693/14/EN
WP 213

Opinion 03/2014 on Personal Data Breach Notification

Adopted on 25 March 2014

Executive Summary

In this Opinion, the Article 29 Working Party provides guidance to controllers in order to help them to decide whether to notify data subjects in case of a "personal data breach". Although this opinion considers the existing obligation of providers of electronic communications regarding Directive 2002/58/EC, it provides examples from multiple sectors, in the context of the draft data protection regulation, and presents good practices for all controllers.

While notification to the competent authority is required for all data breaches under directive 2002/58/EC, this opinion analyses personal data breaches requiring notification to data subjects and presents what the controllers could have done in the implementation of their system to avoid the personal data breach in the first place or, at least, what measures could have been implemented in the first place to exempt the controller from notifying the data subjects.

The opinion also provides answers to some of the main questions regarding personal data breaches and the application of Directive 2002/58/EC.

1. Introduction

A "personal data breach" is defined by Directive 2002/58/EC in Article 2 (i) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."

Directive 2002/58/EC (and the proposed European data protection regulation) requires personal data breaches to be notified to the competent national authority. Considering this notification, the details of the information to provide are available in the Annex I of Regulation 611/2013.

When the personal data breach is likely to adversely affect the personal data or privacy of a data subject[1], the data controller shall also notify the data subject of the breach without undue delay[2].

Directive 2002/58/EC, as well as the Regulation 611/2013, contain an exemption on the notification requirement to data subjects if the data have been rendered unintelligible. If the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures to render the data unintelligible to any person who is not authorised to access it[3] and if those measures were applied to the data concerned by the security breach, then notification of a personal data breach to a data subject shall not be required[4].

The *raison d'être* of this exemption to the notification of individuals is that appropriate measures may reduce the residual privacy risks on the data subject to a negligible level. A confidentiality breach on personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified to the authority. Nevertheless, if the confidentiality of the key is intact, the data are in principle unintelligible to any person who is not authorised, thus the breach is unlikely to adversely affect the data subject and therefore doesn't need to be notified to the data subject.

However, even when data is encrypted, a loss or alteration can have negative effects for data subjects when the data controller has no adequate backups. In this case notification to data subjects should still be required even with encryption protection measures in place.

Therefore, it is important for controllers to be proactive and to plan appropriately. Article 17 of Directive 95/46/EC, as well as article 4.1 and 4.1.a of Directive 2002/58/EC, provide that controllers must take appropriate technological and organizational measures to 'ensure a level

[1] We use in this opinion the term "data subject" as defined in the Directive 95/46/EC. In the context of the Directive 2002/58/EC, this corresponds to "subscriber or individual".

[2] In Directive 2002/58/EC and Regulation 611/2013, notification to the authority shall be done no later than 24 hours after the detection of the personal data breach, where feasible, extensible to 72 hours in some cases. The notification to the subscriber or individual shall be made without undue delay (in the sense of Article 2(2) of Regulation 611/2013) after the detection of the personal data breach. Notification to the data subject shall not be dependent on the notification to the competent national authority.

[3] Directive 2002/58/EC, Article 4(3); Regulation 611/2013, Article 4(1) ; General Data Protection Regulation, unofficial consolidated version after LIBE Committee vote provided by the rapporteur, Article 32(3).

[4] Note that, if the key is later compromised, then all past breaches that were not notified on basis of the secrecy of the key, will have to be notified.

of security appropriate to the risk' represented by the processing. To this effect, it is important to have an appropriate risk management framework in place, presenting the minimum elements that such an approach should have and also providing a set of minimum appropriate technical and organizational controls, that the controller may define, and with a particular focus on those controls rendering data unintelligible when needed. Companies should also define in advance appropriate plans to deal with personal data breaches, which can ensure that they respond quickly and effectively to a personal data breach.

When Article 17 has appropriately been complied with, i.e. before setting up the data processing, the risks related to a personal data breach will have been considered and reduced beforehand. In such cases, personal data breaches may happen more rarely and may have fewer consequences on the data subjects. Since notification to data subjects is not required when the breach does not adversely affect the personal data or privacy of the data subjects, or when appropriate technological protection measures were applied to the data concerned to the breach, the best way to avoid having to notify data subjects is to integrate appropriate privacy safeguards in the projects where personal data are being processed.

