted to prevent against extreme solutions leading to the inability to conduct proper risk assessment before entering into an insurance contract.
Issues concerning definitions used in the Regulation	CEA Members' suggestion ■ It is required to clarify all the new concepts concerning "sensitive" personal data. ■ It is also necessary to supplement the Regulation with all definitions that appear in its text or in its context, such as: security measures, marketing, direct marketing, marketing through electronic means. ■ An alternative is to refer to other EU regulations, where these concepts are already defined. ■ The traces of this approach are references in the Regulation's Explanatory Memorandum to use the technical standards of the ISO -27 000 series for the definition of "sensitive" personal data regarding health.
Data processing in groups of companies and involving service providers	CEA Members' suggestion The insurance business model requires a flow of data within insurance groups, between direct insurance and reinsurance companies and service providers. The insurers face practical problems concerning the consent of the data subject, eg as regards health data. Here as well, a specific legal basis for the data processing in groups of companies and with service providers, including the processing of health data, would have a positive impact on the insurance industry.
Article 4 par.1: Definition of data subject	Clarification is needed on whether the "data subject" definition includes the deceased or not.
Article 4 par.10: Definition of genetic data	The definition of 'genetic data' is much too wide and could potentially include information which is readily identifiable, such as for example gender. A definition of genetic should be an accurate description of genetic such as 'any data about an individual's gene patterns'. All in all, further assessment is needed to see how this definition would affect the insurance industry.
Article 5: Processing principles	All of the processing procedures must be demonstrably compliant with the Regulation. Questions How will this be interpreted? Will it vary from one country to the next? How is "demonstrable" defined? Does this mean that every step in the procedure must be elaborated on in detail? This would mean a considerable increase in the administrative burden. **In the NL** According to the current legislation, an audit and self-assessment are required in order to satisfy the provisions of the Dutch law on Data Protection *(Wet bescherming persoonsgegevens = Wbp)*. However, the insurer is at liberty to determine the manner in which this audit and self-assessment are carried out. In other words, there is a degree of flexibility in the implementation. Questions Can the proposed audit be linked to carrying out a privacy impact assessment (PIA)? This would reduce the burden associated with the process. How will this be applied to all the pending processing work?

Article 7: Consent	The proposed new definition of "consent" is narrow and problematic for the purposes of insurance business practices, as it excludes a consent being implied from other delegations of will and always asks for an explicit one. For instance, when a customer asks for a quotation, which by its nature requires personal data to offer an insurance product properly matching customers' needs, the customer's consent to process his/her personal data shall be allowed to be implied from his/her primary and explicit request for the quotation. Asking for an additional explicit (formerly unambiguous) consent for processing personal data, multiplies the costs (as all these documents have to be stored in insurers' IT systems) and administrative burden, without any real benefit for the customer as this additional request for consent is simply confusing. In labour law, consent as a legal basis for personal data processing should not be excluded by principle as it is also important for insurance business. For example, employee's consent is necessary for an employer to offer insurance products, such as occupational pension schemes or group insurance. CEA Members' suggestion ■ It should be ensured that the rules on consent are not unnecessarily burdensome on organisations or a barrier for consumers. For example regular payment of a premium should be sufficient to confirm consent where an insurance policy automatically renews**.** ■ Article 7 par.4 ■ It is also essential to remove the proposed exclusion of consent as a legal basis for personal data processing in all situations where there is a "significant imbalance in the form of dependence between the position of data subject and data controller". This can lead to invalidating any declaration of will issued by persons subordinated to employment or business relationships, regardless of whether there was a breach of their privacy, or even when giving consent was beneficial for subordinated persons. ■ This may also be used to invalidate data subject's consent that is necessary in order to offer group insurance. This kind of exclusion introduces an unacceptable legal uncertainty in the insurance business, and for that reason it should be removed from the Regulation's draft.
Article 6, par.5: Lawfulness of processing	**In the NL** According to the Dutch *Wbp*, third parties with a legitimate interest may process data. For example, the Dutch Association (being the third party) is carrying out research to gather statistics on customer service through surveys. If the proposed article remains in force, the above process would no longer be possible. The meaning of "legitimate interest" will be restricted, and since insurers are not mentioned in the proposed article, this might create obstacles to the insurance companies; marketing activities. Consequently marketing partnerships with third parties would no longer be possible.
Article 9: Processing of special categories of data/	■ Sensitive data categories This provision mainly concerns life insurance and data collected for the purpose of the conclusion of the contract.

