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

H:\texte\security\DSGVO\MIC Datenschutzrichtline.doc

Change history

Version	Date	Description	Autor	Status
1.0	17.04.2018	Datenschutzrichtline	SU	final
2.0	10.02.2020	Ergänzungen Datenschutzorganisation und Datenschutzfolgenabschätzung	SU	final

Table of contents

1 Ziel 5

2 Geltungsbereich 5

3 Datenschutzprinzipien 5

3.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz 5

3.2 Verarbeitungsgrundsätze 5

3.2.1 Zweckbindung 5

3.2.2 Datenminimierung 6

3.2.3 Datenlöschung 6

3.2.4 sachliche Richtigkeit und Aktualität 6

3.2.5 Datensicherheit, Integrität und Vertraulichkeit 6

3.2.6 Rechenschaftspflicht 6

3.3 Rechtmäßigkeit der Verarbeitung 6

4 Privacy by Design /Privacy by Default 7

5 Datenschutzorganisation 8

5.1 Rollen und Verantwortlichkeiten 8

5.1.1 Geschäftsleitung 8

5.1.2 Data Protection Manager (DPM) 9

5.2 Voraussetzungen 9

5.3 Reporting 9

5.4 GDPR meetings 10

6 Betroffenenrechte 11

6.1 Allgemeine Grundsätze/Prinzipien 11

6.2 Informationspflicht zu personenbezogenen Daten, Art 13f DSGVO 12

6.3 Auskunftsrecht der betroffenen Person, Art 15 DSGVO 14

6.3.1 Auskunftsprozess 15

6.4 Berichtigung, Art 16 DSGVO 17

6.4.1 Berichtigungsprozess 17
6.5 Löschung, Art 17 DSGVO 18
6.5.1 Löschungsprozess 18
6.6 Recht auf Einschränkung der Verarbeitung, Art 18 DSGVO 20
6.7 Recht auf Datenübertragbarkeit, Art 20 DSGVO 21
6.8 Widerspruchsrecht / autom. Entscheidungsfindung im Einzelfall, Art 21f DSGVO 22
6.9 Mitteilungspflicht gegenüber Empfängern, Art 19 DSGVO 23
6.10 Meldung von Datenschutzverletzungen, Art 33f DSGVO 24
6.10.1 Prozess zur data breach notification 25
7 Datenschutzfolgenabschätzung 27

1 Ziel

MIC respektiert die Privatsphäre des Einzelnen und sieht damit verbunden den Schutz personenbezogener Daten als wichtiges Thema an.

MIC als global tätiges Unternehmen ist es außerdem ein großes Anliegen den weltweit unterschiedlichen gesetzlichen Anforderungen, die mit der Erhebung und Verarbeitung personenbezogener Daten verbunden sind, zu entsprechen.

In diesem Dokument sollen basierend auf der Datenschutzgrundverordnung (Verordnung (EU) 2016/679) die innerhalb der MIC anzuwendenden Prinzipien festgelegt werden und so die Einhaltung der rechtlichen Vorgaben sichergestellt werden.

2 Geltungsbereich

Diese Datenschutzrichtlinie gilt für alle Unternehmen der MIC Gruppe und deren Mitarbeiter.

Die MIC Datenschutzrichtlinie deckt die Verarbeitung sämtlicher personenbezogener Daten in der MIC Gruppe ab.

Alle Fragen zu Datenschutzthemen bzw. Auffälligkeiten/vermutete Datenschutzprobleme können per email an folgende email Adresse gerichtet werden: f739c41d.mic.co.at@emea.teams.ms

3 Datenschutzprinzipien

3.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Alle personenbezogenen Daten müssen auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

MIC informiert den Betroffenen im Rahmen der Betroffenenrechte über stattfindende Datenverarbeitungen (sh. unten Punkt 6 sowie die Datenschutzerklärung auf unserer website www.mic-cust.com).

3.2 Verarbeitungsgrundsätze

3.2.1 Zweckbindung

MIC verarbeitet personenbezogene Daten ausschließlich für festgelegte, eindeutige und rechtmäßige Zwecke, eine Verarbeitung der erhobenen Daten erfolgt ausschließlich in Abhängigkeit zum relevanten Zweck.

3.2.2 Datenminimierung

MIC reduziert die Verarbeitung von personenbezogenen Daten auf das Notwendige. Ziel ist es, nur jene Daten zu verarbeiten, die zur Erreichung des angestrebten Zweckes benötigt werden. Soweit sinnvoll und mit vertretbarem Aufwand möglich, wird von der Möglichkeit der Anonymisierung bzw. Pseudonymisierung Gebrauch gemacht.

3.2.3 Datenlöschung

MIC behält personenbezogene Daten nur solange auf, als es die Erreichung des entsprechenden Zweckes erfordert bzw. gesetzliche Vorschriften dies vorgeben.

3.2.4 sachliche Richtigkeit und Aktualität

Personenbezogenen Daten müssen sachlich richtig sein und gegebenenfalls auf den neuesten Stand gebracht werden. MIC trifft entsprechende Maßnahmen, um nicht vollständige oder unrichtige Daten zu löschen bzw. zu aktualisieren.