Notifications to data subjects should be made without undue delay[5] and shall not be dependent on the notification of the personal data breach to the competent national authority. The data controller should bear in mind that, even if it is not a criterion to decide whether or not to notify individuals, one of the primary benefits of the notification is to provide data subjects with the necessary information in order to reduce adverse effects arising from the circumstances of the breach. Where there is doubt in the mind of the data controller regarding the likelihood of adverse effects on the personal data or privacy of the data subjects, he should err on the side of caution and proceed with notification. In addition, account should be taken of the possibility for competent authorities to request notification to individuals after further assessment of the notification.

This opinion proposes a **non-exhaustive list of examples where data subjects should be notified**[6]. We examine each personal data breach through the three classical security criteria: the term "availability breach" will thus correspond to the accidental or unlawful destruction or loss of personal data, "integrity breach" to the alteration of personal data, and "confidentiality breach" to unauthorized disclosure of, or access to, personal data. The opinion then provides **general guidance** on cases not requiring notification. Finally, it **discusses the main issues** that controllers may encounter while considering whether or not to notify data subjects.

[5] In Directive 2002/58/EC and Regulation 611/2013, notification to the authority shall be done no later than 24 hours after the detection of the personal data breach, where feasible, extensible to 72hours in some cases. The notification to the subscriber or individual shall be made without undue delay after the detection of the personal data breach.

[6] As the proposed regulation regarding data protection foresees a generalization of the notification obligation to all sectors, and since several Member States already have a legal notification obligation in place, the examples in the current opinion are not limited to the electronic communications sector.

2. Breaches that may adversely affect data subjects

Breaches should be notified without undue delay to data subjects when there are likely to be adverse effects to personal data or privacy. This section lists examples of breaches that meet these criteria. It also gives examples of technical measures which, if they had been in place prior to the incident, might have allowed avoiding notification to data subjects.

Case 1. *Four laptop computers were stolen from a "Children's Healthcare Institute"; they stored sensitive health and social welfare data as well as other personal data concerning 2050 children.*

This personal data breach concerns confidentiality and (if no backup of the data was available to the controller) availability and integrity of the data.

Potential consequences and adverse effects of the confidentiality breach:

- The first impact is a breach of medical secrecy: the database contains intimate medical information on the children which are available to unauthorized people.
- The publication of those data may impact the school and/or family environment of the children (e.g. data on assault, long terms diseases, mental problems, social or financial difficulties of the family, etc.).
- It may emotionally affect children and parents.
- Those data may be used to blackmail parents and children (depending on their age).
- Parents of critically ill children may be targeted by people eager to profit from their weakness (e.g. charlatan, sects, etc.).

Potential consequences and adverse effects of the availability breach:

- It may disturb the continuity of children's treatment leading to aggravation of the disease or a relapse.
- It may lead to accidental poisoning by drug allergy or by conflicting drugs, which may result in various health problems or death.
- It may lead to undue delay in reimbursement or financial assistance to the data subjects which would have financial impacts on the concerned families.

Potential consequences and adverse effects of the integrity breach:

- The lost data may affect the integrity of the medical records and disrupt the treatments of the children. For example, if only an old back-up of the medical records exists, all changes to the data that were made on the stolen computers will be lost, leading to corruption of the integrity of the data. The use of medical records that are not up-to-date may disrupt the continuity of children's treatments leading to aggravation of the disease or a relapse.

Based on the potential effects, notification in this case should take place but it is also important to take account of the age and maturity of the data subjects. It may be more

appropriate in this case to notify to a parent or legal guardian who will already be taking an active role in the medical care of the child in addition to notification to the children themselves when it is appropriate or required by applicable law.

In this case, notified parents will be able to report abnormality in the continuity of the treatment, check the allergies known by the institute or ask for new medical tests in order to ensure that their children receive the correct treatment. They also may choose to directly inform additional persons of the condition of the children in order to control some of the impacts on the children's environment.

Example of appropriate safeguards that might have reduced the risks, if implemented beforehand:

- The availability and integrity breach could have been prevented, or the consequences and adverse effects mitigated, by having a sufficiently up-to-date, secure back-up available;
- The potential consequences and adverse effects of the confidentiality breach could have been mitigated by protecting the data using an appropriate encryption product with a sufficiently strong and secret key.

Should those safeguards have been in place and remained secure (i.e. the key remained secret and the back-up stayed available), then notification to the individuals may not be required in principle. This should be demonstrated to the satisfaction of the competent authority.

