ePrivacy Directive: circumstances, procedures and formats for personal data breach notifications - Public consultation

[Respostas da APDSI - 8 de Setembro de 2011]

INTRODUÇÃO

A APDSI (Associação para a Promoção e o Desenvolvimento da Sociedade da Informação) agradece a oportunidade de comentar as questões relacionadas com as circunstâncias, procedimentos e formatos das notificações de violações de dados pessoais, considerando que a introdução desta obrigação constitui uma importante medida para proteger a privacidade e segurança dos consumidores.

A APDSI é uma associação que tem como missão a promoção e o desenvolvimento da Sociedade da Informação e do Conhecimento em Portugal, partilhando as preocupações da Comissão Europeia relativamente à necessidade de criar um quadro legal e procedimental harmonizado, evitando assim diferentes critérios e procedimentos de notificação de violações de dados pessoais no espaço europeu.

As respostas abaixo reflectem a posição da APDSI relativamente às questões colocadas pela Comissão Europeia, tendo em consideração o texto da Directiva ePrivacy (Directiva 2009/136/CE do Parlamento Europeu e do Conselho Europeu, de 25 de Novembro), na medida em que a mesma ainda não foi transposta para o ordenamento jurídico Português.

COMENTÁRIOS

Nota: ECP = *Electronic Communications Provider*

2. CIRCUMSTANCES OF PERSONAL DATA BREACH NOTIFICATIONS

2.1. Notifying the national authority

Question 1: Does your organisation handle personal data breaches?	Não. A Directiva ePrivacy ainda não foi transposta para o ordenamento jurídico português, pelo que ainda não existe obrigação de notificação de violações de dados pessoais.
Question 2: If yes, how does your organisation handle personal data breaches currently, and how does it comply, or intend to comply, with this new obligation? What procedures does it have in place? What would be examples of the most common types of personal data breach?	N/A

2.2. Notifying the subscriber or individual

Question 3: In your view, what types of breaches would adversely affect the subscriber or individual? In what kinds of cases has your organisation notified the subscriber or individual so far, or received such notifications?	Existem vários exemplos de violações que potencialmente poderão afectar negativamente os dados ou a privacidade do assinante ou utilizador. Desde logo, qualquer violação que possa resultar no roubo ou usurpação de identidade, poderá afectar negativamente os dados ou a privacidade do assinante ou indivíduo. A APDSI gostaria, no entanto, de salientar o Roubo de Identidade que é, sem dúvida, o *issue* mais importante a considerar, sobretudo porque permite aos autores de tal violação levarem a cabo inúmeros actos que podem comprometer seriamente o assinante ou o utilizador das comunicações electrónicas. Por exemplo: exploração de dados de saúde que estejam residentes ou transitem nos

	sistemas de um ECP específico, exploração ilícita de dados de uma organização no sentido de fazerem chantagem ou espionagem, etc.
Question 4: What are the most common cases where the subscriber and individual would not be the same person or entity?	Os casos mais comuns são: • indivíduos dependentes de alguém: Crianças; Idosos; indivíduos com necessidades especiais (doentes; invisuais; etc.); • indivíduos que representem legalmente terceiros (com Procuração, etc.); • clientes empresariais. A existência desta possibilidade do assinante e o indivíduo não coincidirem significa que deverá ser clara, para efeitos relacionados com proteção de dados pessoais, quem é a entidade responsável pelo tratamento, a fim de se apurarem responsabilidades em caso de violação de dados pessoais.

2.3. Exception relating to technological protection measures

Question 5: What are examples of technological protection measures that can render data unintelligible?	A APDSI considera que deverá ser estabelecida a necessidade de implementação de sistemas tecnológicos para *encryption* forte (no armazenamento e na transmissão) de voz, dados e imagem. Esses sistemas devem ser explorados e monitorados pelos ECP de forma organizada, devendo ser revistos e actualizados periodicamente face a avaliações de risco feitas oportunamente. Os ECP devem implementar processos organizativos internos (regras, procedimentos, etc.) de controlo sobre os acessos aos dados, assegurando-se que são usados esquemas fortes de registo de *audit trails*. O cumprimento desses processos internos deve ser muito rigoroso.

Question 6: In your view, what should be the criteria and methods for assessing their sufficiency? At which stage of the notification process should this be examined?	O *assessment* deverá ser efectuado caso a caso, consoante o tipo de dados e a natureza da violação de dados pessoais. Os principais critérios a considerar (e que devem ser explicados às partes envolvidas aquando do estabelecimento de contratos de serviços) são: • Se o valor atribuído aos dados for ELEVADO: A divulgação e/ou uso não autorizado da informação pode ter grande impacto na actividade do indivíduo, da sua família, do seu círculo social e profissional, facilitando disrupções significativas na sua vida e/ou causando perdas financeiras • Se o valor atribuído aos dados for MODERADO: A divulgação e/ou uso não autorizado da informação não afecta seriamente a actividade do indivíduo, da sua família, do seu círculo social e profissional, podendo facilitar perturbações significativas na sua vida. • Se o valor atribuído aos dados for BAIXO: A divulgação e/ou uso não autorizado da informação não afecta (para além de simples incómodo) a actividade do indivíduo, da sua família, do seu círculo social e profissional. Aquando da contratação dos serviços o assinante deve indicar ao ECP quais os dados que são, na sua avaliação, sensíveis e deve poder actualizar essa avaliação junto do ECP sempre que considerar oportuno. O processo de notificação deve ser examinado nas suas fases inicial e na final.