3.2.5 Datensicherheit, Integrität und Vertraulichkeit

MIC sorgt für die angemessene Sicherheit aller personenbezogenen Daten, die von MIC verarbeitet werden. Durch geeignete technische und organisatorische Maßnahmen wird sichergestellt, dass personenbezogenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind. Details dazu können der MIC Security Policy entnommen werden.

3.2.6 Rechenschaftspflicht

MIC ist für die Einhaltung der oben genannten Prinzipien verantwortlich und muss deren Einhaltung nachweisen können.

3.3 Rechtmäßigkeit der Verarbeitung

MIC verarbeitet personenbezogene Daten nur, wenn dafür ein Rechtmäßigkeitsgrund vorliegt (beispielweise Vertrag, Einwilligung, rechtliche Verpflichtung oder berechtigtes Interesse) und nur im Rahmen des dadurch abgedeckten Zweckes.

Im Falle von besonderen Datenkategorien hält sich MIC an die strengen Vorgaben des Art 9 und 10 DSGVO.

4 Privacy by Design /Privacy by Default

Um den Schutz personenbezogener Daten zu gewährleisten, ist es notwendig, dieses Thema von Beginn des Entwicklungsprozesses an zu berücksichtigen. Das bedeutet, dass es nicht ausreicht, geeignete technische und organisatorische Maßnahmen zum Schutz der Daten zu ergreifen, sondern dass man sich bereits in der frühesten Phase der Entwicklung Gedanken über den Datenschutz machen muss.

Privacy by Designs bedeutet, dass Organisationen den Datenschutz bereits in den ersten Entwurfsphasen und während des gesamten Entwicklungsprozesses neuer Produkte, Verfahren oder Dienstleistungen berücksichtigen.

Datenschutz durch Voreinstellung bedeutet, dass, wenn ein System oder eine Dienstleistung verschiedene Wahlmöglichkeiten bietet, wie viele personenbezogene Daten weitergegeben werden sollen, die Standardeinstellungen die datenschutzfreundlichsten sein sollten.

MIC hat diese beiden Konzepte in seinen Entwicklungsprozess integriert, wodurch sichergestellt wird, dass die Entwicklungsteams in den jeweiligen Entwicklungsphasen geeignete Maßnahmen ergreifen.

Die wichtigsten Punkte bei der Umsetzung dieser Konzepte sind:

- Strenge Zugriffskontrollrichtlinien auf der Basis von "need to know “
- Löschkonzepte für die logische und physische Löschung (einschließlich der Bereitstellung von Diensten für die Löschung bestimmter Daten auf Kundenwunsch)
- Arbeit mit Pseudonymen, wo möglich und sinnvoll

5 Datenschutzorganisation

Um das angestrebte Datenschutzniveau in der MIC sowie die Einhaltung der oben angeführten Prinzipien sicherzustellen, ist ein Aufbau einer entsprechenden Datenschutzorganisation erforderlich.

Für die Umsetzung der Datenschutzorganisation wurde die in Abbildung 1 ersichtliche Organisationsstruktur mit den angeführten Rollen festgelegt.

Die Bestellung eines Datenschutzbeauftragten ist aufgrund der gesetzlichen Vorgaben nicht notwendig und folglich nicht erfolgt.

