Association of British Insurers 51 Gresham Street, London EC2V 7HQ Tel: 020 7600 3333 Fax: 020 7696 8999

Call for Evidence on the EU data protection proposals

The UK Insurance Industry

1. The UK insurance industry is the third largest in the world and the largest in Europe. It is a vital part of the UK economy, managing investments amounting to 26% of the UK's total net worth and contributing £10.4 billion in taxes to the Government. Employing over 290,000 people in the UK alone, the insurance industry is also one of this country's major exporters, with 28% of its net premium income coming from overseas business.

2. Insurance helps individuals and businesses protect themselves against the everyday risks they face, enabling people to own homes, travel overseas, provide for a financially secure future and run businesses. Insurance underpins a healthy and prosperous society, enabling businesses and individuals to thrive, safe in the knowledge that problems can be handled and risks carefully managed. Every day, our members pay out £147 million in benefits to pensioners and long-term savers as well as £60 million in general insurance claims.

The ABI

3. The ABI is the voice of insurance, representing the general insurance, protection, investment and long-term savings industry. It was formed in 1985 to represent the whole of the industry and today has over 300 members, accounting for some 90% of premiums in the UK.

4. The ABI's role is to:

   - Be the voice of the UK insurance industry, leading debate and speaking up for insurers.
   - Represent the UK insurance industry to government, regulators and policy makers in the UK, EU and internationally, driving effective public policy and regulation.
   - Advocate high standards of customer service within the industry and provide useful information to the public about insurance.
   - Promote the benefits of insurance to the government, regulators, policy makers and the public.

5. The ABI welcomes the opportunity to respond to the Ministry of Justice Call for Evidence on the EU data protection proposals.

Summary

6. Insurers recognise the importance of data privacy and take their responsibility for data protection seriously. It is important that data privacy laws strike the right balance between the rights of individuals with the benefits from insurers delivering services to meet the needs of their customers.

7. Being able to access, process and store personal data is central to insurers' ability to provide consumers with appropriate products at fair prices. Inability to use data effectively would almost certainly result in consumer detriment in the form of higher prices and / or under insurance.

8. The Commission estimates that European businesses will benefit to the tune of €2.3bn from the proposed changes. We question how these figures have been reached and do not

believe that harmonisation in the way proposed will deliver that magnitude of savings. The Regulation increases the number of requirements placed on business, however the proposals do not quantify the added cost of compliance. The added costs of compliance and financial risks will wipe out any potential savings and likely result in much higher overall burdens.

9. The Regulations, as they currently stand are not fit for purpose. Given the impact of the Regulation on UK business and consumers we urge the UK Government to ensure that sufficient time is taken to debate and refine the proposals.

10. We wish to emphasise the following key points. The data protection legislative framework:

- Must explicitly recognise the need for organisations, including insurers, to share information to prevent fraud and other financial crime. 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 each UK policyholder.

- Should reflect a pragmatic and proportionate approach to notification such that only serious or significant breaches are notified to the Data Protection Authority (DPA). Mandatory notification requirements are disproportionate, will be unduly burdensome for businesses and the DPA, and will not deliver benefits for the consumer.

- Should not prohibit the right for organisations to charge a fee for subject access requests (SARs), as this helps to deter frivolous requests.

- Must allow organisations sufficient time to respond to SARs rather than specify a time limit. The right of access requires a data controller to take account of many obligations and considerations when responding to a request. This includes locating the source of data, the form in which the information should be provided, redaction of third party data, the provision of health data or the application of legal exemptions.

- Should not go beyond data protection and security. The inclusion of an article on data portability is a substantive and significant addition to the legislation. The proposal clearly falls outside the scope of the legislation. The ability to change providers easily is a consumer and / or competition issue and should be dealt with under other relevant legislation.

Response to key issues

11. We have set out the ABI's initial views on the key EU data protection proposals. Our concerns are set out in priority order.

Data sharing and fraud prevention

12. We are extremely concerned 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. We support measures that ensure appropriate consumer protection, however the

legislative framework must recognise the need for organisations to share information for such purposes.

