Who You Gonna Call When There's Something Wrong in Your Processing? Risk Assessment and Data Breach Notifications in Practice

Susan Gonscherowski, Felix Bieker

Who You Gonna Call When There's Something Wrong in Your Processing? Risk Assessment and Data Breach Notifications in Practice

Susan Gonscherowski, Felix Bieker

Unabhängiges Landeszentrum für Datenschutz (ULD, Independent Centre for Data and Privacy Protection) Schleswig-Holstein, Kiel, Germany
{sgonscherowski | fbieker}@datenschutzzentrum.de

Abstract. With the assessment of the risk to the rights and freedoms of natural persons the GDPR introduces a novel concept. In a workshop participants were introduced to the notion of risk, based on the framework of the German data protection authorities, focusing on personal data breach notifications. This risk framework was then used by participants to assess case studies on data breaches. Taking the perspective of either a controller or a data protection authority, participants discussed the risks, the information provided and the necessary steps required by the GDPR after a data breach.

Keywords: Data Breach, Notification, Supervisory Authority, DPA, Risk to Rights and Freedoms, Risk Assessment, General Data Protection Regulation, Data Protection, Privacy

1 Introduction

Over the last years, data breaches have occurred with increased frequency and more severe impacts on data subjects [1,2,3,4,5,6,7,8]. Since the General Data Protection Regulation (GDPR) has become applicable, new notification and communication requirements in case of a data breach must be fulfilled. As every breach is different, handling it appropriately may prove difficult especially in terms of consequences and risk assessment.

In order to determine whether the data protection authority has to be notified of a data breach and whether this has to be communicated to the data subjects, the controller has to evaluate the risk to the rights and freedoms of natural persons according to Articles 33 and 34 GDPR. This assessment is also crucial for the implementation of technical and organisational measures according to the provisions on the responsibility of controllers, data protection by design and the security of the processing under Articles 24(1), 25(1) and 32(1) and (2) GDPR as well as for the determination whether a Data Protection Impact Assessment has to be carried out (Article 35 GDPR) and whether the prior consultation mechanism of Article 36 should be triggered. The particular notion of risk in the GDPR is thus essential for the correct interpretation and implementation of the regulation as a whole.

In this paper, we introduce the notion of risk in the GDPR as well as the obligations of controllers with regard to data breaches. This will be completed by a summary of the participants' discussions of two fictitious case studies during a workshop at the 2018 IFIP Summer School. Although the provisions on data breaches in Articles 33 and 34 of the GDPR impose some specific obligations on controllers, other aspects, such as the risk methodology, have to be determined. This is also true for determining actions to deal with risks resulting from the incident, e.g. identity theft.

The advantage of an interactive workshop was a more "hands-on" approach. Divided in two groups the participants took the perspectives of a controller or a data protection authority. The first case study involved a public hospital and the disclosure of several categories, including special categories of personal data. The task was to determine whether the submitted breach notification conformed to the requirements of Article 33 GDPR. The notification form is based on actual forms provided by data protection authorities.

The second case involved a private sector controller and in this case the data breach was based on a database mix-up. The second group was asked to determine whether the incident required communication with the data subjects according to Article 34 GDPR.

2 Assessing the Risks to the Rights and Freedoms of Natural Persons

The question, whether notification and communications of data breaches are necessary depends on the assessment of the risk to the rights and freedoms of natural persons according to Articles 33 and 34 GDPR. While the GDPR does not further define this notion of risk, recitals 75 and 76 state that risks of varying likelihood and severity may lead to damage for individuals.

2.1 The Notion of Risk to the Rights and Freedoms of Natural Persons

The specific notion of risk to the rights and freedoms of natural persons introduced in the GDPR can thus best be defined as the product of the likelihood and severity of potential damage for individuals [9]. However, this should not be taken to imply that this is a mathematically precise formula. Rather the assessment, according to recital 76 must be carried out with reference to the nature, scope, context and purpose of the processing and should, as prescribed by the principle of accountability according to Article 5(2) GDPR, be based on verifiable facts.