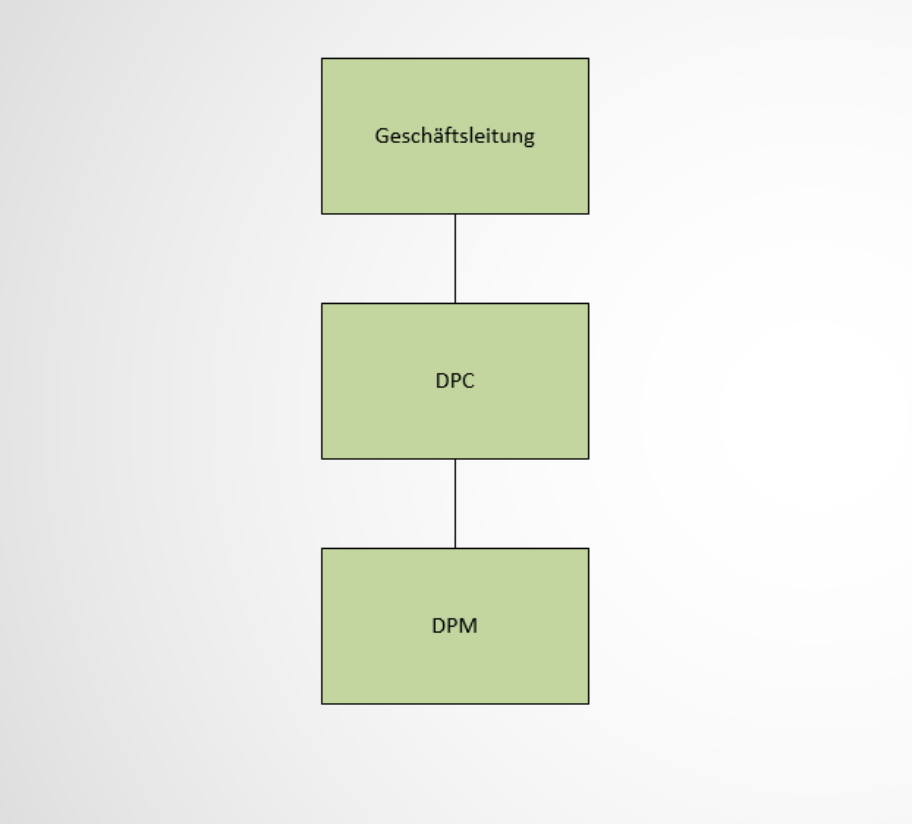

Abbildung 1 – MIC Datenschutzorganisation

5.1 Rollen und Verantwortlichkeiten

Nachfolgend werden die Kernaufgaben und -verantwortlichkeiten der wichtigsten Rollen und Funktionen im Unternehmen festgelegt.

5.1.1 Geschäftsleitung

Die Geschäftsleitung der MIC verantwortet die Einhaltung der Datenschutzgrundverordnung und stellt dazu die benötigten personellen und finanziellen Ressourcen zur Verfügung. Data Protection Coordinator (DPC)

Der DPC ist die zentrale Ansprechperson für alle Datenschutzthemen innerhalb der MIC und trägt die fachliche Verantwortung. Der DPC wird bis auf Widerruf von der Geschäftsleitung bestellt. Aufgaben und Pflichten des DPC sind:

- Hauptansprechpartner für alle Aspekte rund um das Thema Datenschutz
- Festlegung der Datenschutzprinzipien
- Sicherstellung der Einhaltung der datenschutzrechtlich relevanten gesetzlichen Vorschriften
- Untersuchung eventueller Datenschutzvorfälle
- Überprüfung der Umsetzung der Datenschutzrichtline

5.1.2 Data Protection Manager (DPM)

Der DPM unterstützt den DPC und dient als Ansprechpartner für das Thema Datenschutz in der MIC Gruppe. Der DPM wird bis auf Widerruf vom der Geschäftsleitung bestellt. Aufgaben und Pflichten des DPM sind:

- Ansprechpartner für alle Aspekte rund um das Thema Datenschutz.
- Mitwirkung bei der Erstellung der Datenschutzprinzipien
- Mitwirkung bei der Erstellung aller datenschutzrechtlich relevanten Dokumentationen
- Umsetzung der Datenschutzrichtline
- Koordination der Themenbereiche Datenschutz und Informationssicherheit
- Umsetzung der technischen und organisatorischen Maßnahmen
- Untersuchung eventueller Datenschutzvorfälle

5.2 Voraussetzungen

Sowohl für die Rolle des DCM als auch des DPM wird eine einschlägige Ausbildung (Bsp. Ausbildung zum Datenschutzbeauftragten) vorausgesetzt. Neben den darin vermittelten datenschutzrechtlichen Grundkenntnissen ist eine gute Kenntnis der MIC-internen Abläufe notwendig. Der DCM und er DPM haben für die Erhaltung des datenschutzrelevanten Fachwissen Abstimmung mit dem MIC Academy Team Sorge zu tragen. Die Geschäftsleitung stellt dafür die notwendigen Ressourcen zur Verfügung.

5.3 Reporting

Das Datenschutzteam reported direkt an die Geschäftsleitung. Eine Meldung hat im Bedarfsfall zu erfolgen. Darüber hinaus soll halbjährlich eine Meldung über die datenschutzrechtlich relevanten Vorfälle, Anfragen bzw. Änderungen erfolgen.

Es wird hiermit klargestellt, dass der DPC sowie der DPM bei der Erfüllung ihrer Aufgaben keine Anweisungen bezüglich der Ausübung der ihnen übertragenen Aufgaben erhalten. Aufgrund der Erfüllung dieser Aufgaben darf weder eine Abberufung noch eine Benachteiligung erfolgen.

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 (in particular “Verarbeitungsverzeichnis”)
- Check if there were violations against the policies defined in this or other documents.

6 Betroffenenrechte

6.1 Allgemeine Grundsätze/Prinzipien

Um die Informationen und Mitteilungen im Zusammenhang mit den Betroffenenrechten ordnungsgemäß abzuwickeln und sicherzustellen, sind diese in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Diese Mitteilungen erfolgen grundsätzlich in elektronischer Form, sofern dies für den Betroffenen möglich und sinnvoll ist, ansonsten in einer anderen geeigneten Art und Weise. Dem Betroffenen steht dabei auch das Recht zu, die Informationen mündlich einzufordern. Werden die Betroffenenrechte in elektronischer Form eingefordert, wird dies in der Regel auch in elektronsicher Form bearbeitet.

In jedem Fall muss durch Vorlage eines Identitätsnachweises (insb. amtlicher Lichtbildausweis) sichergestellt werden, ob die Rechte auch von der dazu berechtigten Person ausgeübt werden, es sei denn die Identität des Betroffenen ist amtsbekannt; an die Identitätsüberprüfung sind dabei strenge Maßstäbe zu setzen. Ist daher eine einwandfreie Identitätsfeststellung nicht möglich, werden dem Betroffenen/Anfragenden keine Daten und Auskünfte herausgegeben/erteilt; der Anfragende ist vielmehr aufzufordern geeignete Identitätsnachweise vorzulegen.

