BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31(0)6 3964 2738
E rejo.zenger@bof.nl
W www.bof.nl

Bank account 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

European Commission
Policy Development Unit (B1), BU33 7/40
DG Information Society and Media
B-1049 Brussels
Belgium

Re
Response to the consultation on data breach notifications

Datum
Amsterdam, 9 September 2011

Dear Sir, Madam,

1. Dutch digital rights organisation Bits of Freedom would like to respond to the public consultation of the European Commission on “the circumstances, procedures and formats for personal data breach notifications”. Bits of Freedom defends freedom of communication and privacy of internet users and has significant experience maintaining a list of data breaches in The Netherlands for the past one and a half year. Bits of Freedom will consequently focus its response on the aspects most relevant for the internet user, but will also discuss the issue of data breaches from a broader perspective.
2. In short, the purpose of a personal data breach notification is to protect individuals, empower organisations which protect these individuals and gain insight into and awareness about data breaches. Notification obligations should thus apply to all sectors and should be effective, in timing, method and scope. Furthermore, notification to a public registry should provide sufficient information to allow individuals, media and policy makers to analyse the breaches. We explain this below.

The purpose of data breach notification is to protect individuals and gain insight

3. Personal data breaches come in various shapes and forms, and it is therefore difficult to provide a comprehensive definition. The ePrivacy Directive appears to provide a workable starting point, although this definition is too narrow. We will in this document define this as a breach of security which could lead to accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure of personal data (“**data**

breach"). In other words, the organisation entrusted with personal data for processing has lost control over the personal data. This thus includes potential breaches, in order to make the notification obligation less reactive and provide individuals and organisations a better opportunity to minimise damage. When an organisation becomes aware of a potential data breach, it should inform those whose data has been affected and a central authority as soon as possible ("**notification**").

4. The purpose of such a notification is to empower individuals, organisations and the government:

    - The main purpose of such a notification is to enable individuals to take all necessary actions to limit the undesirable effects of such a breach. For example, many people use the same username and password for accounts with several online services. If these have been disclosed for one account, the individual could, after notification, change these for other accounts. If notified, an individual will also become more alert to, for example, unauthorized changes in his account, or identity fraud and take action. In addition, users in some cases will be able to claim damages if the organisation responsible for the data breach can be held liable.

    - The second purpose of such a notification is to create awareness among individuals, organisations and governments of the risks associated with the increasing number of databases storing personal data, especially online. This is important, as an ever-increasing part of our lives takes place online and more sensitive data is stored in databases.[1] Online storage allows data to be cost effectively processed and shared, but the effects of a breach in centralised databases are also more severe. In addition, centralised databases are highly attractive for criminals, which makes the protection of these databases even more difficult. The effects and interactions between leaks and the reuse of this data in other contexts are very complex. Reporting and feedback through notifications should create insight in this complexity and connectedness.

    - As a result of such awareness, organisations will improve the security of their IT-infrastructure. Organisations will be more motivated to take the security measures necessary to prevent data breaches, if they are obliged to make breaches public.

    - Lastly, a public registry of data breaches provides organisations, policy makers and other stakeholders with statistical data on the nature and extent of these breaches. The information will firstly be helpful for organisations processing personal data to determine which measures must be taken to protect personal data and to limit the negative effects of security breaches. The analysis of the data compiled at such a registry also allows for fact-based decisions in law-making. Lastly, the public registrar would also be a valuable source of information for IT-security firms and academic researchers.

5. In order to meet these goals, a data breach notification obligation must adhere to a number of requirements.

1 In a study commissioned by the Dutch data protection authority CBP it is estimated personal data of the average Dutch civilian is stored in between 250 to thousands of databases. This number is higher when people are more active online or if they are part of particular groups, e.g. people in debt or chronically ill. This study can be found at: https://openaccess.leidenuniv.nl/handle/1887/15888

Notification obligations must apply to all sectors

6. Any data controller that is aware of a potential breach of personal data under its responsibility should be subjected to this obligation. This obligation should not be limited to specific sectors, as is currently the case with the personal data breach notification in the ePrivacy Directive, which is limited to the electronic communication sector only.

    - The problem of unauthorized access or unauthorized disclosure is not limited to a specific sector: it is inherent to the processing of personal data. Any organisation processing such data is prone to breaches of security protecting the personal data. This is demonstrated by the list of data breaches that are known to have taken place in the Netherlands in the last one and a half years, as compiled by Bits of Freedom.[2] We have attached a list of high-profile examples in the **appendix**. The list contains incidents in a wide range of sectors including education, finance, medical, governmental and law enforcement. It shows that the problem of data breaches is not limited to one particular sector. This underlines the need for a notification obligation covering all controllers and processors of personal data.