Case 2. *Personal data related to the customers of a life insurance broker was unduly accessed by exploiting a web application vulnerability. Data subjects were identified by name and address, and completed medical questionnaires were included. 700 data subjects were affected.*

Potential consequences and adverse effects of the confidentiality breach:

- Data published on the internet by the attacker may impact the ability of the data subjects to find a job (e.g. answers about health problems, pregnancy, etc.).
- It may impact the work and/or family environment of the data subjects.
- It may also have emotional impacts if the data subjects hide their diagnosed condition.
- It may lead to identity fraud.
- The data (like being a customer or paying for certain services) may be used for phishing.

As this case is likely to adversely affect the data subject, it should be notified to the data subjects.

Example of appropriate safeguards that might have reduced the risks if implemented beforehand:

- A continuous monitoring of potential vulnerabilities of the technologies used, including and not limited to regular vulnerability scanning of the website and updating software (including security software) might have either prevented the breach or limited its impact.

  Even though security vulnerabilities based on zero-day exploits cannot be easily avoided, adequate and effective policies on proactively preventing security vulnerabilities from being exploited, including code review, can reduce the risk margin to an acceptable level. Furthermore, a good security incident management policy can also mitigate the consequences of a breach by limiting its adverse effects in time and scope.

- As in the previous case, the potential consequences and adverse effects of the confidentiality breach could have been mitigated by protecting the customer data using an appropriate encryption product with a sufficiently strong and secret key. This may be particularly effective to protect against theft of the disk or similar circumstances.

- Finally, different privacy enhancing technologies may have been used by the insurance company to minimize the data and/or the identifiability of the data subject. For example, the company may have sent a random ID-number by post to allow its customers to fill in the medical questionnaire online. This may prevent questions about name, address, date of birth or telephone number in the online questionnaire.

Case 3. *An employee of an internet service provider has given to a third party the login and password for an account with global access rights to the client database. Using this account, the third-party can access all the customer information without any restrictions. The database includes name, address, email, phone numbers, access and other identifying data (user name, hashed passwords, customer ID) as well as payment data (account number, credit card details, etc.). Even though payment data was encrypted with a state of the art algorithm, the master account compromised was authorised to access it, thus the third party also had access. The company has more than 100.000 customers.*

Potential consequences and adverse effects of the confidentiality breach:

- Misuse of the payment data (especially credit cards details) would have a financial impact on the customers.
- As the passwords were simply hashed, the third party may easily deduce the corresponding plain text. Access to the account of any customer would be possible even after the breached account was closed.
- The third party could easily use the email and password of some of the concerned data subjects to access accounts of other online services as many people use the same password across a range of different online services.

Potential consequences and adverse effects of the integrity breach:

- The third party had total access to the database, he may have modified, deleted or added some of the account data.
    - If the ISP service included email or web hosting, the third party could have accessed, modified or deleted this content, modified DNS settings or terminated the data subject's account.

Although the financial data were encrypted, the third party had access to the decrypted data via the user interface and therefore the notification exemption does not apply.

If the secured log files are trustworthy (i.e. not compromised) and that it can be seen from the log files that the account did not access the client database, then notification to data subject should not be mandatory.

In any other case, as this case is likely to adversely affect the data subject and the exemption does not apply, it should be notified to the customers affected.

Whenever passwords are compromised, the data controller should securely force the data subjects to create a new password, ensuring that all new passwords are entered by legitimate users and not by third parties who obtained the login credentials. In practice, this may correspond to the secure procedure to renew a lost password and it should include information on the underlying reason for the password renewal. The user's notification should also include a recommendation to not use the previously used password or a similar one again and to change the compromised passwords in every account where the same password was used.

Example of appropriate safeguards that might have reduced the risks if implemented beforehand:

- Each individual must be allocated their own accounts and access to personal data should be exclusively authorized by applying need-to-know and least privilege principles. This also applies to vendors, third party maintenance personnel and others who temporarily need access to the database: they should only be given access to the functionality and the data that they need in order to perform their designated tasks, for no longer than strictly necessary. The use of accounts with "global access" to the database should be limited and methods for tracing and limiting the use of this kind of accounts should be put in place. By putting such safeguards in place, the breach could either have been prevented or its impact mitigated.
- If the passwords had been stored securely (e.g. salted and using a cryptographic hash function), then secondary adverse effects to the individuals would have been greatly reduced. However, individuals with poor password choices may still be at risk, especially where they share those access credentials with other online services. This could have been mitigated by suggesting stronger password choices for these users.

