MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

<02nd of March 2021>

Submission of comments on Guidelines 01/2021 on Examples regarding Data Breach Notification adopted on 14 January 2021 by the European Data Protection Board ("EDPB")

Comments from:

MyData-Trust

When DATA PROTECTION Meets Life Sciences

MyData-TRUST is a company registered under Belgian Laws, active since 2017 in the DATA PROTECTION area. Its Multi-Disciplinary Team includes Data Privacy Lawyers, IT Security Specialists and Clinical Experts providing GDPR related services (such as privacy risk assessments, external DPO as a service, etc.). Our clients include among others Pharmaceutical, Biotech and Medical Device companies, Contract Research Organisations (CROs), Healthcare providers and associations.

Key messages

MyData-Trust ("MD-T") salutes the adoption of the recent guidelines 01/2021 on Examples regarding data breach notification (hereinafter, the `` Guidelines``), but deems that despite the added value of this Guidelines, many uncertanties still exist and need further guidance to support Data Controllers and to improve their response in the management of such complex and sensitive events. MD-T would like to emphasise the following aspects (addressed in further details within the sections of general remarks and specific comments):

- ⇨ Case scenarios are very welcomed, but all situations cannot be described in a guideline. MD-T would advise EDPB to collaborate with ENISA on the update of the old guidelines drafted by ENISA[1] regarding the methodologies to apply in case of a data breach keeping in mind the GDPR approach. A synergy between EDPB and ENISA to develop a common methodology and common best practises on this matter would be very welcomed;
- ⇨ Uncertainties still remain regarding the liability in case of Joint-Controllership. Further clarifications with regard to the management of data breaches could be crucial in such case. For instance, MD-T believes that a solution would be the implementation of a risk evaluation grid. Furthermore, several pratical issues remain outstanding, especially with particular reference to the management of the notification by Joint-Controllers;
- ⇨ MD-T deems important to highlight the risk evaluation of minor breaches. For instance, a recurring reporting activity between the Data Controller and Data Processor could be, in certain cases, more adequate than just a notification within 72 hours. Moreover, the wording of the notion of 'awareness' may need to be nuanced regarding its scope, especially with particular reference to non-EEA companies;

[1] Recommendations for a methodology of the assessment of severity of personal data breaches Working Document, v1.0, December 2013

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

- ⇨ MD-T deems that harmonizing the different methodologies set for the data breach notification within the European Union would certainly enhance the integration process between the various national SA and their cooperation with the Data Controllers;
- ⇨ Further guidance would also be needed to clarify what standard internal documents are necessary to demonstrate compliance with GDPR in the event of data breaches, and their respective data retention period;
- ⇨ Considering the foreseeable difficult economic implications of the ongoing global pandemic, and the limited available resources for SA and Data Controllers, MD-T firmly believes that developing standard approaches, categorizations of incidents and drawing a line between the large and small risks is now more than ever crucial;
- ⇨ MD-T deems essential to provide further clarifications and guidance regarding the scope of the recommended communications to the data subjects. For instance, a sector-specific scenario or a non-exhaustive checklist where such communications are likely to be required could be really useful for Data Controllers;
- ⇨ Lastly, there is a lack of accuracy with regard to the role and duties of Supervisory Authorities that play a key-role in investigating data breaches. Additional rules should be enacted to ensure an effective monitoring to address personal data breaches;
- ⇨ Even though MD-T considers the examples listed in the Guidelines to be relevant, coherent and well-considered, the Annex 1 provides specific use cases aiming to illustrate scenarios occurring in the Life Science sector.

General remarks

First of all, MD-T salutes the adoption of the recent guidelines 01/2021 on Examples regarding data breach notification (hereinafter, the `` Guidelines``) with deep interest. The idea to complement the general guidelines on data breach notification adopted in October 2017 by the former Article 29 Working Party ("WP29") with practical examples on the subject is really welcomed, and MD-T would like to express its gratitude for the efforts made by the European Data Protection Board ("EDPB"). The Guidelines offer a very useful overview on the subject deriving from the common experiences of the Supervisory Authorities within the European Economic Area ("SA"). Moreover, its practical approach results undoubtedly to be a precious tool to advise Data Controllers on how to deal with the challenges posed by data breaches.