Die Geltendmachung und Abwicklung eines Betroffenenrechts wird dokumentiert, insbesondere mit Blick darauf,

- welches Recht wann geltend gemacht wird,
- welche Daten wann herausgegeben werden und
- wie die Identitätsüberprüfung erfolgt ist bzw. ob eine Identitätsfeststellung nicht möglich war und warum.

Zudem ist eine allfällige Fristverlängerung zu dokumentieren. Diese Dokumentation wird für die Dauer von 3 Jahren in geeigneter Weise, sicher und vor Zugriff von unberechtigten Dritten geschützt, aufbewahrt.

Den Betroffenenrechten wird unverzüglich, längstens jedoch binnen eines Monats, nachgekommen; in besonderen Fällen (insb. Komplexität und/oder Anzahl von Betroffenenrechten) kann diese Frist um zwei Monaten verlängert werden. In diesem Fall wird der Betroffene rechtzeitig vor Ablauf der Monatsfrist in geeigneter Weise über die Fristverlängerung informiert.

Wird der Geltendmachung der Betroffenenrechte nicht oder nicht vollständig nachgekommen, wird der Betroffene darüber informiert, dass er dagegen bei der Datenschutzbehörde eine diesbezügliche Beschwerde einlegen oder gerichtliche Schritte ergreifen kann.

Den berechtigter Weise geltend gemachten Betroffenenrechten wird unentgeltlich nachgekommen; dies gilt nicht bei exzessiven oder offenkundig unbegründeten Anträgen. In diesen Fällen kann entweder dem Antrag nachgekommen, dafür aber die tatsächlich entstandenen Kosten vorgeschrieben werden, oder die Erfüllung des Antrags abgelehnt werden.

Unzulässig ist es die betroffenen Rechte für die Betroffenen zu beschränken, indem beispielweise nur bestimmte Kommunikationskanäle für das Auskunftsrecht vorgegeben werden.

Eine Auskunftserteilung per Email ist zulässig, wenn die Vertraulichkeit der übermittelten Daten sichergestellt ist, dies gilt insbesondere bei besonderen Kategorien von personenbezogene Daten nach Art 9 DSGVO (z.B. Bürgerpostfach, e-Brief).

Begehrt der Betroffene das Recht auf Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung, so informiert der MIC alle Empfänger, denen die personenbezogenen Daten offengelegt wurden, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden

Ganz generell gilt allerdings, dass auch die betroffene Person bei der Ausübung ihrer Betroffenenrechte in angemessener Weise und im zumutbaren Umfang mitzuwirken hat („Mitwirkungspflicht“).

6.2 Informationspflicht zu personenbezogenen Daten, Art 13f DSGVO

Im Unterschied zum Auskunftsrecht, dem auf Anfrage des Betroffenen zu entsprechen ist, hat der MIC von sich aus dem Betroffenen bestimmte Informationen zukommen zu lassen, es sei denn

- der Betroffene verfügt bereits über diese oder
- die Speicherung oder Offenlegung der personenbezogenen Daten ist ausdrücklich durch Rechtsvorschriften geregelt oder
- die Unterrichtung der betroffenen Person sich als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist, insbesondere bei der Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

Die Informationen sind den Betroffenen entweder im Einzelfall zugänglich zu machen, oder aber in Form einer allgemeinen „Datenschutzerklärung“ (Art 13 und 14 DSGVO).

Aufgrund der guten Zugänglichkeit und Verfügbarkeit von Internet ist davon auszugehen, dass er Informationsverpflichtung gegenüber den betroffenen Personen auch in Form von Datenschutzerklärungen auf der Website des Verantwortlichen nachgekommen werden kann, sofern diese gut auffindbar sind (vgl. dazu auch WP260, 2016/679).

Werden personenbezogene Daten bei der betroffenen Person erhoben, so wird diesem zum Zeitpunkt der Erhebung Folgendes mitgeteilt:

a) Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) die Zwecke, für die die personenbezogenen Daten verarbeitet werden und die Rechtsgrundlage für die Verarbeitung;

c) wenn die Verarbeitung auf dem Vorliegen berechtigter Interessen beruht, die konkreten berechtigten Interessen, die verfolgt werden;

d) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.

Zudem sind zur Sicherung einer **fairen und transparenten Verarbeitung** folgende Informationen zu geben:

e) die Dauer, für die die personenbezogenen Daten gespeichert werden oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

f) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

g) wenn die Verarbeitung auf einer Einwilligung beruht, den Umstand, dass die Einwilligung jederzeit widerrufen werden kann, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

h) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

i) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen und welche möglichen Folgen die Nichtbereitstellung hätte und

Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so ist längstens binnen Monatsfrist oder mit einer allenfalls früheren Kommunikation oder Offenlegung an Dritte über Folgendes zusätzlich zu obigen Infos zu informieren:

a) die Kategorien personenbezogener Daten, die verarbeitet werden;

b) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen.

Die Informationspflicht kann allerdings entfallen, wenn die Speicherung und Verarbeitung von Daten durch Rechtsvorschriften geregelt ist.

