MIC Datenverarbeitung GmbH
Hafenstraße 24
A-4020 Linz
Tel +43(70)77 84 96-0
Fax +43(70)77 84 96-600
E-Mail office@mic-cust.com

MIC Privacy Policy

Date: 10.02.2020

Version: 2.0

Document information

Change history

Version	Date	Description	Author	Status
1.0	17.04.2018	MIC Data Protection Policy	SU	final
2.0	10.02.2020	Additions to Data Protection Organisation and data protection impact assessment	SU	final

Table of contents

1 Objective

MIC respects the privacy of every individual and considers the protection of personal data a key issue.

Also, compliance with the statutory requirements relating to personal data collection and processing, which vary greatly from country to country, is of great importance to MIC, a globally operating business.

This document specifies the policy applicable at MIC on the basis of the General Data Protection Regulation (Regulation (EU) 2016/679) to ensure compliance with current legislation.

2 Scope

This Privacy Policy applies to all companies of the MIC Group and their employees.

The MIC Privacy Policy covers all personal data processed in the MIC Group.

All questions regarding data protection resp. problems/assumed data protection incidents can be reported to the following email address: f739c41d.mic.co.at@emea.teams.ms

3 Privacy principles

3.1 Lawfulness, fairness and transparency

Personal data shall be processed lawfully, according to the principles of good faith, and in a form intelligible to the data subject.

MIC shall inform the data subject about data processing operations within the scope of the rights of the data subject (see art. 6 below and the privacy policy on our website www.mic-cust.com).

3.2 Processing principles

3.2.1 Purpose limitation

MIC processes personal data exclusively for defined, clear and lawful purposes; the collected data is exclusively processed in a way compatible with the respective purpose.

3.2.2 Data minimization

MIC limits itself to the minimum of personal data which they need in the scope of a processing activity and its purpose. Where it makes sense, personal data will be anonymized and/or pseudonymized to a reasonable extent.

3.2.3 Data erasure

MIC stores personal data only as long as it is necessary to achieve the relevant purpose and/or as required by statutory requirements.

3.2.4 Accuracy and up-to-dateness

Personal data must be accurate and kept up to date, if necessary. MIC takes relevant measures to erase and/or rectify incomplete or inaccurate personal data.

3.2.5 Data security, integrity and confidentiality

MIC provides reasonable security for all personal data processed by MIC. Appropriate technical and organizational measures ensure that personal data is protected against unauthorized or unlawful processing, accidental loss or accidental destruction or accidental damage. For details please refer to the MIC Security Policy.

3.2.6 Accountability

MIC is responsible for compliance with the principles listed above and need to be able to demonstrate that compliance.

3.3 Lawful processing

MIC processes personal data only on the basis of a legal ground (for example contract, consent, legal obligation or legitimate interest) and only in the framework of the purpose covered thereby.

In the case of special categories of data MIC shall comply with the strict requirements of Art 9 and 10 GDPR.

4 Privacy by Design /Privacy by Default

In order to secure privacy of personal data it is necessary to consider that topic from the beginning of the development process. This means it is not enough to implement appropriate technical and organizational measures to protect data, but to think about privacy at the earliest stage of development.

Privacy by Designs means that organizations consider privacy at the initial design stages and throughout the complete development process of new products, processes or services.

Privacy by default means that if a system or service includes different choices on how much personal data should be shared the default settings should be the most privacy friendly ones.

MIC has incorporated these two concepts into its development process, which ensures that the development teams take appropriate measures in the relevant development phases.

Main points of the implementation of these concepts are:

- Strict access control polices on a need to know basis
- Deletion concepts covering logical and physical deletion (including providing services for deletion of specific data on customer's request)
- Working with pseudonyms where possible and appropriate

5 Privacy organization

To ensure the intended level of protection at MIC and compliance with the principles listed above an appropriate privacy organization must be put in place.

For the implementation of the privacy organization the structure in Figure 1 with the roles described was defined.

The statutory provisions do not require the appointment of a data protection officer and therefore no such appointment was made.