collecting and processing health data	However, the extension of categories of sensitive data such as the image of a person may result in additional responsibilities for the non-life insurance as well. This will require increasing restrictions in data protection rules, and their synchronisation with the other already existing law, especially in subject coverage. In order for insurance undertakings to uphold actuarial principles and prevent erroneous payouts insurance undertakings must have the possibility to process sensitive data, such as data relating to health offences and criminal convictions. ■ Collecting and processing of health data The collection and processing of sensitive data, e. g. health data, currently requires the consent of the person who is the data subject. This is continuously posing major legal and practical problems to the different insurers such as life, health and accident insurers, but also third party liability insurers, who need such data either for the fulfillment of the insurance contract or for compensation of personal injury claims. This is acknowledged in the *"Advice paper on special categories of data"* of the Art. 29 Data Protection Working Party. In this paper the problem of insurers relative to the consent for the processing of health data is clearly pointed out (Point II.3.2.2) as well as a need for revision This becomes even more important if the legal provisions on privacy at European level should not envisage any more the "*per facta concludentia*" consent, especially in the field of services offered by supervised sectors, such as insurance companies. It is very difficult to predict what will be the final context of the Regulation – especially when EC according to article 81par.3 shall be empowered to adopt delegated acts for reasons of public interest in the area of public health. To a great extent it seems like the countries can maintain national rules concerning processing of personal health data. This will not result in a harmonisation of the rules within the member states. ■ <u>Article 9par.2(h) *(see link with article 81 below)*</u> Clarification is needed in order to understand what the "for health purposes" mean. Does it include medical advice, insurance purposes or not?
<u>Article 11:</u> Transparent information and communication	These obligations are too burdensome. To enable the data subject to exercise his/her rights, he or she only has to be informed about who has access to his/ her personal data and how to obtain further information. <u>CEA Members' suggestion</u> ■ Article 11.2 reads" the controller shall provide any information and any communication relating to the processing of personal data to the data subject in and intelligible form, using clear and plain language, adapted to the data subject [..]": Does this mean that insurance companies will be obliged to communicate with their consumers using the mother tongue of each consumer or may they use the language of the country they are residing? ■ What is exactly meant by "easily accessible policies"? When information is considered easily accessible and transparent? There is an information requirement for insurers laid down in Dutch Wbp. The question is whether or not a privacy