Case 4. *An envelope containing credit card slips was mistakenly thrown into a waste bin rather than securely destroyed. The waste bin was emptied to a large bin left outside the premises for waste collection. An individual took the envelope out of the second bin and then distributed the credit card slips around in a nearby housing estate. Data included full card details*[7] *and name of card holder. In some cases, signatures of the card holder were also available. 800* data subjects *were affected.*

Potential consequences and adverse effects of the confidentiality breach:

- The breach might have a financial impact on the data subjects if their card details are still valid and misused[8].

As this case is likely to adversely affect the data subject, it should be notified to the concerned data subjects. In this case, if no other records have been kept, it may seem difficult to notify individually each data subject as it may be unknown which specific credit card slips were in the envelope. The shop should alert the card payment processor, so they can monitor possibly fraudulent transactions. Another practical orientation proposed in the Regulation 611/2013[9] provides that when the provider "having made reasonable efforts, is unable to identify within the timeframe referred to in paragraph 3 all individuals who are likely to be adversely affected by the personal data breach, the provider may notify those individuals through advertisements in major national or regional media, in the relevant Member States, within that timeframe". Therefore, in the case of a shop with a customer base which is mostly local, a notification in a regional paper may be considered sufficient. Additionally, informing the credit card companies about the breach might help to protect their customers.

If the envelope had been recovered by the data controller from either of the waste bins and the envelope or otherwise remained unopened it is unlikely that this would adversely affect subscribers; therefore the breach would not need to be notified to the data subjects.

Example of appropriate safeguards that might have reduced the risks if implemented beforehand:

- Informing the employees on the potential consequences of such breaches, and using an appropriate office shredder[10] or archive shredding service to destroy credit card slips (and any similar paper documents containing personal data) before throwing them away, would greatly reduce the risk of such a breach.
- Using point of sale (POS) terminal which does not include full credit card details.

[7] Whilst best practice is to perform payment card data truncation on the customer's printed receipt, it is not a feature available on all Point of sale (POS) terminals and may be printed in full on merchant receipt copies.
[8] As there are still ways to use credit card details without CVV (or equivalents), even breaches that do not include the CVV must be notified.
[9] Although this regulation is not applicable in this context
[10] For example, a class 2 shredder at level P-4 or more in the DIN 66399 classification for paper documents.

Case 5. *The encrypted laptop of a financial adviser has been stolen from the boot of* a *car. All the details of financial assessments - e.g. mortgage, salary, loan applications of 1000 data subjects were affected. The encryption key, the passphrase, is not compromised but no backup is available.*

Potential consequences and adverse effects of the confidentiality breach:

- Depending on the exact nature of the data that was breached, misuse of the data may have various impacts on the data subjects. However, as the laptop had full disk encryption (state of the art) enabled with a strong passphrase which has not been compromised, no unauthorized disclosure occurred.

Potential consequences and adverse effects:

- The unavailability of the data requires that data subjects will need to give the necessary information again. This implies a small adverse effect on the data subjects in the form of time consuming actions and annoyance.
- In some cases it may also cause submission or application deadlines to be missed, which may have various secondary impacts on the data subjects depending on the context: fines, loss of revenue or anticipated profits, loss of opportunity, termination of a purchase agreement, etc.

Since the data were lost and the effects of the availability breach were not mitigated, the personal data breach is likely to adversely affect the data subject. Thus, the breach should be notified to the concerned data subjects. Whilst the notification will explain that information would need to be provided again to the financial adviser it would also inform the data subjects of the different potential consequences and adverse effects they may encounter due to the breach.

Example of appropriate safeguards that might have reduced the risks if implemented beforehand:

- An effective and secure backup solution would have allowed restoring the data. If an up-to-date backup of the data had been available, no availability breach would have occurred and notification would not have been necessary.

Case 6. *A mobile telephone network operator provides an online account facility where subscribers can login and view recent billing and account activity. An illegal access to the database storing the passwords of a website has been discovered. The third party has accessed the authentication data of the users (user name and unsalted MD5-hashed passwords).*

Potential consequences and adverse effects of the confidentiality breach:

- The third party may deduce the password and therefore access the account of any customer as he also has the usernames.