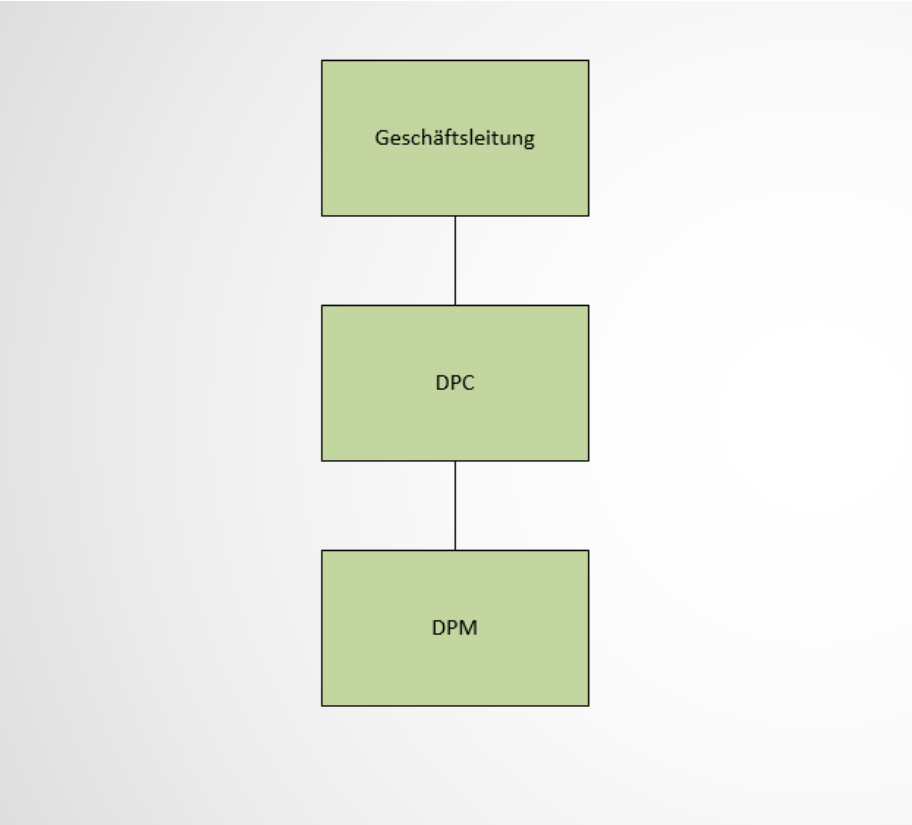

Fig. 1 – MIC data privacy structure

5.1 Roles and responsibilities

The core tasks and responsibilities of the major roles and functions in the company are defined below.

5.1.1 Management

The MIC Management is responsible for compliance with the General Data Protection Regulation and provides the necessary staff and financial resources.

5.1.2 Data Protection Coordinator (DPC)

The DPC is the point of contact for all privacy issues at MIC and bears the technical responsibility. The DPC is appointed by the management until further notice. The duties of the DPC include:

- Principal point of contact for all aspects relating to data privacy
- Definition of the privacy policies
- Ensuring compliance with the relevant statutory privacy provisions
- Investigation of privacy events, if any
- Verifying the implementation of the Data Protection Regulation

5.1.3 Data Protection Manager (DPM)

The DPM assists the DPC and acts as privacy contact person in the MIC Group. The DPM is appointed by the management until further notice. The duties of the DPM include:

- Contact person for all aspects relating to data privacy
- Collaboration in the drawing up the privacy policies
- Collaboration in the drawing up of all privacy-relevant documentations
- Implementation of the Data Protection Regulation
- Coordination of the subject areas data protection and data security
- Implementation of the technical and organizational measures
- Investigation of privacy events, if any

5.2 Requirements

For both the DCM and the DPM an appropriate qualification is required (e.g. certified data protection officer). Beside the data protection right specific qualification a good know how of the MIC process s is needed. DCM and DPM have – in cooperation with the MIC academy team – to take care for the preservation of the required knowledge. The MIC Management provides the necessary resources therefore.

5.3 Reporting

The data protection organisation reports directly to the management. Either in case of need or twice a year. Such report has to include all data protection relevant incidents, requests resp. changes.

It should be clarified that the DPC and the DPM do not receive any instructions regarding the exercise of their tasks. They shall not be dismissed or penalised for performing their tasks.

5.4 GDPR meetings

The Data Protection Coordinator and the Data Protection Manager will meet twice a year. The agenda for these meetings should contain the following topics.

- Discuss past data protection relevant events (Right of access, right of rectification, …) where MIC is the responsible party.
- Discuss past data protection relevant events (Right of access, right of rectification, …) where MIC is the data processor.
- Update this document and all other GDPR relevant documents if needed.
- Check if there were violations against the policies defined in this or other documents.