13. Detecting fraud protects honest consumers. It is important that efforts to combat fraud (which are in the overriding interests of individual consumers and of society as a whole) are supported and explicitly recognised in the development and application of the law rather than being restricted.

14. 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 each 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.

15. Examples of insurance fraud include:

    - Induced motor accidents - where an innocent motorist is forced to crash into the back of the fraudster's vehicle. Claims are then made against the innocent motorist, and these often include accounts of fictitious injuries from gang members, some of whom may not even have been involved in the accident. In many cases these criminal gangs have bogus claims running with numerous insurers at the same time.
    - Arson committed with the intention of submitting a fraudulent insurance claim.
    - Supplier fraud, where insurers receive bills for work that has not been done.

16. 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. For example, insurers will share data (on claims and polices) with the Insurance Fraud Bureau (IFB), a not for profit organisation funded by the insurance industry, specifically focussed on detecting and preventing organised and cross industry insurance fraud.

17. The IFB leads or co-ordinates the industry response to the identification of criminal fraud networks and works closely with the police and other law enforcement agencies. They have been responsible for numerous arrests and tens of millions of pounds of savings for the industry and ultimately the consumer. Such benefits would be lost if the Regulation prevented data sharing for these purposes.

18. For non-sensitive data, Article 6, Clause 1(f)[1] may be intended to include data sharing for fraud purposes. However, the Regulation does not (outside of explicit consent) provide a similar right for sensitive data.

19. **The Regulation should explicitly recognise the need to process data for these purposes through the inclusion of a specific exemption for both sensitive and non-sensitive data where processing is necessary for the purposes of preventing fraud or a particular kind of fraud.** This exemption currently exists in UK Data Protection legislation for sensitive data (schedule 3 7A). We suggest the addition of the following requirement

    (1) The processing—
    (a) is either—

[1] Article 6, Clause 1 (f) 'processing is necessary for the purposes of the legitimate interests pursued by the controller'

(i) the disclosure of personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

20. The Regulations should also not prevent insurers from sharing / processing data relating to criminal convictions for the purposes of fraud prevention and / or detection. The Regulations should also allow criminal convictions to be used for the purposes of risk pricing.

Case study 1: impact on data sharing for preventing fraud in the insurance section – Insurance Fraud Bureau

The Insurance Fraud Bureau (IFB) is a not for profit organisation funded by the insurance industry, specifically focussed on detecting and preventing organised and cross industry insurance fraud. Undetected general insurance claims fraud totals £2billion a year. This adds, on average, £50 to the annual costs individual policyholders face, each year.

The IFB uses data from a multitude of sources to identify patterns enabling insurers to find networks of claims that they would not otherwise be aware of. IFB receives data from insurers and public bodies, such as the police, and private bodies such as the Solicitors Regulatory Authority and other insurance sector partners.

Since its inception, this approach has resulted in 162 successful prosecutions amounting to a total of 136 years imprisonment. The IFB currently has 33 live operations with a total value of £59.5m.

Prohibition of data sharing of this kind would not be in the public interest as many more fraudsters would go undetected. This would have a direct cost to the insurance industry and to consumers as fraudulent claims would increase which will impact on premiums paid by honest consumers.

Case Study 2: Fraud and data sharing; example of an MIB fraud investigation

The example below sets out the importance of exchanging intelligence and information within the context of a fraud investigation and in compliance with the current data protection principles.

The Motor Insurers' Bureau (MIB) was established in 1946 to compensate the victims of negligent uninsured and untraced motorists. Every insurer that underwrites compulsory motor insurance is a member of MIB.

A number of cases were submitted to the MIB by a Claims Management Company (CMC). Concerns were raised when it was noted that the CMC was instructing a particular medical agency to arrange medical examinations of all claimants without prior reference to the MIB,

and that the same medical examiner was used on approximately 25 occasions.

As part of the overall investigation, claimants were interviewed and whilst the MIB noted that there were discrepancies between the content of medical reports and the statements of claimants.

An additional concern was that the surgeon appeared to have travelled considerable distances to complete medical examinations at the home of claimants during a two month period. MIB was concerned that there were unsatisfactory aspects to the medical reports.