    - Secondly, such an approach causes inequality amongst organisations processing personal data and this might lead to unjustified discriminatory economic conditions for organisations offering essentially the same services (for example: social network providers and internet service providers).

    - Thirdly, the consequences of a data breach are similar, regardless of the sector the organisation operates in. For example, leaks of credentials could in all sectors lead to identity fraud. And a leak of personal medical data is harmful, regardless of whether the leak originated at a medical organisation or as a result of the interception of internet traffic.

    - Fourthly, limiting the scope of this notification obligation would severely harm the usefulness of the central registry as a source for supporting material for good policy making.

    - This view is widely shared by stakeholders and experts. The European Parliament proposed – later deleted – amendments to the directive, widening the scope to providers of information society services such as online banks and retailers. The EDPS calls for a wider scope in its second opinion of June 2009. The Article 29 Working Party has voiced its support for the European Parliaments position of the scope during the legislative process. Concerns on the limited scope of the obligation were also raised on a national level. Amongst others, the Dutch government, the Dutch data protection authority CBP, a public prosecutor and a number of members of the Dutch parliament called for a wider scope of such an obligation. No good argument has been put forward to restrict the obligation to the telecommunications sector.

Notification obligations must be effective in timing, method and scope

7. The primary goal of the notification obligation is to provide transparency and to minimize the negative effects for victims of personal data breaches. An individual is only able to take all the

2 See http://www.bof.nl/category/zwartboek-datalekken/

necessary steps to limit damages if he or she is informed adequately and completely:

- Measures to limit the damage are effective only when taken as soon as possible. The time between the actual data breach and the measures taken by individuals must be as short as possible. Hence, it is of the utmost importance that the data controller notifies the individuals immediately after becoming aware of the breach. Because the timing of the notification to affected individuals is crucial, the controller should give notification to individuals a higher priority than notification to the national registry. Delaying the notification should only be possible in exceptional cases, e.g. when the security of the system is not yet restored or when a competent and substantiated request by law enforcement agencies investigating the breach has been received (which demonstrates that disclosure would harm the investigation). The organisation should of course also take into consideration preparations to adequately respond and reduce collateral harm that may ensue for publicizing this particular breach. When considering a delay, the organisation should always firstly consider the interest of the individuals whose data is involved.
- The notification method should be effective. The selected method should thus reach all victims and should be reliable. The data controller should always attempt to contact affected individuals by means of personal communication (e.g. by e-mail, or in case of a smaller number of individuals, by phone). There should be no exceptions, even if such a notification yields an administrative burden on the organisation. Where technically possible on the basis of the data already available, the organisation should verify that the notification has been received. Additionally, a message hard to overlook should be posted on the website of the organisation. Only if the organisation is unable to identify a significant part of affected individuals or is unable to contact them by means of personal communication because it doesn't have any contact data, should it resort to publishing a mass notification in the mainstream media. The choice of the medium should be based on effectiveness. For example, if the data breach affects younger people, notifications using messages or advertisements on frequently used websites should be preferred over a financial newspaper. The decision regarding the medium used for notifying should be reported to the national data protection authority. If an organisation decides to deviate from these principles, it should notify the competent national data protection authority immediately. This allows for the authorities to promptly decide differently and overrule the decision of the organisation.
- To correctly assess measures to be taken, individuals must be informed with all relevant details. A notification to victims should at least include: (i) a simple *and* a comprehensive description of the security breach, (ii) the possible consequences for the victims, (iii) details on the protective measures taken by the organisation, (iv) the suggested countermeasures for the individuals to take (i.e. changing passwords, etc), and (v) contact information for inquiries. When sending a notification, organisations should take measures preventing the facilitation of phishing (where criminals send such a notification in order to convince the victim to provide its credentials). Furthermore, organisations should not be allowed to include marketing information or sales offers in the notification. In relevant cases, it could be

considered to oblige organisations to also inform victims of any judicial recourse they might be able to take, for example in order to claim damages.

- The ePrivacy Directive currently requires data controllers to inform victims only when the breach is likely to "adversely affect" the personal data or privacy of an individual. This is a problematic standard, as it is quite difficult to assess whether a certain breach – in combination with future breaches or future technologies – will affect the privacy of an individual. If an organisation decides not to notify affected individuals because it expects no negative consequences for them, it should notify relevant national data protection authorities of that decision immediately. This allows for the authorities to promptly decide differently and overrule the decision of the organisation.