6 Rights of the data subject

6.1 General principles

Information and communications relating to the rights of data subjects shall be handled and ensured properly; therefore they shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The information shall be provided by electronic means, provided that this is possible and reasonable for the data subject, or else by other suitable means. The data subject has the right to request that the information is provided orally. Where the data subject makes the request by electronic form means, the information will usually be provided by electronic form means.

Unless the identity of the data subject is known to MIC it shall be verified, using strict standards; the person exercising such a right shall present identification (including, but not limited to, an official photo ID) to demonstrate that he or she is actually legitimized to exercise that right. Where clear identity verification is not possible, the data subject/inquirer will not be provided with any data and information; the inquirer shall be asked to submit appropriate identification.

The exercise and handling of a right of a data subject shall be documented, particularly as to

- the right that is being exercised and when,
- the data that is provided and when, and
- how the identity was checked and/or whether identity verification was not possible and why.

Moreover, any extension of time limit shall be documented. Such documentation will be stored securely in a suitable form and protected against unauthorized third party access for a period of 3 years.

The rights of the data subject will be fulfilled without undue delay but no later than within one month; in special cases (particularly complexity and/or number of rights of the data subject) the deadline may be extended by two months. In this case the data subject shall be informed about the extension of time limit in a suitable form in time before expiry of the time limit of one month.

Where the request for exercise of rights of the data subject is not met or not fully met, the data subject will be informed that he or she may lodge a relevant complaint with the Data Protection Authority or take legal action.

Where the rights of a data subject are exercised reasonably, the requests will be fulfilled free of charge; this will not be done in case of excessive or evidently unfounded requests. In these cases a request may either be fulfilled against payment of the costs actually incurred or the request may be declined.

Restricting the rights of a data subject, for example by dictating specific channels of communication for the access right, is prohibited.

Transferring information by email is permitted, provided that the confidentiality of transmitted data is ensured; this applies particularly to special categories of personal data according to Art 9 GDPR (e.g. “Bürgerpostfach”, “e-Brief”).

If the data subject wishes to exercise his or her right to rectification or erasure or restriction of processing of personal data, MIC will inform all recipients to whom the personal data was disclosed, unless this turns out to be impossible or involves a disproportionate effort.

Generally, the data subject must also appropriately and to a reasonable extent cooperate in the exercise of his or her right of a data subject (“duty to cooperate”).

6.2 Information to be provided on personal data, Art 13f GDPR

As distinguished from the right to information, which must be complied with on request of the data subject, MIC is required to automatically provide the data subject with specific information, unless

- the data subject already has the information or
- storage or disclosure of the personal data is expressly governed by legislation or
- informing the data subject is impossible or would involve a disproportionate effort, particularly in the case of processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

The information shall be made accessible to the data subjects either on a case-by-case basis or in the form of a general “privacy policy” (Art 13 and 14 GDPR).

In view of the good internet access availability it is safe to assume that the obligation to provide information to the data subjects can also be fulfilled via privacy policies on the website of the controller, provided that such policies are easy to find (cf. also WP260, 2016/679).

Where personal data are collected from the data subject, the data subject shall, at the time when personal data are obtained, be provided with all of the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller’s representative;

b) the purposes of the processing and the legal basis for the processing;

c) where the processing is based on legitimate interests, the concrete legitimate interests pursued;

d) the recipients or categories of recipients of the personal data, if any.

Additionally, the following further information shall be provided to ensure **fair and transparent processing**:

e) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

f) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing or to object to processing as well as the right to data portability;

g) where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

h) the right to lodge a complaint with a supervisory authority;

i) whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

Where personal data have not been obtained from the data subject, the data subject shall be provided with the following information at the latest within one month or, by earlier communication or disclosure to third parties, in addition to the information referred to above:

a) the categories of personal data concerned;

b) from which source the personal data originates, and if applicable, whether it came from publicly accessible sources.

The information obligation may not apply where storage or disclosure of the personal data is expressly governed by legislation.

6.3 Right of access by the data subject, Art 15 GDPR

The data subject has the right to obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, at his or her request access to the specific information according to Art 15 GDPR; the information from the register of processing operations can be used.

The right to be informed is a two-tier right:

a) the right to be informed as to whether or not personal data is stored ("negative information");

b) in the case of "positive information" the information specified above shall be provided.

MIC provides, free of charge, a copy of the personal data undergoing processing. For any further copies requested by the data subject, MIC may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, the copy of the information will be provided in a commonly used electronic form, unless the data subject requests being informed in a special but reasonable form.