	statement is sufficient according to the proposed regulation? Or should the entire privacy policy be made accessible to clients? In the latter, this will probably not lead to increased transparency. It will definitely result in a considerable increase in the administrative burden for insurers. ■ The question therefore is how should the concept of transparency be interpreted? Dutch insurers already provide transparency in a variety of ways. For example, in the same texts included in policy terms and conditions which indicate which client information is processed and how this is done.
Article 15: Right of access	The right of access should be user friendly. However, it should be possible to charge a fee, as this helps to deter frivolous requests. In the UK, there is evidence that some requests to insurers are motivated by the intention to cause nuisance (for example following repudiation of a claim) rather than to confirm the accuracy of data held. It is also worrying that there are no restrictions on the number of times the data subject have the right to obtain information about personal data undergoing processing. CEA Members' suggestion Since it is administrative burdensome to provide this information there should be some form of limitation on the number of times it is possible to obtain the information Likewise, companies should be allowed to charge a fee.
Article 17: Right to withdraw consent/ right to be forgotten	■ Right to withdraw consent It must be designed in a way that takes into account situations where there is a contractual relationship between an organisation and an individual, and data are needed for the proper performance of the contract. Financial Services providers are also required to retain data to demonstrate regulatory compliance. Careful consideration of this is necessary as insurance policies cannot be fulfilled if key or all underlying data are removed. Withdrawal of consent, where it enables the operation of the contract, may lead to the automatic cancellation of the policy. This unintended consequence would not be in the best interests of the consumer. The simple withdrawal of data shall not lead to the termination of contracts.These rights should not lead to a "cold cancellation" of contracts by making the further fulfilment of an insurance contract impossible. Such behaviour against good faith has to be avoided. ■ Right to be forgotten The introduction of a "right to be forgotten" and the rigorous requirement of removing unnecessary data from data sets, including links to sources of information on the Internet and the data itself. This means additional costs for insurance sector, due to the need for significant adaptation of currently used IT systems, and additional costs associated with their maintenance to fulfil this requirement. Moreover, attention should be drawn to the possible conflicting legal obligations imposed on the insurer as the Data Controller. For instance, in some countries national law provides for long periods of retention of insurance data (which is also personal data), eg in the case of claims the limitation period can last up to 20 years, also increased by up to 6 years due to provisions of the tax law – for such long periods the data will be needed in an insurance company in a legitimate way, so it cannot be forgotten even when the

	data subject asks for it. Long enough retention periods are absolutely necessary in insurance to calculate risks properly. Accepting demands that the necessary personal data "be forgotten" clearly makes impossible basic insurance risk assessments such as *bonus-malus calculi*. Problems might also arise when transferring data to subsidiaries, or when needed for marketing and statistical reasons. This can significantly complicate and generate additional costs of insurance for large groups - banking. In the case of smaller insurance companies this also will involve additional duties - in case of making data available to another entity. To sum up, it is an important issue due to the fact that in many areas of the insurance business, consent is used as a legal condition for the lawfulness of data processing, and the possibility of its unconditional withdrawal has negative economic consequences for insurance companies, and for the customers as well (in situations where the rule of law require consent to acquire the data necessary for the proper assessment of insurance risk). Therefore this right should be subjected to such a limitation as not to be in conflict with insurance contracts underlying the subjected data processing, as the contracts are entered in good faith by both parties (insurer and client being the data subjects). ■ Clause 4(b) of Article 17 states that, instead of erasure, the controller shall restrict processing where the controller no longer needs the data for the accomplishment of its task but they have to be maintained for purposes of proof. However, it is not clear what the "restriction" of processing means, and the extent to which an insurer would be able to retain and use data in certain circumstances, such as for example, in defending legal proceedings, in responding to a complaint raised by a customer or alternative dispute resolution scheme, or in demonstrating regulatory compliance. ■ Paragraph 9(c) of Article 17 states that the Commission is empowered to adopt delegated acts for the purpose of further specifying "the criteria and conditions as regards personal data identified for the purpose of restricting its processing as referred to in paragraph 4". Greater clarity is required on the "criteria and conditions" referred to. Questions What does "restrictive processing" entail? Are insurers expected to maintain an unlawful processing of data? And if so in what kind of situation would this occur?
Article 18: Data Portability	The requirements on data portability might have implications for competition, raising also issues relating to standardisation and potential cost implications for businesses. Careful consideration needs to be given as to whether this could unintentionally require organisations to disclose their underwriting criteria. The requirements as written could have implications for the use of new technology which insurers may use to determine risk and premium pricing. For example, It is not clear whether under this process telematics data would be transferrable from one insurer to another at the request of the data subject The Article refers to a situation "where the data subject has provided the personal data and the processing is based on consent or