In discussion with the fraud team of one of MIB's legal partners reference was made to an ongoing investigation into a medical agency. It became apparent that the investigation related to the same medical agency.

Under Section 29(3) of the Data Protection Act 1998 MIB formally requested information on their investigation and a similar request was received from the legal partner. It was quickly established that the medical reports were fraudulent. MIB handed the information over to the police for investigation.

Had MIB proceeded on the basis of the bogus medical reports, the compensation assessments would potentially have been inaccurate. In a number of cases the claimant would have received inadequate compensation since adverse and on-going injuries, or inability to return to work, were omitted from the bogus reports.

In addition, the medical agency would have directly benefitted from income estimated at £12,000 from the MIB alone.

Breach notification

21. Insurers take their responsibility with regard to data breaches seriously. They have internal processes in place to for identifying, recording, investigating and responding to any data breaches that occur.

22. We are strongly opposed to the proposals for mandatory notification of all breaches to the DPA within 24 hours. The proposals are disproportionate, will be unduly administratively burdensome for businesses and the DPA, and will not deliver benefits for the consumer.

    Under the Commission's proposals, DPAs will be swamped with notifications of trivial or inconsequential breaches. There will be circumstances where the breach poses little or no risk to the individual and notification would merely create an administrative burden for both the organisation concerned and the DPA. For example:

    - A customer address is incorrectly updated following an instruction from the customer. A letter containing marketing information is sent to the wrong address.
    - A customer data file is left on a desk when an employee goes home. The manager sees it and locks it away.

23. Excessive notification will distract DPAs from their important role of investigating serious breaches, and where necessary taking action. This is not in the public interest and undermines the principles underlying breach notification. Notification should have a clear purpose, whether this is to support individuals who may have been affected to take steps to

protect themselves, or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

24. We consider that 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 - should be notified to the DPA. We consider that the UK Information Commissioner's Office (ICO) current guidance on management of data security breaches strikes the right balance between protecting consumers and not imposing an unduly onerous administrative burden upon businesses or the DPA.

25. The target to report data breaches within 24 hours, or provide justification of why a breach cannot be notified with the time limit, is unrealistic. This poses the significant risk that data controllers focus more on notification than dealing with the breach itself. 24 hours is insufficient time for organisations to conduct the necessary investigation into the breach to ascertain its scale and impact and put a remediation action plan in place. For example, once a breach is identified the organisation will conduct an investigation to assess:

- The scale of the breach, including the number of individuals potentially affected.
- The impact of the breach – assessment of the risks to individuals / organisation.
- The action to be taken – for example changes to systems / processes, arrangements to enable an individual to protect themselves. For example offering appropriate insurance cover or protection to guard against credit card fraud or identity theft.

26. It should be noted that regulated financial services companies in the UK already have an obligation to notify those data security incidents to the FSA which may create a heightened risk of financial crime, or which affect the company's ability to provide adequate services to its customers and result in serious detriment to any customer, or have a significant adverse impact on the company's reputation. In practice, the company would also notify the ICO.

27. We agree with the ICO[2] that notification requirements should be 'without undue delay' rather than a stipulated timeframe. This is in line with the e-Privacy Directive approach and the approach set out for consumers in the new Regulations.

28. **The Regulation should reflect a pragmatic and proportionate approach to notification such that only serious or significant breaches are notified to the DPA. Article 31 (1) should be replaced with the following**:

    (1) 'When a personal data breach is likely to pose a significant risk of harm to data subjects - and where data subjects should take action to protect their privacy, the controller shall notify the data breach to the supervisory authority without undue delay.'

Rights of access - fees

29. An individual's right of access should be user friendly. We strongly oppose the removal of the right 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 rather than to confirm the accuracy of data held. For example, a SAR has arisen in the light of a dispute around the insurer's repudiation of a claim or the amount of a claim settlement. It is sometimes also used as a 'fishing expedition' by the individual or a claims management

[2] Information Commissioner's Office: initial analysis of the European Commission's proposals for a revised data protection legislative framework

company, in order to try to unearth some information in support of a claim or merely to cause nuisance by way of causing an undue administrative burden for the data controller. It is widely acknowledged that the current fee does not reflect the average cost incurred by the company, which is significantly higher.