In providing the information a distinction shall be made between information about the personal data and access to documents containing personal data; as to the latter information, GDPR provides for no right of access/right to be informed. In this connection it should be pointed out, for the sake of completeness, that a right of inspection of records as specified by § 17 General Administrative Procedure Act AVG - independently from the right of access under the GDPR - is in place in the public sector.

Also, information shall be provided as to whether special categories of personal data revealing race and ethnic origin, political opinions, religion or beliefs or trade union memberships are being processed, and whether genetic and biometric data for conclusive identification of a natural person, data concerning health or sex life or the sexual orientation of a natural person is undergoing processing (Art 9 GDPR).

Moreover, information shall be provided about information which directly or indirectly allows the identification of natural persons by means of reference to an identifier.

To allow the data subject to verify that his or her processed data is accurate, MIC is also obliged to provide the concrete content of the personal data, i.e. for example which first name or surname is specifically actually undergoing processing.

Thus MIC, under Art 15 para 3 GDPR, shall provide a copy of the personal data of the data subject, i.e. not only the data category but also the concrete personal data.

Where a large amount of data about the data subject is undergoing processing, the data subject has an obligation to specify – the data subject has the duty to cooperate!

6.3.1 How to process requests relating to the right to be informed

The data subject must be informed, **within one month** (this period may be prolonged for 2 months), about the EDP-supported processing or processing in hard copy filing systems affecting the data subject; the procedure for exercising the right to be informed is described below; **each of the steps below shall be durably recorded in terms of time and activity and kept for three years**:

(1) Date of receipt of the request for information and confirmation of receipt

(2) Verification of the identity of the applicant – a copy of an official photo ID must be submitted, unless the applicant is known to MIC

(3) Demanding an electronic mailing address to which the information will be sent or any other delivery medium requested by the data subject

(4) **Negative information** meaning no data is being processed, or the following information (**positive information**) to the electronic address disclosed in a common electronic format or other specifically requested medium:

a. the purposes of processing

b. the personal data undergoing processing and/or special categories of data

c. recipients or categories of recipients of the personal data

d. recipients in third countries or international organizations

e. where possible, the envisaged period of processing or the criteria used to determine that period

f. information as to the source of the personal data, where the data was not collected from the data subject;

g. the existence of automated decision-making, including profiling, and, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

(5) The following general communication:

"You have the right to request rectification or erasure or restriction of processing of your personal data or to object to a processing carried out for specific purposes.

You have the right to lodge a complaint to the Data Protection Authority about being treated unlawfully, according to your opinion, referring to the right to protection of your personal data; this applies particularly if you feel you are put at a disadvantage in connection with the exercise of the right to be informed.

You have to right to receive, once a year, a free copy of your personal data undergoing processing. For any further copies we may charge a reasonable fee based on administrative costs".

(6) Where the information is not provided, the data subject shall be informed without undue delay that the information will not be provided or restricted and why, e.g. inappropriate evidence of identity, misuse of the right to be informed.

6.4 Rectification, Art 16 GDPR

The data subject has the right to request the prompt (i.e. without undue delay)

▪ rectification or

▪ completion

of inaccurate or incomplete personal data concerning him or her. Thus the rule includes not only rectification but also completion of incomplete data.

Data rectification must also be kept in mind within the meaning of the principle of "data accuracy" according to Art 5 para 1 subpara d GDPR – thus MIC must ensure that data are accurate at all times, and, where applicable, keep them up to date.

6.4.1 How to process requests for rectification

A request for rectification shall be processed without undue delay; each of the steps below shall be durably recorded in terms of time and activity and kept for three years:

(1) Date of receipt of the request for information

(2) Checking the identity of the applicant – demanding a copy of an official photo ID, unless the applicant is known to MIC

(3) Demanding an official document showing that the dataset to be rectified is inaccurate

(4) Demanding an electronic or other address to which the information about the completion/refusal of rectification shall be sent

(5) Notification that the rectification was completed or the rectification was not performed and why

6.5 Erasure, Art 17 GDPR

The data subject has the right to obtain from MIC, without undue delay, the erasure of personal data concerning him or her where there is no longer a legal ground for the processing (including, but not limited to, contract, legitimate interest, legal/statutory obligation).

Where MIC has made the data public, MIC, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other processors that the data subject has requested erasure of any links to, or copy or replication of, those personal data.