	on a contract". It is not clear to what extent telematics data has been provided by the data subject. Whilst it relates to the data subject, it is only produced because of actions (i.e. driving) undertaken by the data subject and analysis conducted by the insurer. If that data is to be transferred then the format could be prescribed. This would not sit comfortably with the different types of telematics technology. Most importantly this could result in insurers sharing information, for example on their underwriting criteria and product design. This could raise competition issues**.** Questions ■ How is "automated means" defined? For example does it apply to computer files only? Does this article imply that clients should receive a summary of all data processed regarding him/ her by an insurer? ■ What does the "right to data portability" entail? Does data portability refer to the requirement to use systems other than those used by controller. May enriched data automatically be sent to (for example) a competitor if teh client involved requested this? For example, a client indicates his or her desire to switch from insurer A to insurer B. Should insurer A be expected to supply ready-to-use data to insurer B? If that is the case, insurers would have to modify their systems to create a uniform format for data exchange.
Article 20: Profiling	Any rules on profiling should not prohibit or restrict risk-adequate rating, rate classification and risk assessments that are necessary for the purpose of premium calculation. An assessment of a policyholder's risk and profile is a core activity of the insurance business and the basis to calculate an adequate individual premium. We must ensure that the provisions in clause 2(a), Article 18 allow insurers to continue to use data in this way. Restrictions on profiling would have a significant impact on an organisation's ability to target marketing at their customers. Additionally, it should not affect the possibility of insurance companies to rate their customers in order to calculate their premiums. These measures are crucial for the insurance industry and are even required by insurance supervision law. This applies in particular to the profiling of children and the use of health data.
Article 22 (&25): Responsibilities of data controllers (DC)	Article 22 paragraph. 1 and 2: DC required adopting policies and measures for data protection in such a way as to prove that the processing is carried out in accordance with the Regulation. The assessment criteria shown in the paragraph. 2 is not an exhaustive list (wording such as: "in particular include"). Such wording of this provision does not protect DC against the recognition by the Supervisory Authority that the DC does not comply with obligations in this regard. In addition, Regulation shifts the burden of proof on the DC in this field. The requirement to carry out an external audit is a considerable increase of the controller's obligations. This article requires an extremely detailed documentation. The question is whether or not these requirements will lead to the desired effect. Does this result in increased efficiency? Does the mandatory appointment of a data protection officer actually prevent the misuse of data?
Article 26: Data Processor	Questions

	According to sub 4, in the event of a breach of contract, as a controller, you will have to rectify this with another processor being also a controller? What does this entail and how will this work in practice? Why is a shared responsibility necessary?
Article 31: Data breach notification (ok)	The proposals are disproportionate, will be unduly administratively burdensome for businesses and will not deliver benefits and for the consumer. Only breaches that pose a significant risk of harm to data subjects - and where data subjects should take action (e.g. to prevent identity theft) or remain vigilant – or a serious violation of their rights should be notified. Excessive notification requirements could lead to consumer apathy, as has been the case in the US. Timely notification of breaches that risk significant harm to the individual is vital however legislation should not prescribe response timescales but should encourage it to be conducted at the earliest opportunity and without excessive delay. Generally, the legally justified objectives are closely linked with the main objective of data processing and in insurance business they generally arise from duties or powers under the rule of law. Therefore, the rational solution is to limit this obligation to inform the data subject about who and on what legal basis has been granted access to his/her data, and how to get further information. **In the NL** Currently the Dutch personal data protection act is under revision. The establishment of a mandatory notification of personal data breaches is intended by the government. Our concern with the national as well as European mandatory notification is the following. Well-organised compliant companies will be able to identify and report data breaches at an early stage, whereas less compliant companies will not. This could result in a distorted picture of reality. According to the current Dutch Financial Supervision Act, insurers and some other financial institutions are exempt from the reporting requirement. Financial institutions under supervision of the Dutch Central Bank or the Financial Market Authority must report incidents to these supervisors. Financial institutions neither have reporting requirements vis-a-vis the Dutch Data Protection Authority neither to the data subject involved. Will the proposed regulation allow for a similar exemption?
Article 33: Impact Assessment (IA)	The wording data protection impact assessment is disputable, some less ambiguous terminology shall be proposed – borrowed from the risk analysis and information security. IT systems' security, including security of the data collected, granting access to data processing, copying or deleting, are and will always be one of the areas continuously monitored under the system of risk management in insurance companies. Therefore, the creation of the obligation to perform additional analysis of risk is unfounded. It significantly expands the obligations currently imposed on insurance companies as Data Controllers (DCs). Such an "impact assessment" duty is disproportionate to the objective pursued, since it conflicts with the principle of economic freedom and the right to make their own risk assessment by an entrepreneur. The obligation to publish these assessments endangers insurers' trade secrets, and may lead to forcing them to an unlawful disclosure of insurance confidential information. This rule also leads to extensive bureaucracy. The obligation even to seek the view of data subjects is disproportionate as it interferes with the entrepreneurial freedom to decide upon the business's policy by oneself. The publication of these assessments