As well clarified by the Guidelines, Data Controllers face multiple challenges and risks when handling such complex events. Hence, it is fundamental to have a clear guidance on the factors to take into consideration when assessing the risks arising from a data breach and the measures to be taken to mitigate the potential harmful impact(s) on the organization(s) and the affected data subjects, especially when it is likely to result in a high risk to the rights and freedoms of natural persons. When addressing the issues created by data breaches, Data Controllers are exposed to internal and external pressure, and they are required to manage carefully the time limit imposed by the General Data Protection Regulation 2016/679 ("GDPR") for the data breach notification. Therefore, it is extremely important for Data Controllers to have in place a methodology to follow, and internal procedures to promptly address these critical events.

MD-T welcomes that EDPB underlined the importance to have a full log of all the breaches occurring within an organization (as, in our experience, many organisations do not properly

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

record minor breaches) and considers that the provided examples are very clear and well presented.
However, it would be important to provide even more examples of typical scenarios of minor data breaches and to further explain the need to keep such an exhaustive log, further to the need to demonstrate compliance in case of an audit request sent by a national SA. In our experience, the complete log of all breaches feeds the daily work of privacy teams and Data Protection Officers providing useful elements to monitor the effectiveness of the organisational and technical measures put in place, improving the quality of privacy impact assessments (by providing more objective way to evaluate the frequency of certain risks) and ensuring that the measures implemented are not only proportionate to the risk, but also take into account the likelihood of it.
The availability of additional practical examples and statistics from Regulators regarding the high and low risk breaches scenarios, would be very instructive for data protection practitioners and for public and private organizations as, on the one hand, they could be used to keep up to date the workforce regarding cybersecurity risks; on the other hand, they could be used by organizations as a benchmark to evaluate the implementation of internal security measures. Moreover, they could be used to have a better understanding of the notion of data breach and of the actions to be taken to manage and report these events to the relevant SA, and where applicable, to the affected data subjects. MD-T would advise EPDB to collaborate with ENISA on the update of the old guidelines drafted by ENISA[2] regarding the methodologies to apply in case of a data breach keeping in mind the GDPR approach. A synergy between EDPB and ENISA to develop a common methodology and common best practises on this matter would be very welcomed;

Specific comments:

1) Joint-Controllers Relationship

When two or more entities are considered as Joint-Controllers, they **shall determine their respective responsibilities** to comply with the GDPR, including determining which party will have responsibility **for complying with the obligations under Articles 33 and 34**. As per Guidelines on personal data breach notification adopted on 3 October 2017 by the WP29, the contractual arrangements between Joint-Controllers shall include provisions that determine which Data Controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.
MD-T deems that there are two different situations here.
Fist of all, according to the division of responsibilities, one Data Controller may act as the one responsible for complying with the obligations under Article 33 and 34 while the other is taking the role similar to the one of a Data Processor, by reporting any data breach and by meeting a duty of assistance (e.g., when the breach occurred in its own premises).
However, this first situation can be discussed and some uncertainties still remain.

[2] Recommendations for a methodology of the assessment of severity of personal data breaches Working Document, v1.0, December 2013

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

Does the fact that only one Data Controller will take the lead on, or be responsible for, compliance with data breach related obligations mean that the other Controller shall not take any part in the compliance with the obligations under Article 33 and Article 34? Considering the fact that both controllers may be held liable in case they are responsible for any damage caused by the processing activities, wouldn't it be better that Joint-Controllers cooperate together at least for the evaluation of the risks resulting fom a data breach in regards to the rights and freedoms of Data Subjects? The question also arises in view of the fact that the SA have the power to impose administrative fines. GDPR specifies that the contractual arrangements between Joint-Controllers are not opposable to the Data Subjects but it is unclear if the SA should or should not take into account the determination of responsibilities as set up in the contractual arrangements when exercising their power of imposing such fines.
Morevorer, both GDPR and EDPB remain silent about the following question: shall the Joint-Controllers agree within 72 hours on the risks arising from the data breach and on the decision to notify the breach or not?
Considering that these uncertainties are crucial in terms of liability, MD-T deems that further clarifications and examples are required regarding how a data breach should be managed in case of Joint- Controllers relationship as well as a better guidance on their responsibilities.
Furthermore, MD-T believes a solution would be that Joint-Controllers agree upstream on the identification of different data breaches scenarios that may occur during the processing operation as well as on a risk evaluation grid. Such upstream analysis may be attached to the contractual arrangements.
Another relevant situation is when a data breach extends over several processing activities, involving more than one processing operation of the entity suffering the breach and at the same time the processing operation for which that entity is considered as a Joint-Controller with another entity.
Let's take the example of an hospital victim of phishing. This results in unauthorised access to the hospital's databases including study data for which the Sponsor of the clinical study is considered as Joint-Controller with the hospital (despite the opinion of the EDPB as per Guidelines 07/2020 on the concepts of Data Controller and Processor, the qualification of an Investigator Site as Joint-Controller still exists in some EU countries in a clinical study context). The following questions remain: shall both Controllers make a separate notification? In that case, what could be the extent of each notification and how the Joint-Controllers are responsible to assess the likelyhood and the severity of the risks resulting from a data breach to the processing operation for which they are Joint-Controllers? Same question arises in regards to the case n°2 (see Annex 1) that MD-T chose to share in order to provide specific use cases concerning the Life science sector and specifically clinical trials. In order to avoid redundancy, more clarification on the responsibilities of both Controllers is essential.