- As many people use the same username and password combination for many online accounts the third party is likely to be able to access other accounts of some of the concerned data subjects, including email accounts in some cases.

As the passwords were simply hashed, they may not be considered as being unintelligible as defined in the Article 4(2) of Commission Regulation 611/2013[11]. Thus, the exemption to notification to the data subjects does not apply.

As this case is likely to adversely affect the data subject and the exemption does not apply, it should be notified to the customers affected with a clear recommendation to the user to change their passwords in all the accounts sharing the same compromised password. In any case, all the users should be forced to change their passwords – using a secure method – when trying to access the service.

Example of appropriate safeguards that might have reduced the risks if implemented beforehand:

- If the passwords had been stored securely (salted cryptographic hashed with state of the art hash function and a key or salt) then adverse affects to the individuals would be greatly reduced. However, individuals with poor password choice may still be at risk, especially where they share those access credentials with other online services.

Case 7. *An internet service provider provides a facility for subscribers to view details of their account, internet usage history including monthly bandwidth and frequently visited domains. A coding error in the website results in the user's access credentials not being validated and data being accessible by tampering with the subscriber ID value submitted in the URL parameters. The account details of all customers may be accessed by cycling through consecutive subscriber IDs.*

Potential consequences and adverse effects of the confidentiality breach:

- The data may be used for spamming the data subjects by email or phone call.
- The data may profile the subscriber, and reveals details of its behaviour that could expose sensitive information. It may impact the work and/or family environment of the data subjects.

This breach is likely to have an adverse effect on the individual thus it should be notified to the customers.

[11] Article 4(2) provides that :

Data shall be considered unintelligible if:

(a) it has been securely encrypted with a standardised algorithm, the key used to decrypt the data has not been compromised in any security breach, and the key used to decrypt the data has been generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key; or

(b) it has been replaced by its hashed value calculated with a standardised cryptographic keyed hash function, the key used to hash the data has not been compromised in any security breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access the key.

Example of appropriate safeguards that might have reduced the risks if implemented beforehand:

- Monitoring the potential vulnerabilities of the technologies used, as described in case 2, as well as tests on a pre-production platform before deployment and code review may have allowed to avoid the breach.

3. Possible scenarios where notification to the data subjects is not required

While the assessment the consequences of a personal data breach must be done on a case by case basis, in order to take all the elements appropriately into account in the assessment of the likely adverse effects on individuals, as a general guidance and to complement the exemptions described in the previous section, the controller may also consider that notification to data subjects is not required in some specific cases.

Those cases may include:

- A personal data breach only relating to confidentiality, where data was securely encrypted with a state of the art algorithm, the key to decrypt the data was not compromised in any security breach, and the key to decrypt the data was generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key. Indeed, such measures make the data unintelligible to any person not authorised to access it.

- Data, such as passwords, were securely hashed and salted. The hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not been compromised in any security breach, and the key used to hash the data had been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access the key.

4. Q&As

When is notification to individuals not mandatory?

- Whenever the security breach is not a personal data breach (see next question).
- Whenever the personal data breach is not likely to adversely affect the personal data or the privacy of the data subject according to the results of a severity assessment, to the satisfaction of the competent authority.
- Whenever the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. For example, if a (confidentiality only) personal data breach only concerns either encrypted data with a state of the art algorithm or salted/keyed hashed data with a state of the art hash function, and that all the concerned secret keys and salts are not compromised.
- Notification of data breaches as described in this Opinion constitutes a good practice for all data controllers, even if notification is not mandatory.

When does a security breach become a personal data breach?

A security breach is a personal data breach when the breached data are personal data, as defined in the Directive 95/46/EC in its Article 2 (a) : *'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*

Opinion 4/2007 explains that it concerns data related to a person: "a person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.)". Additional guidance on this point is available in Opinion 4/2007.

Should likely secondary effects be considered?

Yes, data breaches should be notified to the data subjects if the breach is likely to adversely affect the personal data or the privacy of the data subjects.
Thus, all the potential consequences and potential adverse effects on the data subjects should be taken into account.