30. **The Regulation should not prohibit the right to charge a small administrative fee for processing SARs.**

Rights of access - timescales

31. We are also opposed to the specification of a time limit of one month on the response to access request. We agree that data should be provided without excessive delay, however there must be sufficient time to collect all the data and conduct any required redaction.

32. The right of access requires a data controller to take account of many obligations and considerations when responding to a request. This includes locating the source of data, the form in which the information should be provided, redaction of third party data, the provision of health data or the application of legal exemptions. Therefore, there may be a considerable number of tasks that a data controller needs to complete within the regulatory timeframe. The Regulation does not appear to include any exemptions for legal professional privilege, management planning and prevention of crime. These exemptions are necessary to protect the data controller's interest.

33. It should also be borne in mind that a data controller has no control over the frequency or numbers of SARs that they might receive and, therefore, the availability of suitable resource. For example, Insurance Database Services Limited (IDSL) who manage the Claims and Underwriting Exchange and Motor Insurance Anti-Fraud & Theft Register (insurance fraud prevention databases), on average receive 70 SARs a month, and in extreme cases have recieved 300 requests in one calendar month. It is likely that the removal of the right to charge a fee for SARs will result in an increase in the number of vexatious or spurious requests. Add to this a shorter time frame to respond, and there will be costly impacts on business in trying to adhere to the proposed requirements.

34. The proposed timescales fail to take account of the size and diverse nature of organisations, and the different issues experienced in relation to the recovery of data from other organisations within the group or associated organisations. Such data may be held across many different locations. This could require data to be gathered from data processors and sub processors. The proposals also fail to take into account the complexity of some SARs, be it in terms of the volume or nature of information requested. For example:

    - An insurer receives a SAR from a customer who has held a life insurance policy with the firm for 20 years. They request 'all data' relating to them.
    - An employee makes a SAR which requires other employee email accounts to be searched for their personal data.
    - An employee makes a SAR for their HR file which is very large. The firm needs to consult with the individual's psychiatrist to ensure that disclosure would not be detrimental to their health.
    - A policy holder makes a claim for damage to buildings caused by subcontractors. This individual makes a SAR for all information held by the insurer on them. Whist many reports and conversations relating to the claim are not personal the policy holder's name is used in the naming of any correspondence / paperwork concerning the claim. As a

result this information must be retrieved and considered as part of the SAR. This data is not personal, but relates to the policy they hold and can include confidential third party reports. Determining what information can be disclosed is complex and takes time.

35. Insurers report that some SARs result in multiple boxes of information being provided to the individual. Each piece of data must be reviewed individually to identify whether there is any third party data, and in certain circumstances to check whether information should not be disclosed, as it could create a tipping off offence under anti-money laundering regulations. One ABI member has reported that a recent SAR has resulted in 3000 pages of A4 – all of which needed to be checked and where necessary have information redacted.

36. **The Regulation should require information to be provided 'without excessive delay'. The first sentence of Article 12 (2) should be deleted and replaced with:**

    (3) The controller shall inform the data subject without constraint at reasonable intervals and without excessive delay whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information.

37. There is inadequate flexibility within the legislation for circumstances where the individual is unreasonable in framing their request. A lack of information from the data subject can make it difficult to locate their personal data, particularly in circumstances where the individual is a former policy holder.

38. **Processing of a SAR should be conditional upon sufficient information having been provided to the controller to satisfy them of the identity of the data subject and to locate the information requested. This provision exists in the UK data protection legislation (Part 2, 7 (3)). The Regulation should include a requirement such as the one below**:

    Where a data controller—
    (a) reasonably requires further information in order to satisfy himself as to the identity of the person making a request under this section and to locate the information which that person seeks, and
    (b) has informed him of that requirement, the data controller is not obliged to comply with the request unless he is supplied with that further information.