The right to erasure shall not apply to processing operations necessary for exercising the right of freedom of expression or for compliance with a legal obligation or for the performance of a task carried out in the public interest or for the establishment, exercise or defense of legal claims.

Erasure does not necessarily mean physical deletion but may also comprise logical deletion. It is settled case-law that the Supreme Court of Justice OGH calls for physical erasure in any event when the data is/was collected/processed unlawfully.

In most cases a “request for erasure” by the data subject should be understood/interpreted as change of purpose because certain other grounds of justification for the processing (including, but not limited to, public interest, legitimate interests of the controller/third party or legal obligations) continue to exist. In these cases, physical erasure of the data will be impossible; rather the data access authorization will be adapted to the change of purpose (“logical deletion”).

6.5.1 How to process requests for erasure

A request for erasure shall be processed without undue delay; each of the steps below shall be durably recorded in terms of time and activity and kept for three years:

(1) Date of receipt of the request for information

(2) Checking the identity of the applicant – demanding a copy of an official photo ID, unless the applicant is known to MIC

(3) Demanding an electronic or other address to which the information about the completion/refusal of erasure shall be sent

(4) Checking the request for erasure with regard to:

a. **data collected and processed lawfully:**

   In this case the purposes of processing are in fact modified:

   Example: Dismissing an employee => removal of the active database, i.e. data shall be technically marked "deleted" but further stored, to the extent necessary, for other purposes provided for by law (e.g. issuing a testimonial, warranty and guarantee periods); change of the authorization concept.

b. **data collected and processed unlawfully**:

   i. Data must be "physically deleted".

   ii. This physical deletion shall also be implemented in the backups: Requests for erasure shall not be implemented in backups immediately but at the next possible point in time from an economic and technical point of view; until that point in time logical erasure in the backups (restricted access) is possible (§ 4 para 2 Data Protection Act DSG). It must be ensured, however, that the data to be deleted physically is not integrated into the current system again (activated), if the backup is reloaded.

(5) The **request for erasure shall not be met particularly** if the data is needed

a. for compliance with a legal obligation or

b. for the performance of a task carried out in the public interest or

c. for the exercise of official authority or

d. for reasons in the public interest in the area of public health or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(6) Informing the data subject as to whether or not the request for erasure was granted; if the request is refused, the reasons for the refusal must be given.

6.6 Right to restriction of processing, Art 18 GDPR

The data subject shall have the right to obtain restriction of processing where one of the following applies:

a) the accuracy of the personal data of the data subject is contested,

b) the processing is unlawful and the data subject requests the restriction of their use,

c) MIC no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims, or

d) the data subject has objected to processing and it is not confirmed yet whether the legitimate grounds of MIC override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the consent of the data subject or for the establishment, exercise or defense of legal claims. Before the restriction of processing is lifted, the data subject shall be informed. Other recipients shall be informed of the restriction of processing.

6.7 Right to data portability, Art 20 GDPR

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to MIC, in a structured, commonly used and machine-readable format or to request MIC to transmit those data to another controller, provided that

a) the processing is based on consent or a contract, and

b) the processing is carried out by automated means.

Thus the right to data portability shall not apply vis-à-vis controllers processing personal data for the performance of tasks carried out in the public interest. Nor shall it apply where processing of the personal data is necessary for compliance with a legal obligation to which MIC is subject or for the performance of a task carried out in the public interest assigned to MIC or in the exercise of official authority vested in MIC.

6.8 Right to object / Automated individual decision-making, Art 21f GDPR

The data subject shall have the right to object, on special grounds, at any time to processing of personal data which is based on a legitimate interest or in exercise of public authority, including profiling based on those provisions.

The processing shall be stopped unless MIC demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, particularly for the establishment, exercise or defense of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing including profiling to the extent that it is related to such direct marketing.

At the latest at the time of the first communication the right to object shall be brought to the attention of the data subject. This information shall be presented clearly and separately from any other information.

6.9 Notification obligation to recipients, Art 19 GDPR

It must be ensured that any restriction of processing or erasure or rectification of data is communicated to each data recipient, unless this proves impossible or involves disproportionate effort. The scope of the notification and/or why a notification to recipients is impossible or involves disproportionate effort in a specific case shall be documented.

The data subject shall be informed about the recipients to whom the data have been disclosed if the data subject requests it (see register of processing – Appendix); if this is impossible, it shall be properly documented.