	endangers business secrets. In what way can an IA be made public without disclosing commercial interests? Clarification regarding how and when an IA should be performed is desirable also in terms of consulting the subjects involved. In principle, carrying out an IA is a good initiative. It will support insurers in being compliant. At present, the Dutch PIA is being developed (but not completed yet) by VVO- NCW. Also a privacy scan is provided by Dutch Data Protection Authority. However, detailed provisions on the PIA as proposed by the EC can result in and additional administrative burden. Therefore, a certain degree of flexibility must remain regarding the implementation of the PIA.
Article 34: Prior authorisation and prior consultation	Article 34 paragraph. 2: the obligation to consult with the local Supervisory Authority before the start of data processing might create delays in the processing of personal data which will result in further delays connected with businesses processing data. This might result in losses incurring by businesses seeking to process the data.

Article 35: Data Protection Officers	The essential empowering of the Data Protection Officer (DPO) makes him in some extent a co-operator of the Data Protection supervisory authority. After this change, insurance companies will need:
	
	■ Provide DPO genuine independence in the exercise of his functions, positioning him as reporting directly to the Board. This means a fundamental change, because now a frequent solution is a DPO e.g. in an IT, Security, or Compliance department, as an employee of such department.
	■ Provide sufficient resources to the DPO, necessary for the implementation of an extended range of his tasks.
	■ Ensure the DPO's employment stability of his position - DPO will be engaged for a minimum of 2 years period, with virtually no possibility of an earlier release.
	■ One of many new DPO's tasks jobs will also be the duty to inform data subjects and Personal Data Supervisory Authority. Because this substantially increases the risk of occupational tasks and the scope of the DPO duties, an increase of decent salary expectations of this professional group and necessity to ensure its systematic training has to be also taken into account. Currently in the Polish law, DPO is regulated in one sentence, the draft Regulation pays him more than 2 pages, carefully specifying the terms of reference.
	■ The practical implementation of this idea (a stronger DPO) also involves some substantial risks:
	  ■ Complete information on the European Parliament latest changes can be found in the February Roadmap.
	  ■ The DPO is one of the DC tools, designed to ensure the efficiency of personal data protection. It should be remembered that all responsibility for proper data protection still lies with the DC, not the DPO.
	  ■ Weakening the position of DC to the DPO thus may lead to the opposite of the intended effect - weaken the entire system of protection of personal data in the insurance company.
	This is mainly a requirement for large organisations with more than 250 employees. It involves additional costs yet the strict regulations make it flexible.
	
	In the UK
	
	In the UK financial services sector, many firms already employ a DPO. The proposals may help to ensure that data protection is