39. **We believe the safeguards for data controllers, in cases where requests are manifestly excessive (Article 12, (4)) need to be strengthened. The Regulation should include the following requirements (as currently enshrined in the UK data protection legislation)** :

    (a) Where a data controller has previously complied with a request made under Article 14 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

    (b) In determining for the purposes of subsection (a) whether requests under Article 14 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

40. We are concerned about the inclusion of a requirement for organisations to provide SAR information in an electronic format (Article 12 (2)) where the individual requests it. As stated

earlier, SARs can be complex and result in significant volumes of data being provided. As with the proposed time limits, this proposal does not take account the many obligations and considerations required of a data controller when responding to a request. A requirement to send data electronically could be unduly burdensome on organisations.

41. Our members report that, apart from very specific circumstances, responses to SARs are usually paper-based and transmitted via recorded delivery or courier service. There are a number of issues associated with requiring such requests to be transmitted electronically:

    - Verification. Organisations must make sure that it is the genuine data subject making the request. There is concern that email addresses can easily be spoofed.
    - Security. There is an interception risk when data passes across the internet, regardless of interception or review within the data subject's home. Encryption is not an easy answer to this, as the sender and the receiver will not necessarily have the same encryption tools.
    - Not all data is held electronically. Providing information electronically would require documents to be scanned. This would take time and resource. Some documents could be electronically altered for redaction, but not all. If electronic redaction is not possible this would require information to be manually redacted, then scanned and sent.
    - Even where data is held electronically, it is not always in a 'sendable' format. For example, certain areas of databases may not currently include the function to extract the data in a report.
    - Large volumes of data. Many SARs are large and could cause system issues to the receiver, depending on the system they have and their individual settings. This could be assisted by splitting up what is sent – but again, this is more time-consuming than packing up the documents to send out by mail.

42. **The requirement to respond electronically should be removed from the Regulation**.

Data portability

43. The inclusion of an article on data portability is a substantive and significant addition to the legislation. The proposal clearly falls outside the scope of the legislation as it is not about data protection or security. The ability to change providers easily is a consumer and / or competition issue and should be dealt with under other relevant legislation at which point any data protection considerations can be taken into account.

44. We are very concerned about the inclusion of this proposal as it has implications for competition and intellectual property, it raises issues relating to standardisation and has potential cost implications for businesses. For example, this could unintentionally require insurers to disclose their underwriting criteria.

45. The requirements could have implications for the use of new technology which insurers may use to determine risk and inform premium pricing. For example, some motor insurers are investing in the development of new technology to monitor driving behaviour to lower premium prices for careful drivers ('telematics'). It is not clear whether under this article telematics data would be transferrable from one insurer to another at the request of the data

subject. The transferability of this data is an issue that should be dealt with any legislation that fully assesses the costs and benefits of such a requirement.

46. 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.

47. **Proposals on data portability do not belong in data protection legislation, accordingly Article 18 should be removed. If the proposals are taken forward, as a minimum safeguards must be included to protect intellectual property and commercially sensitive data**.

Right to withdraw consent/the right to be forgotten

48. The commentary surrounding 'the right to be forgotten' seems to stem from concerns relating to access to data in a social network context. We believe that it is more appropriate for any new right to be restricted to public online access to data in social networking sites. If this is approach is not adopted, the right of the data subject to withdraw their consent, or to be forgotten, 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 is needed for the proper performance of the contract.

49. Financial services providers are required to retain data to demonstrate regulatory compliance. As a minimum, such data must be kept for six years.

50. The ability for individuals to remove claim records would have high potential risk to insurers. As discussed earlier, insurers use and share data to prevent or detect fraud. One of the ways insurers detect suspicious activity is via previous claims history (multiple claims of the same nature, multiple claims featuring same parties, etc). Removing the ability to retain such data would seriously impinge upon detection.

51. Unless the 'right to be forgotten' is appropriately designed, there is a significant risk that dishonest individuals will exploit the system to remove their data for fraudulent intentions.