Recital 75 finds that the damage to individuals, which can be caused by the processing of personal data can be physical, material and non-material, for instance causing bodily harm, financial loss or deprive data subjects of their rights. With reference to Article 8 Charter of Fundamental Rights (CFR) this becomes even clearer: as every processing of personal data constitutes an interference with this fundamental right, any processing operation can potentially cause damage to the rights of individuals [10]. However, this interference can, of course, be justified under the conditions of

Article 52(1) CFR, which contains a clause on justifications for all fundamental rights contained in the CFR.[1] For Article 8 CFR this is the case when the interference caused by the processing of personal data is as minimal as possible, i.e. when the risks to the rights and freedoms of individuals have been mitigated appropriately [11]. However, there are also other rights that must be considered, such as the right to privacy under Article 7 CFR, the freedom of speech and assembly according to Articles 11 et seq. CFR as well as the rights to non-discrimination of Articles 21 and 23 CFR [12].

2.2 Risk Identification

The assessment must take into account negative consequences of the processing operation as planned as well as deviations from the processing, such as access by unauthorized parties, unauthorized or accidental disclosure, linking or destruction of data, failure or unavailability of designated procedures, accidental or intentional alteration of data or the failure to provide information. All of these incidents may be caused by parties internal or external to the controller. Thus, the assessment must include all potential negative consequences of a processing operation for the rights and freedoms of natural persons, their economic, financial and non-material interests, their access to goods and services, their professional and social reputation, health status and any other legitimate interests [9].

Furthermore, the sources of these risks must be identified. Under data protection law, the organization itself is a significant risk source, as it processes the individuals' personal data. Thus, for instance the marketing department or individual employees using data without authorizations pose risks for data subjects. However, risks may also emanate from authorized or unauthorized third parties, such as processors, contractors, manufacturers, hackers or public authorities, especially law enforcement, pursuing vested interests. Further, technical malfunctions and external factors, such as force majeure, have to be taken into account [13].

2.3 Risk Assessment

The likelihood and severity of potential damage must be assessed. However, attempts trying to ascribe a precise numerical value to either of these should be rejected, as they suggest an objectivity that is not attainable. Rather, the likelihood and severity should be classified in categories, which give an estimate and follow from a thorough-

[1] In order to be justified, the interference must respect the essence of the law, pursue a legitimate aim and be proportionate. On the level of secondary law, this is implemented by Article 6 GDPR: In order to protect the fundamental rights of individuals and as every processing of personal data interferes at least with Article 8 CFR, the processing of data is only permissible when it is based on a legal basis (as provided in Article 6(a)–(f) or (2) and (3)), which must be proportionate. Further, the controller must implement safeguards in order to ensure a level of security appropriate to the risk for fundamental rights, cf. Article 32(1) GDPR.

ly argued justification providing the basis of considerations for the assessment. A classification could use a four-tiered scale, ranging from minor, limited to high and major [9].

The likelihood describes how likely a certain event, which itself might be damage, occurs and how likely it is that this may lead to (further) damage. The motivation and the operational possibilities of an organisation to use data for incompatible purposes should, inter alia, be taken into consideration as criteria for the assessment of the likelihood [9].

The severity of potential damage must, according to recital 76 be determined with respect to the nature, scope, context and purposes of the processing. The Article 29 Working Party has identified criteria to assess whether a high risk is likely to occur for a processing operation [14]. These criteria are derived from provisions where the legislator considered potential damage to be particularly sever, such as where the processing occurs on a large scale (recital 75), affects vulnerable individuals, such as children or employees (recital 75), may prevent data subjects from exercising their rights (recitals 75 and 91), concerns special categories of data (Articles 9 and 10 GDPR) involves automated decision-making and profiling (Article 22 and 35(3)(a) GDPR),or allows for systematic monitoring (Article 35(3)(c) GDPR).

Once the likelihood and severity of potential damage have been assessed, the risk to the rights and freedoms of natural persons has to be evaluated and classified according to the categories of low, medium or high risk. However, the GDPR does not contain any provisions concerning a specific methodology for this evaluation.

The risk of the processing operation follows from the highest risk category of all individual risks. However, in cases where there are many individual risks within a category, this leads to cumulative effects, which require a higher classification of the risk [15].