2) Relationship Controller-Processor

In case of a data breach, a Data Processor has to comply with two kind of obligations: a duty of notification and a duty of assistance to the Data Controller (art 28 (3) f), art 33 (2) GDPR). This notification's requirement is crucial since it enables the Data Controller to take steps to address the breach and meet its breach-reporting duties.

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

As Data Controller has a limited time to notify the breach, WP29 recommends to consider the notion of "*without undue delay*" as an immediate notification. As per guidelines 07/2020 on the concepts of controller and processor, the EDPB goes further and recommends foreseeing a specific time frame through *number of hours* which varies between 24h and 48h. In practice, this time frame may be contractually required (ICO). This further guidance about the time frame gives a more concrete idea of the expectations regarding the notification. It is therefore regrettable that this is not included in the present guidelines. For more consistency, reemphasize the importance of this time frame in the context of data breach seems essential.

Moreover, MD-T deems important to clarify and insist about the risk evaluation. In principle, this evaluation is an obligation of the Data Controller but a delegation to the Data Processor is always possible. In the case of a delegation, the Data Processor shall notify all breaches to the Data Controller, including minor breaches. For the sake of practicality, Controller and Processor may agree upfront on the specific list of minor breaches (not requiring notification to SA or data subjects), where it may be practical to notify Data Controller regularly, but not within 72 hours. For instance, despite all the measures in place, in large corporations a misdirection of an e-mail to a trusted third party may occur with a certain frequency. Therefore, it may be more practical to notify the Data Controller (provided the existence of an agreement upfront) in a bundled manner and on a monthly basis. This way, the breach log will be completed regularly without creating overwhelming flows.

Furthermore, in principle, the Data Controller should be considered as “aware” once the Data Processor has become aware. According to WP29, the notion of awareness means “*having reasonable degree of certainty that a security breach has occurred and that has led to personal data being compromised”*. However, this wording still seems to have some shortcomings, especially when non-EEA companies are involved. In practice, a data breach starts from an incident or a suspicion of a breach. Given the example of the lost laptop, it shall first be determined if the laptop contains any personal data. In case of a breach occurred within non-EEA organizations, where only some of the data processing activities are under GDPR scope, organizations shall also determine if the breach is related to activities falling under GDPR scope. Therefore, it would be useful to clarify the term “aware” as “*it is likely reasonably to believe that the incident relates to the personal data and processing activities under GDPR scope*”.

3) Lack of harmonization regarding the form of the data breach notification

Another important aspect which is not taken into due account by articles 33 and 34 GDPR refers to the form of the data breach notification. As GDPR does not specify the means to be used to ensure a timely notification, each national SA has adopted different methodologies to enable notifications.

On the one hand, the approach of the European legislator can be considered positive in that it has left to the SA full decision-making autonomy concerning the application of GDPR on this specific point. On the other hand, however, the lack of harmonization may have a negative impact on Data Controllers frustrating their efforts to minimize the consequences deriving from a breach, and triggering the risk of a delayed notification. If the lead European SA (such as, ICO, CNIL, Garante and AEDP) offer online data breach self-assessment tools,

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

notification report mechanisms and a clear and informative description of the steps to be taken to complete it successfully, there are several others that do not ensure the same service levels.
Even though at first glance this may not be critical as breaches are reported to the lead SA, for Data Processors this may represent a hurdle. Processors may work with several Controllers reporting to different lead SA. Disrepancies, even minor in the content of the form, may lead to unnecessary delays in reporting if information is not readily available. This is the reason why it would be really beneficial to standardize the form of the notification and harmonize the procedures within the European Union. For instance, adopting a standard e-form for the notification. Perhaps, a practical tool as an open and common Q&A could be really helpful for organizations at stake. A standard approach would undoubtedly increase the support provided by the national SA and reduce the pressure posed by the time restriction of 72 hours on Data Controllers. Furthermore, it would facilitate the communication of breaches not only to the competent SA, but also to the affected data subjects.
Therefore, MD-T deems firmly that harmonizing the different methodologies at the EU level could be an additional step towards further integration between the various national SA, would give greater certainty to the actions to be taken to complete the notification process timely and successfully, and would also increase the support provided to Data Controllers in such a complex and sensitive events. To this purpose, we are calling for a close cooperation at European level to develop and adopt a common methodology on the issue.