2.4. National authority requiring notification of individual

Question 7: Has this happened in relation to your organisation? If yes, what were the circumstances, timeframe and exchanges with the provider or authority? If not, can circumstances be envisaged where this power would need to be invoked?	Não. Uma organização da sociedade civil, especialmente actuando no domínio da protecção dos direitos do cidadão, deverá ter meios para impelir a autoridade nacional a agir sempre que entenda que esta não está a desempenhar adequadamente o seu papel.

2.5. Interests of law enforcement authorities

Question 8: How should the legitimate interests of law enforcement authorities be taken into account, and how should this affect the two requirements to notify breaches?	Por norma os direitos legítimos de cidadão não podem ser prejudicados. Eventuais situações de excepção só devem poder ter lugar por acção judicial e sempre no quadro da Constituição e das leis nacionais.

3. PROCEDURES FOR PERSONAL DATA BREACH NOTIFICATIONS

3.1. Notification deadline – 'undue delay'

Question 9: What should "undue delay" mean in the context of notifying national authorities? What would be the most effective and realistic approach, taking into account issues such as consumers' needs and administrative burden?	O prazo de notificação deverá ter em consideração diferentes factores, desde logo o tipo de dados em causa e a complexidade da violação, na medida em que o ECP poderá levar algum tempo a reunir a informação. Em todo o caso, e da perspectiva da defesa do interesse dos consumidores, os ECP deverão notificar a ocorrência no menor período de tempo possível. A APDSI sugere as seguintes *guidelines*:

	• Se o valor atribuído aos dados for ELEVADO: A primeira notificação de acesso indevido aos dados deve ser feita, de forma sigilosa, à Autoridade e ao assinante e/ou indivíduo imediatamente (com urgência). • Se o valor atribuído aos dados for MODERADO: A primeiranotificação de acesso indevido aos dados deve ser feita à Autoridade e ao assinante e/ou indivíduo (de forma sigilosa), imediatamente (com rapidez). • Se o valor atribuído aos dados for BAIXO: A primeira notificação deve ser feita à Autoridade e ao assinante e/ou indivíduo, assim que for possível (num prazo de tempo razoável). A notificação deve por norma ser feita por forma electrónica, devendo evitar-se a adopção de procedimentos morosos e burocráticos no cumprimento da obrigação de notificar as violações de dados pessoais. Em casos em que estejam em causa dados relativos a volumes significativos de assinantes e/ou indivíduos, devem ser utilizados os órgãos de comunicação social para a notificação.
Question 10: What should "undue delay" mean in the context of notifying subscribers or individuals? What would be the most effective and realistic approach, taking into account issues such as consumers' needs and administrative burden?	Cf. Resposta à questão 9
3.2. Means of notification	
Question 11: Which communications channels should be used for notifying	Commummente a todos os ECP deverão ser seguidos procedimentos estabelecidos e validados pela autoridade nacional.

national authorities? What would be the most efficient way of reducing administrative burden for all parties?	No sentido de assegurar níveis adequados de sigilo, as notificações são feitas electronicamente usando soluções tecnológicas e organizativas de *encryption* e com certificação. Em casos de grande severidade, nomeadamente quando estiver em dúvida a integridade dos sistemas de comunicações, podem usar-se vias alternativas.
Question 12: Which communications channels should be used for notifying subscribers or individuals? What would be the most efficient way of reducing administrative burden for all parties?	É muito importante que seja assegurada formalmente a recepção da notificação pelo assinante e/ou indivíduo – sobretudo para que ele possa desencadear rapidamente as acções que tiver que fazer para mitigação dos danos reais e potenciais decorrentes da exploração indevida da violação de dados pessoais detectada. A notificação deve, por norma, ser feita por forma electrónica, devendo usar-se meios alternativos na medida do adequado. Em casos em que estejam em causa dados relativos a volumes significativos de assinantes e/ou indivíduos ou em que os próprios canais de comunicação elctrónica estejam comprometidos, devem ser utilizados os órgãos de comunicação social para a notificação dos indivíduos / assinantes. Outra alternativa possível será a comunicação através do website do ECP. Para efeitos de notificação, os ECP devem dispor de bases de dados permanentemente actualizadas com dados de contacto desses assinantes. A este respeito, a APDSI alerta para a dificuldade prática dos ECP notificarem os indivíduos afectados, na medida em que, não tendo qualquer contrato com estes, não terão naturalmente os seus dados de contacto.
3.3. Procedure for an individual case	
Question 13: For an individual case of data breach, how long does it take to	Sugerimos que a Comissão emita orientações sobre o assunto. O tempo de demora variará de caso para caso, dependendo do tipo e natureza da