3 Data Breaches

Data Breaches occur on an almost daily basis. Often, such an event confronts the controller with a multitude of problems. One of the first problems for the controller might be to determine whether or not an incident related to the data processing is a data breach at all. In 2017 approximately 20 % of small and medium-sized businesses in Germany indicated they had had no IT-security incidents at all [16]. However, this is not a reason to celebrate the high standard in IT-security and data protection in those companies. It is more likely their detection measures are insufficient and incidents were simply not detected.

If and when a controller becomes aware of a problem, the next question is whether a security breach or a data breach occurred. A personal data breach is defined in Article 4(12) GDPR as “a breach of security leading to the accidental or unlawful destruction, loss or alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed”. While a data breach is often understood as an unauthorised disclosure of personal data [1,2,3,4,5,6,7,8], data protection law also classifies loss of integrity and/or availability as a breach. The reference to the three

standing requirements for IT-security leads to the conclusion that every data breach is also a security breach, but not every security breach is always a personal data breach [17]. In case of an incident the controller must investigate if personal data is affected by the breach in any way. The awareness that personal data was indeed compromised then triggers a 72 hour deadline for further actions. According to the GDPR, a notification of the supervisory authority (Article 33) and possibly the communication of the breach to the data subject (Article 34) may be necessary. At this point the risks posed to individuals by the data breach have to be assessed. This differs from the initial assessment of the risks posed by the processing operation, which is obligatory under the provisions concerning the responsibility of controllers, data protection by design and the security of the processing in Articles 24, 25(1) and 32 GDPR. As described above, the likelihood and severity are the main factors in risk assessment. In case of a personal data breach the likelihood of the risks relating to a breach is 100% leaving the severity as the only variable. The potential impact on the rights and freedoms of data subjects ranges from no risk, to risk up to a high risk.

Article 34 of the GDPR defines three preconditions that must be fulfilled before a controller has the obligation to communicate the incident to concerned individuals. Firstly, the controller must become aware of a breach. Secondly, the risk assessment leads to the conclusion that the breach poses a high risk to the rights and freedoms. Thirdly, the controller is able to identify the individuals affected by the breach.

There are circumstances when these pre-conditions are difficult to meet and therefore data subjects do not receive a message informing them of a breach that may have negative consequences for them. Some circumstances were already foreseen by the legislator. If the controller is not sure whether or not a breach occurred the issue may be investigated further for three days. Therefore, it is crucial that effective detection methods are being used. As mentioned above a considerable number of controllers and processors lack the ability to achieve this. However, the ability to detect a breach is an essential part to ensure the security of processing as demanded in Article 32 GDPR.

It is also possible that the controller responsible for a breach is no longer available, because the company went bankrupt or the service was terminated. For instance, unintentionally or unlawfully disclosed sensitive personal data originating from phishing attacks are freely available on the internet [18]. In these cases there is no controller to become aware of a breach. The legislator did not provide a solution in the GDPR. However the research project EIDI aims to develop a warning system in order to close this gap in responsibility [19].

The risk assessment for a certain data breach represents the risk for that precise moment. However, the external conditions may change. Technological developments can weaken encryption and the combination of data stemming from different breaches might reveal sensitive information e.g. linking clear text passwords for specific accounts. A breach classified as not being a risk to data subjects rights at the time of the incident might become a risk later on.

And lastly, the direct identification of the concerned data subjects may not be possible. For instance, the provided service may not require contact information or the individual is no longer using the service. This could mean there is no contact infor-

mation or the available information is outdated. Of course, the incident itself can be the reason for missing contact information, e.g. when after a malware attack the relevant data is encrypted [20]. Article 34 GDPR, as a backup, requires information via public communication when no contact information is available. Yet, this requires the same level of effectiveness as a direct communication. It is doubtful that any public annunciation meets this high standard.

4 Hands-On: Assessment of Case Studies

After the input statements, participants were divided into two groups to discuss the two following case studies, identify risks for the rights and freedoms of natural persons and discuss them. These were then summarized by participants of each group and discussed with all participants.