6.3 Auskunftsrecht der betroffenen Person, Art 15 DSGVO

Dem Betroffenen ist zu bestätigen, ob ihn betreffende personenbezogene Daten verarbeitet werden, und wenn ja, sind ihm auf Verlangen spezifische Informationen nach Art 15 DSGVO zu geben, wobei dazu die Angaben aus dem Verarbeitungsverzeichnis herangezogen werden können.

Das Auskunftsrecht ist also zweistufig:

a) Zunächst ist eine Auskunft zu geben, ob Daten gespeichert sind oder nicht („Negativauskunft“);

b) im Falle einer „Positivauskunft“ sind die oben angegebenen Informationen zu erteilen.

MIC stellt dazu auch kostenlos einmalig eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann MIC ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Wenn die betroffene Person den Antrag elektronisch stellt, so wird die Kopie der Informationen in einem gängigen elektronischen Format zur Verfügung gestellt, es sei denn der Betroffene verlangt eine besondere, aber angemessene Form der Auskunftserteilung.

Bei der Auskunftserteilung ist zwischen Auskunft über die personenbezogenen Daten einerseits und den Zugang zu Dokumenten, die personenbezogene Daten enthalten, andererseits zu differenzieren; hinsichtlich der zuletzt genannten Informationen besteht kein Zugangs-/Auskunftsrecht nach der DSGVO. In diesem Zusammenhang sei allerdings der Vollständigkeit halber auf das im öffentlichen Bereich existierende Recht auf Akteneinsicht nach § 17 AVG verwiesen, das vom Auskunftsrecht nach der DSGVO unabhängig existiert.

Auskunft ist auch darüber zu geben, ob besondere Kategorien personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, verarbeitet werden, sowie ob eine Verarbeitung von genetischen und biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person erfolgt (Art 9 DSGVO).

Zudem ist Auskunft über Informationen zu geben, die direkt oder indirekt mittels Zuordnung zu einer Kennung eine Identifizierung von natürlichen Personen ermöglicht.

Um dem Betroffenen es zu ermöglichen, dass er die von ihm verarbeiteten Daten auch auf Richtigkeit überprüfen kann, ist MIC auch verpflichtet den konkreten Inhalt der personenbezogenen Daten zu beauskunften, also z.B. welcher Vorname oder Nachname im Konkreten tatsächlich verarbeitet wird.

Insgesamt hat MIC nach Art 15 Abs 3 DSGVO eine Kopie der personenbezogenen Daten des Betroffenen herauszugeben, also nicht nur die Datenkategorie, sondern die konkreten personenbezogenen Daten.

Wird allerdings eine große Menge an Daten über die betroffene Person verarbeitet, trifft diese eine Präzisierungsobliegenheit – der Betroffene hat eine Mitwirkungspflicht!

6.3.1 Auskunftsprozess

Den betroffenen Personen ist **binnen eines Monats** (Verlängerungsmöglichkeit um 2 Monate) über die sie betreffenden automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell geführten Dateien Auskunft zu geben; der Auskunftsprozess ist wie folgt durchzuführen, wobei **jeder der nachfolgenden Schritte hinsichtlich Zeitpunkt und Tätigkeit entsprechend dauerhaft zu protokollieren und dieses Protokoll drei Jahre lang aufzubewahren**:

(1) Datum des Einlangens des Auskunftsbegehrens und Bestätigung des Einlangens

(2) Prüfung der Identität des Antragstellers – einfordern einer Kopie eines amtlichen Lichtbildausweises, es sei denn der Anspruchsteller ist amtsbekannt

(3) Einfordern einer elektronischen Zustelladresse für die Auskunft oder sonstiges vom Betroffenen gewünschtes Zustellmedium

(4) **Negativauskunft**, weil keine Daten verarbeitet werden, oder Übermittlung folgender Informationen (**Positivauskunft**) an die bekanntgegebene elektronische Adresse in einem gängigen elektronischen Format oder sonst speziell gewünschten Medium:

a. Verarbeitungszweck

b. die personenbezogenen Daten die verarbeitet werden bzw. besondere Kategorien von Daten

c. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

d. allenfalls Empfänger in Drittländern oder bei internationalen Organisationen

e. falls möglich die geplante Dauer der Verarbeitung oder Kriterien für die Festlegung der Dauer

f. Informationen über die Herkunft der personenbezogenen Daten, wenn die Daten nicht bei der betroffenen Person erhoben wurden;

g. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und wenn ja, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen

(5) folgende allgemeine Mitteilung:

„Sie haben grundsätzlich das Recht im Zusammenhang mit den Sie betreffenden personenbezogenen Daten die Berichtigung oder Löschung oder Einschränkung der Verarbeitung zu verlangen sowie Widerspruch gegen eine bestimmte Verarbeitung einzulegen.

Sie haben zudem das Recht, sich bei der Datenschutzbehörde über Ihrer Meinung nach im Zusammenhang mit dem Recht auf Schutz Ihrer personenbezogenen Daten unberechtigte Behandlung zu beschweren; das gilt insbesondere, wenn Sie sich im Zusammenhang mit der Geltendmachung des Auskunftsrechts benachteiligt fühlen.