	taken seriously by senior management. But any proposals should not necessitate costly and burdensome structural corporate changes where there is no commensurate consumer protection benefit. Further, there is a need to clarify what is meant by 'independent'. While DPOs try to remain objective and independent, the commercial reality is that the DPO must look for solutions that support corporate goals.
Article 38: Codes of conduct	The Code of Conduct for processing personal data by financial institutions (self-regulation) is applicable to all members of the Dutch Association. According to the proposed regulation this code of conduct can be maintained. However, modification of this Conduct will be necessary and will once again result in an increase in the administrative costs.
Article 39: Certification	This should not lead to a proliferation of quality marks and additional obligations in order to qualify. We would prefer correspondence to existing Dutch initiatives such as the Quality Mark for Client- Oriented Insurance (*Keurmerk Klantgericht Verzekeren)*.
Article 52 and 79: Powers of Data Protection Authorities	The Regulation, as currently drafted, does not consider the role of other regulators. Financial services firms should not face any threat of 'double jeopardy' as a result of dual regulation by the other national regulators and the DPA. In the UK, the Financial Services Authority already has the power to impose unlimited fines for data breaches, and these often prove substantial – running to several million pounds. Fines may also be imposed if the Supervisory Authority finds that, among others, documentation or technical and organizational measures applied by DC are not sufficient to fulfil its responsibilities under the Regulation. The concerns are related primarily to the fact that the Supervisory Authority becomes empowered to assess whether the documentation, data protection measures taken and the DC's conduct in data treatment are effective enough from the DC's perspective. As a consequence of a negative assessment, a heavy fine may be imposed on the DC.
Article 76: Class action	This mechanism may lead to a flood of unjustified claims against insurance companies. **In PL** There is a well-functioning consumer protection law, it has a separate independent supervisory authority (Insurance Ombudsman) and the Financial Supervisory Commission is also interested in the data subject's rights. Therefore, there is no real need for such class action suits. **In DE** There are already enough suitable measures on conflict resolution apart from individual claims such as ombudsmen and the well-functioning public control of insurance companies.
Article 79: Administrative sanctions	**In PL** The amount of financial sanctions is inadequate to the actual adverse effects on the data subjects. In particular, the penalty for

	violation of the data subject's rights is completely mismatched with economic realities of individual EU Member States. For example, a penalty of 250.000 Euros means that (given the national average gross salary in Poland at 3400 PLN and Euro exchange rate of 4.4 PLN) a person, to whom such a penalty will be imposed, will have to repay it, spending the entire gross salary for nearly 27 years. Taking into account the fact that there are also higher sanctions' thresholds envisaged, restrictions are not so much to make Data Controllers aware of costs of possible mistakes or errors, but rather to make them scary of personal data processing in general. **In DK** Under the Danish conditions, the suggested level of the amount is very high – and not in accordance with Danish traditions. The fines proposed would be a huge threat for the future existence of small companies.
Article 81: Processing health data concerning health *(to be read in conjunction with article 9par.2(h) and preamble 123)*	CEA Members' suggestion ■ Clarification is needed on whether insurance companies are included in the "health-care services" or not. This is very important because if insurance companies are covered by this provision, they also fall under article 9 par.2(h) and therefore they consent of the data subject is not needed by the data subject/ consumer. ■ the legal basis for processing personal data regarding health should be expanded so as to cover more data processing purposes, other than only those related to insurance claims, especially risk assessment and insurance fraud detection. More types of insurance than the health insurance system only: it should be legally allowed for all insurance covering risks associated with health status. The Regulation shall not instate artificial limitations which will contradict with legitimate needs of insurers. Insurers as being legal entities of public trust shall be allowed to process health related personal data in all processes where such data is required in order to conduct insurance business according to the rules of law, in line with customer's interests. It is in scope of insurance law and not of this Regulation to judge on what kind of health data specifically and for what exact purposes insures are allowed to process. The only specific provisions regarding health data processing by insurers in this Regulation may refer to its proper processing's security as it is required for highly sensitive data. Such an extension is very important to ensure the legal basis for personal data regarding health processing necessary for insurance purposes and to avoid conflicts with provisions of the insurance law. The legal basis should also be enlarged to more purposes of processing other than for settling claims and to more branches of the insurance industry other than health insurance.
Article 86: Delegated and Implementing Acts	The EC is empowered to adopt a big number of Delegated Acts and Implementing Acts. This makes it very difficult to get an overview of the level of harmonisation and the potential consequences in different countries. Though these envisaged empowerments of the European Commission allow much flexibility, this situation also bears considerable legal certainty. More direct rules within the future regulation are preferred than delegated and implementing acts.