Notification to a public registry should inform individuals, media and policy-makers

8. A public registry with information on data breaches ensures transparency, which is useful for several reasons. It allows others than the data protection authorities to determine the nature and the extent of personal data breaches. It allows people to complain to governmental authorities or media when disturbed about a particular high volume of leaks or extensive leaks. It allows media to further investigate specific data leaks and investigate sectors or organisations that have a relatively high number of leaks or leaks of highly sensitive data. In addition, civil organisations would be able to perform their own analysis and to verify the analysis of the data protection authorities. As a result, legislators and policy makers will be able to learn from the possible causes of data leaks and take appropriate measures to counter them. It could be considered to create an EU-wide public registry, especially for EU-wide breaches.

9. A notification to a national data protection authority should at least include (i) a description of the breach itself, (ii) the number of individuals affected, (iii) the type of data that was lost, (iv) the method of notification of victims, (v) the protective measures taken by the organisations, (vi) the countermeasures suggested to the victims and (vii) whether the data that was leaked is comprehensible for someone with state of the art knowledge of information security methods (i.e. technologies to decrypt information). In addition, an organisation should also inform the authorities what possible consequences or opportunities for abuse are created as a result of the breach.

Breaches of critical infrastructure

10. Lastly, we would like to draw your attention to the recent security breach at Dutch certificate-provider Diginotar. Diginotar is one of the hundreds of certification authorities on which the authenticity and confidentiality of internet traffic to a large extent depends. An investigation into the breach demonstrated that Diginotar was already aware of the breach for several weeks, but decided to keep the breach secret. As a result, false certificates have been issued and used for several weeks to intercept internet traffic of Iranian users. In addition, after Diginotar made the breach public and an extensive investigation into the breach was initiated, it turned out that it could not be excluded that certificates used by the Dutch government were also fraudulently issued. The Dutch government decided to switch to certificates provided by a different

organisation with far-reaching implications for the operations of the Dutch government.

11. This incident leads us to conclude that a security breach notification obligation – i.e. not necessarily relating to personal data breaches – is also necessary for certain sectors. Diginotar should have been obliged to immediately report the incident, as the security of hundreds of thousands of individuals as well as Dutch government communications was at stake. The same might apply to software being used by millions of people to scan viruses or a widely deployed operating system. Article 13a of the Framework Directive could provide a useful starting point for such an obligation. The obligation could be restricted to security breaches in vital or critical infrastructure. The European Commission should explore the parameters and boundaries of such an obligation urgently, as the Diginotar incident demonstrates.

Conclusion

12. We trust this provides you with all the information you require. Should you have any further questions, please do not hesitate to contact us. If possible, Bits of Freedom would like to remain informed on the further steps of the European Commission in this field.

Sincerely yours,

Rejo Zenger

Selection of significant Dutch data breaches in the last 12 months

Bits of Freedom since approximately one and a half years maintains a list of personal data breaches in The Netherlands which are known to the public. The real number of incidents is likely to be bigger: it is likely that most incidents are not reported, and even if they are, do not receive attention from the media. The list demonstrates that all organisations processing personal data are vulnerable to breaches. It also shows there's a wide range of causes. Sometimes it is the result of some technical problem, but most frequently, the breach is caused by insufficient security measures.

The following is a list of some the significant breaches of the last 12 months. The complete list of all known breaches is available on the website of Bits of Freedom.[3]

- In October 2010 a website processing financial information of users proved to be badly secured and allowed anyone to access nearly 9,000 files with personal data. The website provides a tool to users to manage their financial administration and view their financial situation. To do this, users upload their bank transactions to the website. The information that was leaked included an overview of more than one million banking transactions with a total value of 200 million euros and an average of 640 euros a transaction. Most of the transactions included identifiable information, such as as name, address, account number and recipient.
- In another incident (in December 2010) Excel files with the usernames, passwords and email addresses of 63,000 customers of an energy company were freely accessible to internet users. The credentials could be used to log in to the personal section of the customer at the website of the energy company. When logged in, one had access to the customers profile, including identifying information like name, address, invoices, details on the customers energy usage and other information.
- Using social engineering, a journalist of a Dutch national newspaper was able to get hold of the medical dossier of a well-known soccer player. Apparently, a single phone call was enough to obtain the complete medical dossier including details of an MRI-scan of the injured player. The CD with the information was conveniently sent to an address of the researching journalist. This incident took place in December 2010.
- A Dutch public TV-broadcasting organisation dissolved in 2010. Its database was apparently forgotten about until it was discovered to be insufficiently secured this summer. As a result, the entire member administration of the organisation became publicly available. Identifying information including name, address, bank account numbers, IP-addresses, usernames and passwords of about 153,000 members were accessible.
- Due to technical problems, users of the website of a Dutch national bank were shown the information of other customers. The mix up allowed 900 customers to freely browse through the personal information of another account. This incident took place in April 2011.

* * *

3 See http://www.bof.nl/category/zwartboek-datalekken/.