Sie haben das Recht, einmal im Jahr, eine kostenlose Kopie über den Gegenstand der Sie betreffenden Verarbeitung der personenbezogenen Daten, zu erhalten. Für darüberhinausgehende Kopien sind wir berechtigt ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten zu verlangen.

(6) Im Falle einer Nichterteilung der Auskunft ist der betroffenen Person unverzüglich schriftlich über die Verweigerung oder die Einschränkung der Auskunft und die Gründe hierfür zu unterrichten, z.B. ungeeigneter Identitätsnachweis, missbräuchliches Ausüben des Auskunftsrechts.

6.4 Berichtigung, Art 16 DSGVO

Der Betroffene hat das Recht unverzüglich (also ohne unnötige Verzögerung) die

- Berichtigung oder
- Vervollständigung

der ihn betreffenden unrichtigen oder unvollständigen personenbezogenen Daten zu verlangen. Die Norm regelt also nicht nur die Richtigstellung, sondern auch die Vervollständigung von unvollständigen Daten.

Die Datenberichtigung ist allerdings auch im Sinne des Grundsatzes der „Datenrichtigkeit“ nach Art 5 Abs 1 lit d DSGVO stets zu beachten - Daten sind seitens MIC demnach stets sachlich richtig und erforderlichenfalls auf dem neuesten Stand zu halten.

6.4.1 Berichtigungsprozess

Die Abwicklung des Berichtigungsbegehrens ist ohne unnötige Verzögerung vorzunehmen; es ist jeder der nachfolgenden Schritte hinsichtlich Zeitpunkt und Tätigkeit entsprechend dauerhaft zu protokollieren und dieses Protokoll drei Jahre lang aufzubewahren:

(1) Datum des Einlangens des Auskunftsbegehrens

(2) Prüfung der Identität des Antragstellers – einfordern einer Kopie eines amtlichen Lichtbildausweises, es sei denn der Anspruchsteller ist amtsbekannt

(3) Einfordern eines amtlichen Dokuments, aus dem sich die Unrichtigkeit des zu berichtigenden Datensatzes ergibt

(4) Einfordern einer elektronischen oder sonstigen Adresse an die die Information über die Durchführung/Ablehnung der Berichtigung gesendet wird

(5) Mitteilung über die durchgeführte Berichtigung oder nicht durchgeführte Berichtigung samt Ablehnungsbegründung

6.5 Löschung, Art 17 DSGVO

Der Betroffene hat das Recht, von MIC zu verlangen, dass die ihn betreffenden personenbezogenen Daten unverzüglich gelöscht werden, sofern keine Rechtsgrundlage mehr für die zulässige Verarbeitung vorliegt (insbesondere Vertrag, berechtigtes Interesse, rechtliche/gesetzliche Verpflichtung).

Im Falle der Veröffentlichung der Daten durch MIC hat diese unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art zu ergreifen, um andere Verarbeiter darüber zu informieren, dass der Betroffene die Löschung aller Links zu den personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Ausgenommen vom Löschungsrecht sind Verarbeitungen, die erforderlich sind um die Meinungsäußerung sicher zu stellen oder für die eine rechtliche Verpflichtung besteht oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Löschung heißt nicht zwingend nur physisch löschen, sondern kann auch eine logische Löschung umfassen. Nach der ständigen Rechtsprechung verlangt der OGH eine physische Löschung jedenfalls dann, wenn die Datenerhebung/-verarbeitung rechtswidrig war/ist.

In den meisten Fällen ist ein „Löschbegehren“ der betroffenen Person aber als Zweckänderung zu verstehen/interpretieren, weil bestimmte andere Rechtfertigungsgründe zur Datenverarbeitung (insbesondere öffentliches Interesse, berechtigte Interessen des Verantwortlichen/Dritten oder rechtliche Verpflichtungen) weiter bestehen bleiben. In diesen Fällen wird eine physische Löschung der Daten nicht möglich sein, vielmehr wird durch Änderung der Datenzugriffsberechtigung der Zweckänderung entsprochen („logisches Löschen“).

6.5.1 Löschungsprozess

Die Abwicklung des Löschungsbegehrens ist grundsätzlich ohne unnötige Verzögerung vorzunehmen, wobei jeder der nachfolgenden Schritte hinsichtlich Zeitpunkt und Tätigkeit entsprechend dauerhaft zu protokollieren und dieses Protokoll drei Jahre lang aufzubewahren ist:

(1) Datum des Einlangens des Löschungsbegehrens

(2) Prüfung der Identität des Antragstellers – einfordern einer Kopie eines amtlichen Lichtbildausweises, es sei denn der Anspruchsteller ist amtsbekannt

(3) Einfordern einer elektronischen oder sonstigen Adresse an die die Information über die Durchführung/Ablehnung der Löschung gesendet wird

(4) Prüfung des Löschungsbegehrens in der Sache:

a. **Rechtmäßig erhobene und verarbeitete Daten:**

   Es handelt sich hier de facto um Änderung des Verarbeitungszweckes:

   Beispiel: Kündigung eines Mitarbeiters => Beseitigung des aktiven Datenvorhalts, dh Daten sind technisch als „gelöscht" zu kennzeichnen, für andere Zwecke, die rechtliche vorgesehen sind, aber im notwendigen Umfang auch weiterhin zu speichern (zB Ausstellung eines Dienstzeugnisses, Gewährleistungs- und Garantiefristen); Änderung des Berechtigungskonzepts.