4.1 Case Studies

Case Study 1: Public Hospital.
A public hospital wants to combat cases of an acute disease, which can cause severe damage to the nerve system if not diagnosed within 24 hours of the first symptoms. As some of these symptoms are similar to the flu, the other characteristic symptoms are often not properly recognized. In order to assist doctors in the diagnosis, the hospital wants to develop an app for its own managed mobile devices used by clinicians, which recognizes these symptoms and alerts doctors to this potential diagnosis. The app uses machine learning technology, which, based on patient data, constantly improves the recognition of relevant symptoms.

In order to train the algorithm, the hospital gives the department that carries out the development of the app full access to all of its 1.5 million patient data records. These data consist of records of former as well as current patients dating back to the 1980s and include the address, date of birth, phone number, occupation as well as the patient's medical history concerning all treatments at the hospital. When the data are collected, the hospital informs patients that their data will be processed in order to facilitate the treatment of their medical conditions at the hospital.

In order to process the patient data, the hospital moves the data, which it encrypts beforehand, in its own cloud environment. However, an unencrypted backup of the data is stored on a server with an open port, which leads to all the patient files that are analysed by the algorithm being available online. This concerns 150,000 of the hospital's patient files.

Task for Case Study 1. 23 hours after this incident is detected, the hospital submits a notification to you [Table 1], the competent data protection authority. Determine whether the notification conforms to the requirements of Article 33 GDPR, focusing especially on the assessment of likely consequences of the breach, and covers the entirety of data breaches. Then consider which actions you would take next.

Table 1. Notification Form Submitted to Data Protection Authority

1. Controller
Contact Data Data Protection Officer of a Public Hospital in an EU Member State DPO@public-hospital.health
2. Timeline
When did you discover the breach? On Tuesday 21/8/2018 at 10:43
When did the breach occur? On Monday 20/8/2018 at 17:19
This notification is made within 72 hrs of discovery ⊗ Yes O No **If not, why was there no earlier notification?** ---
3. Description of Data Breach
Kind of data breach O Device lost/stolen O Papers lost/stolen/kept in unsafe environment O Unencrypted email sent O Mail was lost/opened accidentally O Hacking/Malware/Phishing ⊗ Accidental disclosure/publication O Wrong recipient(s) O Misuse of access rights O Other, please specify: ---
Please describe the data breach in detail Backup was uploaded to cloud environment; data was encrypted; port on server was

open after maintenance work and data accessible online; encryption can be broken due to security flaw in algorithm
Categories of personal data ⊗ Basic personal identifier, e.g. name, contact details O Passwords O Data revealing racial or ethnic origin O Political opinions O Religious or philosophical beliefs O Trade union membership ⊗ Data on sex life or sexual orientation ⊗ Health data ⊗ Genetic or biometric data O Criminal convictions, offences O Location data O Not yet known O Other, please specify: ---
Number of individuals concerned? 150,000
Number of records affected? 150,000 patient records
Description of likely consequences of the personal data breach: Loss of confidentiality of patient records, potentially identity theft
The personal data were safeguarded by the following appropriate technical security measures: Encryption of personal data
4. Measure taken to address the personal data breach
Description of measures taken to address data breach: Patient records have been removed from cloud environment, port on server has been closed

Description of measures proposed to be taken to address data breach: Encryption with new algorithm
Description of measures taken to mitigate adverse effects of data breach: Communication of breach to data subjects
Description of measures proposed to be taken to mitigate adverse effects of data breach: --
5. Communication to data subjects
The personal data breach has been communicated to data subjects ⊗ Yes On Tuesday 21/8/2018 at 18:00: all patients have received information about the breach to their contact details via email or mail, depending on available information O No, as O Appropriate technical and organisational measures have been taken; please describe: --- O Follow-up measures ensure that the high risk for the rights and freedoms of data subjects does no longer exist; please describe: --- O Communication to data subjects would involve disproportionate effort; please describe: ---

Discussions on Case Study 1. In the discussion of the first case study, participants quickly discovered flaws in the envisaged processing operation: they pointed out that the breach that had been notified to the supervisory authority might, in fact, not be the first data breach that had occurred during the processing operation. The definition of personal data breach under Article 4(12) GDPR also encompasses a breach of security leading to the unauthorised access to stored personal data. As the participants noted, the hospital, when collecting the data of patients stated that their data would be processed in order to facilitate their treatment at the hospital. While this purpose was rather generic, it could refer to both a contract on medical treatment according to Article 6(1)(b) in conjunction with Article 9(2)(h) or, for medical emergencies, the pro-

tection of vital interests of data subjects according to Article 6(1)(d) in conjunction with Article 9(2)(c) GDPR.