52. **Article 17 (3) should be restricted to public online access to data in a social networking context. If the Article is not restricted in this way safeguards must be put in place to ensure that data can be retained for regulatory and anti-fraud purposes.**

53. Careful consideration of the use of the right to be forgotten is necessary as insurance policies cannot be fulfilled if key, or all underlying data, are removed. Withdrawal of consent, where it enables the underwriting 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.

54. The proposals place the burden of proof on the data controller to evidence that explicit consent has been captured. It is unclear how this will interplay with the right to be forgotten, in that if the consumer has the right to be forgotten and have all their data erased, how will the data controller be able to evidence that consent has been legitimately captured, if that too has be erased? This would leave the data controller unable to defend any complaint relating to the capture of data.

55. 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. For example, in defending legal proceedings, responding to a complaint raised by a customer or through an alternative dispute resolution scheme.

56. **The regulation must include provision for the fact that some liabilities last long after a policy has ended.** For example subsidence claims or employer liability claims which require data to be held for much longer in the interests of the individual policy holder.

57. 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" that the Commission intend.

Profiling

58. Being able to access, process and store personal data is central to insurers' ability to provide consumers with appropriate products at fair prices. Inability to use data effectively would almost certainly result in consumer detriment in the form of higher prices and / or under insurance.

59. 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. There is a direct relationship between expected claims and the policyholders' profiled risk. An assessment of these risks is the basis of technical insurance risk and adequate individual premium calculation. It is important that the provision in clause 2(a), Article 20 allow insurers to continue to use data in this way.

60. We are also concerned that the Regulation as currently drafted will have a significant impact on an organisations ability to target marketing at their customers.

61. **We seek reassurance that Article 20 (3) will not prohibit insurers from processing data concerning offences or criminal convictions (with the individuals consent).** This is an important component of the underwriting process. Premiums are calculated on the basis of risk and evidence shows that relevant unspent convictions can indicate the likelihood of making a future or a fraudulent claim.

62. Restricting insurers ability to use this information will impact on lower risk consumers as it would inhibit the insurers ability to weight according to risk. This would potentially result in premiums rising for all policy holders. This would not be fair to the consumer and is no incentive on individuals to act responsibly.

Consent

63. We urge the Government to seek rules on consent that are not unnecessarily burdensome on organisations or act as a barrier for consumers. For example:

- If a policy holder gives their explicit consent at policy inception, regular payment of a premium should be sufficient to confirm consent where an insurance policy automatically renews.

- Explicit consent at policy inception should cover the transfer of data between insurer and reinsurer where the processing relates to the continued operation of the contract for which the customer has given their consent.

- Where a policy holder includes an additional driver on their car insurance, the policy holders consent to process the data should be sufficient under the law of agency. Requiring the insurer to speak directly to each individual would be inconvenient for the customer and unnecessarily time consuming. The same principle holds for other types of joint insurance policies.

64. In the UK, the majority of insurance is sold via an intermediary (e.g. brokers, banks independent advisors) or third parties. Insurers should not be required to re-confirm consent that the customer has already provided to the intermediary on the understanding that it would be used to obtain an insurance product. For example, a provider of group protection products, collects employees' membership details through the intermediary/employer on the basis of implied consent by virtue of the member joining the scheme. The intermediary has already gained the consent of the data subject. There is no direct contact between product provider and potential members. Requiring consent to be expressed explicitly at set up would significantly increase the administration burden of the employer and also increase the scheme administration costs of the provider. This would increase the administrative burden on the consumer also and make it more time consuming.

65. We seek clarity as to how the requirement for explicit consent would apply to data collected prior to the rules coming into force. Could this data still be processed and how would this be regulated, if run in parallel with the new requirement for explicit consent.

66. We are also unclear how the requirements on explicit consent interplay with the e-Privacy Directive, particularly the 'soft-opt in' option for email marketing to customers. We believe this option should continue to be valid.

67. The level of information required to satisfy requirements for consent must be proportionate. It is not clear whether the proposals could embrace the concept of layered privacy notices. The Regulation requires increasing amounts of information to be provided to the individual, for example in fair processing notices. There is a risk that individuals will be bombarded with information which they will not read, increasing consumer apathy. The proposals should embrace the concept of layered privacy notices.