4) The internal documentation of a breach

According to the Article 33 (5) GDPR, “the Controller shall document any personal data breach, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Supervisory Authority to verify compliance with this Article”.
Indeed, the importance to have internal documentation for compliance purpose is highligted by the Guidelines: “the internal documentation of a breach is an obligation independent of the risks pertaining to the breach, and must be performed in each and every case”. The internal documentation permits to assess the risk of harm but also makes Data Controllers accountable for their assessments by describing and documenting each incident. Therefore, it plays a key-role as an accountability mechanism. Moreover, this documentation enables the SA to review the compliance regarding the company's history of data breaches.
MD-T deems that there might be the need for further guidance under this standpoint.
First of all, no retention period has been set for this documentation. Although it might be difficult to establish a fixed retention period due to a variety of factors (such as, the different national approaches and legislations regulating the matter, or the regulatory requirements governing specific sectors), MD-T deems fundamental for Data Controllers to have a clear understanding on how to establish a reasonable retention period balancing the interests of Data Controllers, data subjects and the legal requirements. MD-T recommends keeping such a documentation, at least, for the period of time necessary to enable Data Controllers to protect their interests, with particular reference to potential complaints lodged by data subjects with a SA, or before the national civil courts for failing to comply with the obligations imposed by GDPR.

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

Secondly, no specific guidance has been given to clarify what documents are required to demonstrate compliance with GDPR. MD-T deems that establishing a standard checklist or templates for sector-specific situations may not only provide a better guidance to Data Controllers on how to comply with the principle of accountability and decrease the risk of non-observance of GDPR, but it would also constitute an effective measure to enhance the cooperation between the Data Controllers and the SA. In fact, on the one hand, it would decrease the workload of SA regarding the management of data breaches; and on the other hand, it would help Data Controllers to develop and strengthen an internal coordinated approach for the detection, investigation, and reporting of data breaches.
Lastly, considering the foreseeable difficult economic implications of the ongoing global pandemic, and the limited available resources for SA and Data Controllers, the need to develop standard approaches and categorizations of incidents is now more than ever crucial. There is a stringent need to ensure that all the available resources shall be primarily focused on the most serious incidents, and that a data breach shall be managed implementing the right countermeasures, especially when it implies a potential risk or high risk for the rights of the data subjects concerned.

5) A threshold for the risk assessment

Recitals 75 and 76 GDPR suggest that the assessment of the risks to the rights and freedoms of natural persons depends on both the likelihood and severity. It further states that risk should be evaluated on the basis of an objective assessment. To this end, WP29 recommends taking into account different criteria, notably, the number of affected individuals. As stated by the WP29 guidelines , “generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature and context of the personal data that has been compromised”.
As a general rule, the number of affected individuals can be crucial in determiningthe impact breach can have. Thanks to the EDPB’s case-based guidance, we have a better understanding about which number is likely to raise considerable concerns. However, in our view, a clarification is needed to draw a line between large and small risks and a difference (if any) between the risk to individual and impact of the breach overall. Therefore, it could be useful to clarify how the breach communication relates to the specific amount of affected individuals. MD-T understands numbers may be different depending on the context. However, EDPB can recommend, for example, that every organization clearly defines the parameters to evaluate a data breach and to assess objectively if a data breach occurred according to data by design principles.

6) Recommended communication to the data subject

GDPR states that “*when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall communicate the personal data breach to the data subject without undue delay*” (Art. 34 (1)).
However, EDPB provides two examples where, even though a breach may be unlikely to result in a high risk for individuals, the communication could still be recommended (e.g. when passwords are involved, exfiltration from business data from an employee).

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

In these cases, EDPB states that the communication could be a mitigating factor despite the fact there is no duty to do so. A clarification about these recommended communications could be useful. For instance, it is recommended to indicate the specific scenario or sector where a communication to the data subjects is likely to be required, or a non-exhaustive list of specified subject matters.
MD-T deems essential to have further guidance, for instance through a standard checklist for specific scenarios, especially in the clinical trials where the communication is far to be easy.