However, under the principle of purpose limitation of Article 5(1)(b) GDPR, the data could not be further processed for purposes that are incompatible with this initial purpose of treating a medical condition. It could be argued that the use of the data to train the algorithm was a processing of personal data for the compatible purpose of medical research under this provision, which would, however, be subject to the test of Article 6(4) GDPR, which requires that the controller takes into account inter alia the link between the purposes, the nature of the data, the possible consequences for data subjects and the existence of appropriate safeguards. As the hospital granted access to the full patient files, the participants found that with regard to the principle of data minimisation, which requires that only data necessary to achieve a specific purpose are processed according to Article 5(1)(c) GDPR, the hospital did not conform to the legal requirements for further processing. Therefore, the sharing of the patient record data with a different department of the hospital, which was not tasked with the treatment of the patients was an unauthorised and unlawful processing of personal data and hence constituted an independent data breach, which was not notified to the supervisory authority, even though there was a risk that patient data would be further disseminated than necessary. While this first breach was limited to an internal department of the hospital, it did concern all of the 1.5 million patient data records and thus occurred on a very large scale. Ultimately, with the subsequent data breach this specific risk to the rights and freedoms of patients even materialized with regard to the files of 150,000 patients.

Concerning the notification of the second data breach, the participants of the workshop noted that the hospital described neither the processing operation nor the breach accurately or in much detail. From the perspective of the supervisory authority, participants found that it would be helpful to receive a Data Protection Impact Assessment concerning the relevant processing operation in order to have a more concrete idea of the systems and data used as well as the controller's initial assessment of the risks that the processing operation entails. While this is not foreseen by Article 33 GDPR, the supervisory authority may request any relevant information from a controller under Article 58(1)(a) GDPR. However, participants pointed out that in a time-sensitive situation where the rights of individuals could be in jeopardy, requiring a formal request only after the submission of the breach notification

Most notably, the controller made the counterfactual statement that the backup stored in a cloud environment could be decrypted due to a security flaw in the algorithm, whereas the backup that was accessible through a port opened for remote maintenance was actually not encrypted at all. This extended to the claim that the personal data affected by the breach were safeguarded by encryption. While this was the case for the live data, the hospital stored its backup without any encryption, which seriously undermines the protection.

Participants further found the risk analysis of the controller to be lacking. By recourse to the framework for risk assessment provided in the first part of the workshop, they could easily identify risks beyond those noted by the controller, which encompassed only the loss of confidentiality of patient records and the potential for identity

theft. In this regard, it could be seen that the controller was very much focused on an information security perspective. As the concept of breach notification originated in this field, this is not surprising. However, it is a common pitfall to equate an information security breach with a personal data breach. Instead it must be seen from the perspective of data protection law, which, unlike information security is not concerned with the protection of the controller, but rather states under Article 1 GDPR that it serves to protect the rights and freedoms of natural persons and especially data subjects. Therefore, the risks to the rights and freedoms of individuals, which must be assessed for a personal data breach, differ from those of information security.

Applying these principles to the case at hand, participants pointed out that beside the contact information, the files also included the medical records and thus a patient's medical history, which themselves constitute health data and are this covered by Article 9 GDPR as a special category of personal data. With regard to the patient's medical history, risk sources were not limited to criminal third parties engaging in identity theft. The health data could potentially be of interest to the data subject's employers, pharmaceutical companies, insurance companies as wells as banks or credit scoring agencies. From the identification of risk sources alone, several other risks to the rights of individuals could be deduced, such as an employer terminating the contracts of severely or chronically ill employees, while pharmaceutical companies could be interested in contacting individuals in order to market medicinal products. Furthermore, insurance companies could individualize the cost of insurances, such as life or health insurance and thus increase prices. Similarly, a credit scoring agency or bank could downgrade an individual's score where they are aware of heavy costs incurred by illness or decreased life expectancy.