b. **Rechtswidrig erhobene und verarbeitete Daten**:

   i. Daten sind „physisch zu löschen".

   ii. Diese physische Löschung ist auch in den Sicherungskopien umzusetzen: Löschungsansprüche sind aber in den Sicherungskopien nicht unverzüglich umzusetzen, sondern nur zum, aus wirtschaftlicher und technischer Sicht, nächstmöglichen Zeitpunkt; bis zu diesem Zeitpunkt ist eine logische Löschung in den Sicherungskopien (Zugriffsbeschränkung) möglich (§ 4 Abs 2 DSG idF Nov. 2018). Es ist allerdings sicherzustellen, dass im Fall des Einspielens des Back-ups an sich physisch zu löschende Daten nicht wieder in das laufende System aufgenommen (aktiviert) werden.

(5) Dem **Löschungsanspruch ist daher insbesondere dann nicht nachzukommen**, wenn die Daten notwendig sind

a. zur Erfüllung einer rechtlichen Verpflichtung oder

b. zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder

c. um der Ausübung öffentlicher Gewalt nachzukommen oder

d. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

(6) Mitteilung an den Betroffenen, ob dem Löschungsbegehren nachgekommen wurde oder nicht; wird dem Begehren nicht nachgekommen, ist dies zu begründen.

6.6 Recht auf Einschränkung der Verarbeitung, Art 18 DSGVO

Die Einschränkung der Verarbeitung kann verlangt werden, wenn

a) die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird,

b) die Verarbeitung unrechtmäßig ist und der Betroffene die Einschränkung der Nutzung verlangt,

c) MIC die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

d) die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe seitens MIC gegenüber denen der betroffenen Person überwiegen.

Wenn die Verarbeitung eingeschränkt wird, so dürfen diese personenbezogenen Daten nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen verarbeitet werden; die bloße Speicherung bleibt aber zulässig. Wird die Einschränkung der Verarbeitung aufgehoben, wird die betroffene Person davon verständigt. Die Einschränkung der Verarbeitung wird anderen Empfängern der Daten mitgeteilt.

6.7 Recht auf Datenübertragbarkeit, Art 20 DSGVO

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie MIC bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder zu verlangen, dass diese Daten einem anderen Verantwortlichen zu übermitteln, sofern

a) die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht und

b) die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Das Recht auf Datenübertragbarkeit kann daher nicht gegen Verantwortliche ausgeübt werden, die personenbezogenen Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es gilt auch nicht, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der MIC unterliegt, oder für die Wahrnehmung einer ihr übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt, erforderlich ist.

6.8 Widerspruchsrecht / autom. Entscheidungsfindung im Einzelfall, Art 21f DSGVO

Der Betroffene hat das Recht, aus besonderen Gründen, jederzeit gegen die Verarbeitung der personenbezogenen Daten, die aufgrund eines berechtigten Interesses oder in Ausübung öffentlicher Gewalt verarbeitet werden, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.

Die Verarbeitung ist einzustellen, es sei denn, MIC kann zwingende Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen, insb zur Ausübung oder Verteidigung von Rechtsansprüchen.

Gegen Datenverarbeitungen, die der Direktwerbung dienen, kann jederzeit Widerspruch eingelegt werden. Dies gilt auch für das Profiling, soweit es mit Direktwerbung in Verbindung steht.

Über das Widerspruchsrecht muss der Betroffene spätestens zum Zeitpunkt der ersten Kommunikation hingewiesen werden. Dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen.

6.9 Mitteilungspflicht gegenüber Empfängern, Art 19 DSGVO

Es ist sicherzustellen, dass Einschränkungen oder Löschungen der Verarbeitung sowie Berichtigung der Daten auch an die Datenempfänger kommuniziert werden. Eine Ausnahme davon besteht nur bei Unmöglichkeit oder unverhältnismäßigem Aufwand. Es ist zu dokumentieren in welchem Umfang die Mitteilung erfolgt bzw. warum eine Mitteilung an Empfänger im Konkreten unmöglich oder unverhältnismäßig ist.

Sollte die betroffene Person die konkreten Datenempfänger verlangen, so ist dieser die Liste der Datenempfänger offenzulegen (siehe Verarbeitungsverzeichnis – Anhang), im Falle der Unmöglichkeit der Offenlegung ist dies entsprechend zu dokumentieren.

6.10 Meldung von Datenschutzverletzungen, Art 33f DSGVO

Der Datenschutzbehörde ist Meldung im Falle einer Datenschutzverletzung mit Risken für die Rechte und Freiheiten der davon betroffenen Personen zu machen („**Data Breach Notification**“). Für die Melde- bzw. Benachrichtigungsverpflichtung nach Art 33 und 34 DSGVO gilt grundsätzlich Folgendes (vgl. dazu auch WP250, 2016/679):

Nach Art 33 DSGVO ist eine Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzbehörde notwendig, und zwar unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Wenn einem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, hat er diese MIC unverzüglich mitzuteilen.