7) The duties of Supervisory Authorities

The competent SA play a key-role in investigating and deciding on data breaches. According to the Article 58 (2) GDPR, SA have a number of corrective measures at their disposal (warnings, reprimands, limitation, administrative fines…). As highlighted by both recital 87 GDPR and Article 34 (4) GDPR, such notification may result in an intervention of these authorities.
Their roles are highlighted but not well explained and described. Any expected time limit regulates the response from competent authorities. However, this response is essential in the management of the data breach. Furthermore, in case of no reaction from them, what are the consequences? Could we assume, after a specific deadline, that the case is closed? Within what period of time should the Data Controller provide additional information (when a notification is made step by step or when the additional information is requested by SA)? Finally, shouldn't Data Controllers keep the SA informed of the measures that are and will be taken to ensure that the breach does not recur? Don't the authorities have a role to play in defining and monitoring the measures?
Further guidance must be enacted to regulate and enforce rules regarding the role and duties of SA. These additional rules are crucial to ensure a consistent approach at the European level regarding the measures to be taken by organizations to address data breaches.

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

Annex 1 – Additional use cases

MD-T could contribute to the Guidelines providing specific use cases concerning the Life science sector and specifically clinical trials (though also relevant to other sectors using courriers or pseudonymous data):

Case N°1
Clinical Trial foresees the collection of pseudonymous data and, specifically in relation to the collection of the medical imaging data, Sponsor uses specialized validated softwares which enable pseudonymization of images uploaded by the Investigator site (images frequently have patient identifiers in the image itself and specialized softwares are altering this part of the image to hide this part before the image becomes available to the Sponsor). The validated software has 1% failure rate, meaning once every 100 properly pseudonymized images, one image could get to the Sponsor with parts of the patient name or hospital chart numbers still visible.
Sponsor has a standard procedure in place where this image is directly deleted and the Investigator site is asked to repeat the procedure (and during the second upload the image is pseudonymized adequately).
From our perspective, this data breach has been mitigated almost immediately through application of standard measures (privacy by design) and does not represent any risk to the data subjects.

Case N°2
Clinical Trial foresees the collection of pseudonymous data and, despite a clear instruction to protect patient identity, the Investigator by mistake mentions patient's initials in one of the text fields of the form.
Sponsor has a standard procedure in place where any data which are not allowed to be collected are directly deleted and the Investigator site is reminded to pay attention to keep patient's direct identifiers confidential.
From our perspective, this data breach has been mitigated almost immediately through the application of standard measures (privacy by design) and does not represent any risk to the data subjects.

Case N°3
Adequately pseudonymized limited extracts from medical records (as strictly relevant to the clinical trial) are sent by a registred courier (e.i. DHL, Fedex or any other) to the Sponsor. The courier is delivered to the wrong recipient (not otherwise in a contractual agreement with the Sponsor). The mistake is discovered one week later. The wrong recipient did not return the package to the courier and tells not knowing where it is.
It would be usefull to have a two teared clarification about this type of breach:

- risk evaluation (in our view it is a reportable breach – to SA or to SA and data subject depending on the nature and amount of data in the envelope);

- role and obligations of the courier:

MyData-TRUST S.A.
Boulevard Initialis 7
Boite 3 7000 Mons
legal@mydata-trust.com
+32 (0) 65 55 42 10
www.mydata-trust.com

- are they a processor or a third party in this scope (in our opinion they are a third party)?
- what are their obligations of reporting to the Data Controller, provided they may even not be aware that the package contain personal data (in our opinion yes, within 24 - 48 hours for the registered envelope)?

Case N°4

Data Controller (Sponsor) instructs the clinical site (Data Processor for the clinical trial, but Data Controller on its own of the handling of the patient medical file) to provide data relevant to the clinical trial.

The Clinical site, on its own initiative, provides more data than requested by the Sponsor (for the relevant data subjects). For example, upon receiving a question aiming to confirm the correctness of a piece of data, the Clinical site sends a pseudonymized extract of the patient medical file, containing too much information (instead of just answering the question). Sponsor immediately destroys the data and asks the Clinical site to provide the answer in the requested format and informs Clinical site's Data Protection Officer.

In our view, this is a data breach as it goes against the minimization principle for the receiving Data Controller and it is a non-authorised access to the patient medical file (so under the responsibility of the Clinical Site). However, provided mitigation measures, in our view there is no risk for the data subject.