Participants also criticized that due to the poor risk assessment carried out by the controller, the potential measures taken to address these risks were insufficient. Especially with regard to the communication of the data breach, the workshop participants were sceptical whether it would be possible for the hospital to reach all of the affected individuals, due to the fact that the patient's files dated back to the 1980s and the contact information of former patients may have since changed.

In order to improve the handling of personal data by the hospital, the participants argued that the hospital should process only the necessary information from the patient records and ensure proper pseudonymisation of these data. While pseudonymised data is still personal data in the sense of Article 4(2) GDPR, as an individual can still be identified with reference to the assignment function, pseudonymisation is a technical and organisational measure which helps to reduce the risks to the rights of individuals. Participants found that proper pseudonymisation should ensure that the individuals cannot be identified by the department carrying out the relevant research, i.e. the assignment function should remain in the department which initially collected the data, or, in order to provide an additional layer of security, be stored by a third party, which in turn has no access to the pseudonymised data. This would also serve to reduce the risk of a data breach, as it would be hard to identify individuals, if the data collected were reduced appropriately and perhaps randomized in order to hamper attempts to identify individuals by drawing inferences.

Case Study 2: Online Shop.

The online shop "Fancy Foods" offers its European customer a wide variety of delicacies. To get to know its 3.5 million customers better and attract new customers. Fancy Foods' management launched the application my favourite poison for mobile devices where people can share and rate their favourite recipes.

In order to be able to share their own recipes a user first has to answer five questions about personal eating habits and then consent to the Terms and Conditions (including privacy policy) of the app. In the next step the user can swipe to the left to like a picture and to the right to dislike a dish. Afterwards the user gains access to the liked recipes' list of ingredients and may add these to a personal cookbook or delete the recipe. In both cases, the user needs to select from a variety of reasons why the dish was chosen or erased, e.g. categories like allergies, religious diet limitations, love for sugar and sweets or childhood memories, before access to new pictures is granted. To purchase ingredients for a certain recipe online the app user may just enter an email address, a credit card number and shipping address or log into the online account.

In 2017, a leading health insurance company (HIC) started a project together with Fancy Foods to counter the effects of an unhealthy diet. Thus, Fancy Foods created a separate database accessible for HIC containing pseudonymised costumer profiles. Aside from a user-ID (instead of login credentials) the database contains the whole user profile including address, credit card number and the reasons for selection and rejection of all recipes. After the subsequent update (1st August 2018) every registered member of the Fancy Foods online shop automatically receives dishes chosen according to their individual health needs in their personal cookbook.

Task for Case Study 2. Due to a wrong setting in the database the ID is not permanently linked to the rest of a data set. After the next database access (18th August 2018) the mix-up was detected and the insurance company immediately informed "Fancy Foods". Fancy Foods' IT department fixed the problem this morning and re-established the link between ID and data set.

Assume the position of the controller and decide whether the mix up requires communication with the data subjects. Use the attached form for documentation.

Discussions on Case Study 2. The second case study is based on a different breach type. Instead of unwanted disclosure of personal data, here the integrity of the data is compromised. This approach was specifically chosen to raise the participants' awareness for varying incidents. The task for group II combined the practical application of Articles 33 as well as 34 GDPR and the risk assessment introduced at the beginning of the workshop.

The participants had no problem with the identification of the integrity breach as this was already hinted at in the task. Article 34(2) GDPR states which information must be included in the communication of a breach to the data subjects. It refers to Article 33(3)(b) to (d) GDPR. The group used all provided information to describe the

breach in as much detail as possible.[2] The counter measure re-establishment of the correct link between user ID and database was recognized as well. The distinction of awareness and occurrence was not debated. Yet, even with precise numbers some discussion was necessary. The affected individuals and records were at first set with 3.5 million, but then corrected to unknown. Here a few group members correctly objected to the figure of 3.5 million, because the database consists of the app-profiles and not the online shop costumers. The case did not state any user or download numbers concerning the app. Also the affected categories, in particular the special categories according to Article 9(1) GDPR, like data on health and religion, were correctly identified.