6.10 Notification of personal data breach, Art 33f GDPR

In the case of a personal data breach which is likely to result in a high risk to the rights and freedoms of natural persons the data protection authority shall be notified (”**Data Breach Notification**”). As to the notification and/or communication obligation as defined by Art 33 and 34 GDPR, the following applies (cf. also WP250, 2016/679):

According to Art 33 GDPR notification of personal data breach to the data protection authority is required without undue delay, if possible within 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to result in a high risk to the rights and freedoms of natural persons.

If a processor becomes aware of a personal data breach, he or she shall notify MIC without undue delay.

In the case of a notification the data protection authority shall be provided with the following information:

a) a description of the type of personal data breach stating, if possible, the categories and the approximate number of the persons affected, the categories affected and the approximate number of the data sets affected;

b) the identities and the contact details of the internal contact point for further information;

c) a description of the likely consequences of the personal data breach;

d) a description of the measures undertaken or proposed by MIC to be undertaken to address the personal data breach and, where applicable, measures to mitigate their possible adverse effects.

According to Art 34 GDPR a personal data breach shall also be communicated to the data subject, if the breach is likely to result in a high risk to the rights and freedoms of **natural persons**. The communication shall be made without undue delay and describe in clear and plain language the nature of the personal data breach.

The communication shall not be required, if

a) MIC has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the breach, in particular those that make the personal data inaccessible to any person who is not authorized to access it, such as **encryption**; or

b) MIC has taken appropriate measures which ensure that the high risk to the rights and freedoms of the data subjects referred to in paragraph 1 breach is no longer likely to occur; or

c) it would involve disproportionate effort. In such case there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Where the data subject must be notified, the information referred to in b, c and d shall be provided.

6.10.1 Data breach notification procedure

According to Art 33 and/or 34 GDPR a personal data breach must under certain conditions be notified to the data protection authority **no later than 72 hours after having become aware of it and/or without undue delay** after becoming aware of it to the data subjects as follows:

1. In the case of a personal data breach (because e.g. a USB stick or any other storage device was lost or a laptop was stolen) which does **not result in a risk to** the rights/freedoms of the data subjects, **no notification shall be required**, i.e. neither to the authority nor to the data subject. For example, where storage devices containing personal data but with appropriate protection against unauthorized access (e.g. encryption or secure password) are lost or stolen.

2. In the case of a personal data breach (because e.g. a USB stick or any other storage device was lost or a laptop was stolen) which **results in a risk to** the rights/freedoms of the data subjects, **such a breach shall be notified to the data protection authority but not communicated to the data subjects (Art 33 GDPR)**. For example, where no reasonable protection against unauthorized access to the personal data is in place but the data concerned is not a special category of data (Art 9 GDPR = data concerning health etc.) or data going beyond mere master data or data that is particularly important to a data subject through its combination with other accessible data.

3. In the case of a personal data breach (because e.g. a USB stick or any other storage device was lost or a laptop was stolen) which **results in a risk to** the rights/freedoms of the data subjects, **the breach shall be notified to the data protection authority (Art 33 GDPR) and without undue delay to the data subjects (Art 34 GDPR)**. For example, where no reasonable protection against unauthorized access to special categories of personal data (Art 9 GDPR = data concerning health etc.) or to data going beyond mere master data or to data that is particularly important to a data subject through its combination with other accessible data (e.g. because behavior patterns or profiles of the data subjects could be created from them) is in place.

The following information shall be notified to the data protection authority no later than 72 hours after having become aware of the breach in the case of a risk to the data subjects:

a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) the name and contact details of a contact point where more information can be obtained;

c) a description of the likely consequences of the personal data breach;

d) a description of the measures taken or proposed by MIC to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The following information shall be communicated to the data subject without undue delay in the case of a high risk to the data subjects:

a) the name and contact details of a contact point where more information can be obtained;

b) a description of the likely consequences of the personal data breach;

c) a description of the measures taken or proposed by MIC to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The considerations leading to a notification or no notification to the data protection authority and/or the data subjects shall be durably recorded and kept for at least three years.

7 Assesment of impact

According to art 35 GRPD an assessment of impact has to be carried out, when a type of processing

- in particular using new technologies
- and taking into account the nature, scope, context and purposes of the processing
- is likely to result in a high risk to the rights and freedoms of natural persons

Right now there is not need to do an assessment of impact within MIC, this is also documented in our data processing register. If any data protection which requires an assessment of impact will get relevant, this will be carried out by the MIC data processing organisation in cooperation with our external specialist for data protection questions.