> ***Example 1:*** *The web site of a Music Entertainment Company is hacked and the users' database is stolen and published on the web. The personal data leaked consist of names/surnames, music preferences, as well as usernames and passwords of the registered users in the company's website. 9000 users were affected.*

In this breach, the direct adverse effect on the individuals might seem quite limited in most cases (i.e. leak of information on musical preferences) and may lead to wonder whether to notify the data subjects. However, since the passwords were compromised, they will have to be renewed by the data controller. In this process, it will be necessary to inform the users on

the reasons why the passwords are renewed. In addition, since many users use the same password on different accounts[12], it is also likely that the breach implies, as a secondary adverse effect, a confidentiality breach regarding another account. The data subject will be able to minimize these secondary effects by changing the passwords of all their other accounts. Thus, the notification should also include information on the likely adverse effects concerning other accounts and should therefore include a recommendation to use different passwords on different websites and renew the passwords of any accounts that was using the compromised password.

> ***Example 2:*** *A second example may be evidence for a criminal case concerning one individual was sent on a CD via recorded delivery to a lawyer but the CD is lost in the post.*

The direct breach is an unavailability breach. It may have either a negligible or a very high impact on the individual(s) involved depending on the possibility to take appropriate action on time or not.
But a secondary adverse effect is likely to happen if the CD is sent without proper protection and the data accessed. Indeed, that person may read it, sell it to journalists, etc. This secondary effect may have a very high impact on the individual(s).

In this case, if the CD can be resent on time, the direct impact on the individual would be negligible and would not imply to notify the individuals while the potential secondary breach may be very high and would definitely imply to notify the individuals.

If only one person is concerned, is it necessary to notify the individual?

Yes, the Directive 2002/58/EC does not set a minimum of data subjects to be concerned by a data breach to start a notification. The Telecommunication directive says in Article 3-1: "*When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall, in addition to the notification referred to in Article 2, also notify the subscriber or individual of the breach."*

Thus, the controller should notify, depending on the likely adversely effects, independently to the number of data subjects concerned.

How to deal with data which is likely to be public?

Two points should be considered.

1. "Public" may imply different levels of availability: data may be freely accessible on the internet, publicly available within a subscribed service, publicly available offline upon request, etc.
   For example, in France the electoral roll are displayed on the walls of city hall during elections, any voter or any political party can obtain it but online publication of those lists is not permitted by law.

[12] According to recent studies, 55% to 80% of internet users use the same password on different accounts.

Thus accidentally sending the electronic version of the roll to the wrong voter or losing a paper version of the list would not be a confidentiality breach while a publication on the internet of the list would be one and should be notified.

2. Some data may be public for some data subjects and not public for others.
   For example, a list of phone numbers linked to a last name may contain both phone numbers publicly available in phone books and unlisted phone numbers.

To sum up, whenever the level of availability or publicity of the data is changed by the breach then, it should be considered as a confidentiality breach and should be notified (if the breach is likely to adversely affect the data subjects concerned).

How to notify when the contact details of the individuals affected are insufficient or not known?

There are cases in which, even having a direct contractual relationship with the end user, the provider has not enough details to ensure proper notification. In that sense, even taking into account the possibility of notifying through advertisements in media, the obligation of pursuing individual notifications by making all reasonable efforts still persists[13].

Even though the obligation of maintaining reasonable efforts lies with the provider by putting in place all the reasonable mechanisms to ensure that all affected individuals are made aware of the breach, this does not, however, exclude the possibility to request support from other providers or controllers in possession of the contact details. Thus, considering case 4, the controller not having the contact details of the cardholders affected could report the intermediary payment agent that may easily contact the individuals. Other cases may require collaboration of the competent authorities that should be made aware, in any event, of the fact that the provider cannot guarantee individual notifications.

Is it necessary to notify to data subjects who were not affected by the breach?

No, provided it can be reliably determined which data subjects were not affected by the data breach. For example, if it can be demonstrated a subset of data subjects were not affected by the security incident then these data subjects may not need to be notified. However, the data controller must consider all likely adverse effects in making this decision. Depending on the nature of the breach, not receiving a notification may also cause distress to individuals.

[13] According to Article 3(7) of Regulation 611/2013, when the provider, despite having made reasonable efforts, is unable to identify all individuals who are likely to be adversely affected by the personal data breach, the provider will notify those individuals through advertisements in major national or regional media in the relevant Member States, within the applicable timeframe. In the same line, it is stated that the provider shall continue to make all reasonable efforts to identify those individuals and to notify them as soon as possible.