Aside from these special categories, the risk assessment required that aggravating factors given in the case description were discovered first, e.g. missing or insufficient IT-security measures and the unlawful processing. This was partly directed to the basic principles of data processing referred to in Article 5(1) GDPR. Several of these were violated by the processing. The first five questions about data subjects' personal eating habits represent an unlawful processing, because the users consent was given after these data were processed. Data minimisation in the app could be increased: It is questionable why the user always needs to justify the decision to store or delete a recipe. The getting-to-know-you purpose may as well be accomplished with less personal data.

Participants further found a violation of the purpose limitation principle poses the project with the health insurance company: The participants indicated the purpose change and the missing consent for the disclosure of data from the app and the online shop, but did not raise questions concerning the risk of disclosing the complete user profile to the insurance company. Due to the groups' lively exchange of arguments the aspects of the profiling could not be discussed any further. The unlawful processing would have been the second data breach in this case study. The joint controllers neither asked the users for consent nor did "Fancy Food" limit the access to the stored user data and user profiles. The available database consists of almost the same personal data as the user profiles. HIC therefore processes personal data not necessary for the purpose of countering the effects of an unhealthy diet. Contact information, credit card numbers and addresses are not covered by this purpose. However these categories enable the company to link their own costumer database to app users. This could lead to higher insurance fees for those who are branded as unhealthy eaters, because their risk to suffer from diet-related diseases may be considered higher. Policy holders with a similar lifestyle that do not use the app would not need to pay the higher fees.

The risk assessment in this case study was quite challenging for the group. Discrimination based on health or religious data processed was discussed only in the context of the processing within the app. However, further negative consequences related to the processing of the insurance company were not as easily recognized.

[2] The provided notification form differed in two aspects from the first one [see Table 1]. Number three only referred to the basic IT-security incidents and did not mention specific examples and number five included further communication channels.

Furthermore, the database mix up poses not only a risk to data protection but could even be fatal to “Fancy Food” costumers with food allergies: For three weeks registered online shop members automatically received recipes chosen in according to their health requirements. As the selected dishes were based on another person’s data and thus may have contained ingredients they could have caused an anaphylactic shock to the recipients who did not check the recipe.

A further risk of identity fraud can be identified with regard to the low level of security measures in the food ordering process. As no authentication procedure is mentioned, an attacker may use any email address, credit card and shipping address to order from the online store.

5 Conclusion

As can be seen from the introduction of the framework for the assessment of the risk to the rights and freedoms of natural persons, the GDPR introduces a new concept, which has been adopted from information security. However, it is important to stress that the concept has been adopted from its former context and has been fully adapted to the requirements of data protection law. This concerns most importantly the object of protection, which has shifted from the organisation using information technology to the protection of individuals subject to the processing of data. Like all data protection law, this concept thus serves to protect these individuals’ rights and interests.

From the practical exercise carried out by way of participants using the risk framework of the GDPR to assess data breaches in two case studies several lessons can be learned:

The risk assessment in case of a data breach is crucial. Firstly, the initial risk assessment which has to be carried out to conform to the responsibility of the controller and ensure the security of the processing under Articles 24 and 32 GDPR is important in order to determine measures which prevent a data breach from happening. Secondly, the measures to be taken in cases where a data breach has occurred are dependent on a comprehensive assessment of the risks emanating from the specific data breach in question.

Furthermore, the information contained in a notification to the supervisory authority is very limited and should be supplemented by the initial risk assessment carried out by the controller and include a description of the processing operation or, in cases of a high risk processing operation, the Data Protection Impact Assessment.

The notification process itself depends not only on a correct risk assessment but also the right timing, detection methods and were necessary the communication channel. While Articles 33 and 34 GDPR provide some clues for controllers as to if, when, and how to react in case of a data breach there are many instances in which standard procedures may not be applicable. The case study illustrated how controllers can fail to consider data protection risks arising from inside their own organisation. In these cases, the controller will be the single point of failure.