68. **The Regulation should include an exemption, similar to Section 35 Data Protection Act, covering disclosures required by law or made in connection with legal proceedings. The following should be added to Article 6**:

    1. *Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.*

    2. *Personal data are exempt from the non-disclosure provisions where the disclosure is necessary—*
        (a) *for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or*
        (b) *for the purpose of obtaining legal advice,*
        (c) *or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.*

Articles 53, 78 and 79 Powers of Data Protection Authorities

69. We support DPAs having effective sanctions at their disposal where the oversight framework has a risk-based approach, focussing priorities on areas where there is a real likelihood of serious harm to an individual or society at large. Any duplication of oversight should be for a specific purpose and not lead to a disproportionate additional administrative burden on insurers.

70. The Regulations, as currently drafted, do 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.

71. **As a minimum, the Regulation should include requirements for DPA to establish Memoranda of Understanding with regulators setting out how they will work together to ensure there is no overlap of roles and that organisations are not subject to overly burdensome regulation. The DPAs and other regulators should be required to consult with key stakeholders in the content of the any memoranda**.

72. We believe proposed level of fines are disproportionate. For example, given the imposed time limits for responding to SARs, a fine of up to 0.5% annual worldwide turnover (which would run into millions for some insures) for responding a few days late, where there is no impact on the individual, is draconian. Additionally the Regulation does not define what is meant by an 'enterprise'. It is unclear whether this relates to a legal entity or a group of companies.

73. We agree with the UK ICO that there should be a demonstrable link between the breach in question and the impact on data privacy.

74. **The levels of fines are disproportionate and should be revised. The test for whether a fine is warranted, and if so the level of fine, should be demonstrable link to the impact on privacy associated with the breach**.

75. **The Regulation should clearly define 'enterprise' for the purposes of the imposition of sanctions and fines**.

76. With regard to Article 53 (Powers of DPAs) we would not expect the Regulations to change the current UK legislative provisions for the ICO to access premises for the purposes of a data protection investigation. We seek confirmation from the Ministry of Justice that this is the case.

Data Protection Officers (DPO)

77. In the UK financial services sector, many firms already employ a DPO.

78. 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. We agree with the ICO that DPOs need not necessarily be mandatory.

79. We do not agree with the minimum term appointment of a DPO for 2 years. We do not think a regulation on data protection should seek to specify employment terms and conditions.

Careful consideration is needed as to whether this would conflict with an employee's rights under employment legislation, for example, or an employer's flexibility to reallocate resources and/or remove underperforming personnel.

80. 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.

81. The Regulation should not require the mandatory appointment of DPOs or specify a minimum term of employment.

Other comments

Definition of personal data and data subject

82. There are issues around the interpretation of the definition of 'personal data'. We advocate a narrower definition of personal data.

83. The term 'natural person' is not defined within the Regulation, or comprehensively in other pieces of law in the UK, to satisfy that it only relates to living individuals. There is a need to make a distinction in terms between 'Natural Person' and 'Deceased Natural Person'. Additionally, when an individual, sole trader or partnership is operating in a business capacity this should not constitute personal data.

Health data

84. The proposed requirement in the proposed Regulation on handling health data is not specific on the required safeguards. Article 81 states that the processing of health data must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests. It is not clear if this means that the processing of health data remains an issue for Member State law, or if there will be additional EU-level proposals. In addition, the term "health services" should be defined in detail and it should be specified that insurance data is a required element in providing health services.

Compliance obligations

85. The standard for the legitimate interests condition in the Regulation is set at a much higher level than it is currently, requiring data controllers to document their legitimate interests and to explicitly inform the individual of what these are. This would be quite an onerous requirement. There will also be additional burdens on organisations in respect to requirements for extra documenting of processing activities and the requirement to provide more fair processing information including storage information, the source of the info. This would mean a major overhaul of privacy notices, documentation, and websites.

Association of British Insurers
March 2012

For further information contact:
Jennifer Will
Policy Advisor, Conduct Regulation
Financial Conduct Regulation Team
jennifer.will@abi.org.uk
Tel: 020 7216 7688