Folgende Infos sind im Falle der Meldung an die Datenschutzbehörde zu geben:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten der internen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von MIC ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Nach Art 34 DSGVO ist auch eine Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes personenbezogener Daten erforderlich, wenn diese voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten **natürlicher Personen** zur Folge hat. Die Benachrichtigung hat unverzüglich zu erfolgen und beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten.

Die **Benachrichtigung kann unterbleiben**, wenn

a) MIC geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch **Verschlüsselung**; oder

b) MIC durch geeignete Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Abs 1 aller Wahrscheinlichkeit nach nicht mehr besteht; oder

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Die Infos nach b, c und d sind dem Betroffenen im Falle der Benachrichtigungspflicht mitzuteilen.

6.10.1 Prozess zur data breach notification

Nach Art 33 bzw. 34 DSGVO ist im Falle einer Verletzung des Schutzes personenbezogener Daten unter bestimmten Voraussetzungen eine Meldung an die Datenschutzbehörde **bis längstens 72 Stunden ab Bekanntwerden bzw. unverzüglich** ab Bekanntwerden eine Benachrichtigung an die davon betroffenen Personen, vorzunehmen, und zwar nach folgenden Vorgaben:

1. Liegt eine Verletzung des Schutzes personenbezogener Daten vor (weil z.B. ein USB-Stick oder anderes Speichermedium verloren oder ein Laptop gestohlen wurde), führt dieses aber **nicht zu einem Risiko** für die Rechte/Freiheiten der Betroffenen, ist **keine Meldung erforderlich**, und zwar weder an die Behörde noch an die betroffene Person. Dies ist bspw. der Fall, wenn zwar Speichermedien mit personenbezogene Daten abhandenkommen, das Speichermedium aber vor unberechtigtem Zugriff angemessen geschützt ist (z.B. Datenverschlüsselung oder Zugriffsschutz durch ausreichendes Passwort).

2. Liegt eine Verletzung des Schutzes personenbezogener Daten vor (weil z.B. ein USB-Stick oder anderes Speichermedium verloren oder ein Laptop gestohlen wurde) und führt dies **zu einem Risiko** für die Rechte/Freiheiten der Betroffenen, ist **zwar diese Verletzung an die Datenschutzbehörde zu melden**, **nicht aber an die davon betroffenen Personen (Art 33 DSGVO)**. Dies ist bspw. der Fall, wenn kein angemessener Schutz vor unberechtigten Zugriff auf die personenbezogenen Daten gegeben ist, es sich aber nicht um besondere Kategorien von Daten (Art 9 DSGVO = Gesundheitsdaten odgl) handelt oder um Daten die über bloße Stammdaten hinausgehen oder durch Zusammenführung mit anderen zugänglichen Daten für eine betroffene Person besondere Bedeutung haben.

3. Liegt eine Verletzung des Schutzes personenbezogener Daten vor (weil z.B. ein USB-Stick oder anderes Speichermedium verloren oder ein Laptop gestohlen wurde) und führt dies **zu einem hohen Risiko** für die Rechte/Freiheiten der Betroffenen, ist **diese Verletzung sowohl an die Datenschutzbehörde (Art 33 DSGVO)**, **als auch unverzüglich an die davon betroffenen Personen zu melden (Art 34 DSGVO)**. Dies ist bspw. der Fall, wenn kein angemessener Schutz vor unberechtigten Zugriff auf besondere Kategorien von Daten gegeben ist (Art 9 DSGVO = Gesundheitsdaten odgl) oder auf Daten die über bloße Stammdaten hinausgehen oder auf Daten die durch Zusammenführung mit anderen zugänglichen Daten für eine betroffene Person besondere Bedeutung haben (weil bspw besondere Verhaltensweisen oder Profile des Betroffenen erstellt werden könnten).

Folgende Infos sind an die Datenschutzbehörde im Falle eines Risikos für die Betroffenen binnen längstens 72 Stunden ab Bekanntwerden der Verletzung zu melden:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten einer Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von MIC ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Folgende Infos sind dem Betroffenen im Falle eines hohen Risikos für die Betroffenen unverzüglich zu geben:

a) den Namen und die Kontaktdaten einer Anlaufstelle für weitere Informationen;

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

c) eine Beschreibung der von MIC ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die Überlegungen, die zu einer oder keiner Meldung an die Datenschutzbehörde und/oder die betroffenen Personen führen, sind entsprechend dauerhaft zu protokollieren und zumindest drei Jahre lang aufzubewahren.

7 Datenschutzfolgenabschätzung

Gemäß Art 35 DSGVO ist eine Datenschutzfolgenabschätzung durchzuführen, wenn eine Form der Verarbeitung

- insbesondere bei Verwendung neuer Technologien
- aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
- ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen hat

Innerhalb der MIC ist aktuell keine Datenschutzfolgenabschätzung notwendig, dies ist auch so im Datenverarbeitungsverzeichnis dokumentiert. Sollte es zu Datenverarbeitungen kommen, die eine Datenschutzfolgenabschätzung notwendig machen, so ist diese von der Datenschutzorganisation unter Einbeziehung unseres externen Spezialisten für Datenschutzfragen durchzuführen.