On the other hand, legislators need to reconsider their focus on the controller in terms of breach notification procedures. An unwilling or unknown controller leads to

a dead end in the notification process and leaves data subjects unprotected. Future work should thus develop ways to address this very practical issue for data subjects.

Acknowledgement

This work is partially funded by the German Federal Ministry of Education and Research through the project ‘Forum Privacy and Self-determined Life in the Digital World’, https://www.forum-privatheit.de/forum-privatheit-de/index.php and the project EIDI (efficient notification after digital identity fraud), https://itsec.cs.uni-bonn.de/eidi/.

References

1. Khaira, R., Rs 500, 10 minutes, and you have access to billion Aadhaar details, The Tribune of 4 January 2018, http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html
2. Barret, D., Yadron, D., Paletta, D., U.S. Suspects Hackers in China Breached About 4 Million People’s Records, Officials Say, Wall Street Journal of 5 June 2015, https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888
3. Donelly, L., Security breach fears over 26 million NHS patients, The Telegraph of 17 March 2017, https://www.telegraph.co.uk/news/2017/03/17/security-breach-fears-26-million-nhs-patients/
4. Swedish authority handed over 'keys to the Kingdom' in IT security slip-up, The Local of 17 July 2017, https://www.thelocal.se/20170717/swedish-authority-handed-over-keys-to-the-kingdom-in-it-security-slip-up
5. Goel, V., Perlroth, N., Yahoo Says 1 Billion User Accounts Were Hacked, New York Times of 14 December 2017, https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?action=Click&contentCollection=BreakingNews&contentID=64651831&pgtype=Homepage&_r=0
6. Haselton, T., Credit reporting firm Equifax says data breach could potentially affect 143 million US consumers, CNBC of 7 September 2017, https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html
7. Cadwalladr, C., Graham-Harrison, E., Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian of 17 March 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election?CMP=twt_gu
8. Ghorayshi, A., Ray, S., Grindr Is Letting Other Companies See User HIV Status And Location Data, BuzzFeedNews of 2 April 2018, https://www.buzzfeed.com/azeenghorayshi/grindr-hiv-status-privacy?utm_term=.oj8dJKebLJ#.hwOGAMBZKA

9. DSK, Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, https://www.datenschutzzentrum.de/artikel/1225-Kurzpapier-Nr.-18-Risiko-fuer-die-Rechte-und-Freiheiten-natuerlicher-Personen.html
10. ECJ, Judgment of 9 November 2010, Volker und Markus Schecke und Eifert, C-92/09 and C-93/09, ECLI:EU:C:2010:662, paras. 60-63.
11. Bieker, F., Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, Datenschutz und Datensicherheit (DuD) 2018, pp. 27-31
12. Bieker, F., Bremert, B., Hansen, M., Die Risikobeurteilung nach der DSGVO, Datenschutz und Datensicherheit (DuD) 2018, pp. 492-496
13. Friedewald, M. u.a. (2017), 'White Paper Datenschutz-Folgenabschätzung', 3rd edition, https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/ Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf
14. Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 of 3 October 2017, WP250rev.01, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
15. The Standard Data Protection Model (SDM), V.1.0 EN1 (2017), https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methodology_V1_EN1.pdf
16. Henseler-Unger, I., Hillebrand, A., Aktuelle Lage der IT-Sicherheit in KMU, Datenschutz und Datensicherheit (DuD) 2018
17. Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 of 3 October 2017, WP250rev.01, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
18. Malderle, T., Wübbeling, M., Knauer, S., Sykosch, A., Meier, M., Gathering and Analysing Identity Leaks for a proactive Warning of affected Users, Proceedings of the ACM International Conference on Computing Frontiers (CF '16). ACM, New York, NY, USA, 2018, https://itsec.cs.uni-bonn.de/eidi/files/malderle-cf18.pdf
19. EIDI, https://itsec.cs.uni-bonn.de/eidi/
20. Blinder, A., Perlroth, N., A Cyberattack Hobbles Atlanta, and Security Experts Shudder, New York Times of 27 March 2018, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html