gather all necessary information, and what information should be gathered at first?	violação de segurança e da complexidade do caso.
Question 14: What information should be provided to the authority/individual, and at which stages?	A definição da informação a fornecer deve ser harmonizada a nível europeu. Um assinante deverá ter o mesmo tipo de tratmento, independentemente da região ou do país em que o serviço foi contratado.
Question 15: What kind of feedback and follow-up should the provider and national authority expect from each other?	As autoridades nacionais deverão emitir *guidelines* de forma a que os ECP adoptem as medidas necessárias e evitar a ocorrência de violações de segurança. Caso uma violação ocorra, as autoridade deverão dar orientações aos ECP sobre a forma como as notificações deverão ser efectuadas, assim como quanto às medidas a adoptar para minimizar o impacto negativo de tal violação. Da perspectiva dos ECP, devem cooperar com as autoridades nacionais, disponibilizando a informação necessária e efectuando follow-ups periódicos quanto às medidas adoptadas na sequência de uma violação de dados pessoais. Assim, todos os intervenientes no processo devem cooperar no sentido de garantir interesse e a protecção do assinante e/ou indivíduo.

4. FORMATS FOR PERSONAL DATA BREACH NOTIFICATIONS

Question 16: What should be included in the notification to national authorities? Where possible, please indicate a "minimum" and "maximum" list of elements.	Em termos gerais, a notificação às autoridades competentes deverá conter a seguinte informação: (i) Descrição da violação; (ii) Medidas adoptadas para resolver/solucionar a violação;

	(iii) Comunicações aos clientes (se aplicável); (iv) Descrição de medidas adoptadas para evitar semelhantes problemas no futuro.
Question 17: What should be included in the notification to subscribers or individuals? Where possible, please indicate a "minimum" and "maximum" list of elements.	A notificação aos assinantes e/ou indivíduos deverá conter, pelo menos, a seguinte informação: (i) Data estimada da ocorrência (ii) Natureza da violação (iii) Dados afectados, incluindo volumes (iv) Que medidas o assinante e/ou indivíduo deve tomar (v) Que procedimentos foram accionados pelo ECP para proteger o interesse do assinante e/ou indivíduo Não havendo razões de natureza de segurança, não é razoável considerar-se que há limite máximo para a informação a fornecer.
Question 18: What kind of standard formats does your organisation use for breach notifications?	N/A
Question 19: Are there examples of best practice from other fields?	N/A
Question 20: Would it be feasible to have a standard EU format for notifications, and if so, what form should it take? Would this reduce or add to the costs of notification?	Sim. O formato deve ser estabelecido ainda que como orientação. A APDSI considera que essa standardização é fundamental e que desse facto não resultarão custos adicionais.

5. ADDITIONAL ISSUES

5.1. Inventory of personal data breaches

Question 21: Which elements should be included in the inventory of personal data breaches that providers are to maintain? Where possible, please indicate a "minimum" and "maximum" list of elements.	Se não houver razões de segurança, não é razoável considerar-se que há limite máximo para a informação a registar.
Question 22: Should there be a common format, and if so, what?	Sim, como *guidelines.*
Question 23: Which parties should have access to the inventory? What would be the most efficient way to allow national authorities access to the inventory?	O ECP, autoridade nacional e entidades com mandato legal para o efeito deverão ter acesso ao registo das violações de dados pessoais. Devem contudo ser assegurados processos técnicos e organizativos para que haja um controlo restrito e que sejam registados todos os acessos efectuados. Qualquer intervenção sobre os registos só deve ser feita mediante autorização específica da autoridade nacional. O acesso a estes registos pela autoridade nacional só deve se feita pelos seus elementos *in loco*, isto é, não deve ser permitido acesso remoto aos mesmos.

5.2. Audits by national authorities

Question 24: What is your organisation's experience so far with audits? In which circumstances and when should audits take place?	N/A As auditorias devem ser feitas regularmente e também em situações excepcionais.
Question 25:	Sim, a APDSI considera benéficos os esforços de harmonização nesta matéria.

Should there be a common EU format for audits, and if so, what?	Para as auditorias regulares é conveniente procurar-se um formato que seja tão comum quanto for possível. Pelo contrário, para as auditorias não regulares, as quais são motivadas por situações excepcionais, não será razoável a sua standardização.

5.3. Cross-border breaches

Question 26: Has your organisation dealt with a cross-border data breach before? If so, how was it resolved? In general, what are the frequency and circumstances of these cases, and what would be the most effective way of dealing with them?	Não.

5.4. Notification of risk of security breach

Question 27: Is there a need for harmonisation of national measures relating to this provision?	Sim. A APDSI considera benéficos os esforços de harmonização nesta matéria, minimizando-se assim o risco de divergência de procedimentos ao nível europeu.

5.5. Relationship with security breach notifications under Article 13a of the Framework Directive

Question 28: How will your organisation handle incidents that might be subject to the notification requirements under both Article 4 of the ePrivacy Directive and under Article 13a of the Framework Directive? Are there any internal procedures for informing national competent authorities other than the one responsible for notifications of personal data breaches under Article 4 of the ePrivacy Directive?	N/A