Raumrichtlinie

der Gebrüder Meiser GmbH,

Schmelz-Limbach

Int. Dok.-Name.: RAULI

Version: 1.4

Stand: 09.01.2020

Inhaltsverzeichnis

	<u>Seite</u>
I. Zweck der Richtlinie.....	1
II. Räumliche Grundschutzmaßnahmen.....	2
1. Zutrittskontrolle.....	2
2. Videoüberwachung	2
3. Einbruchmeldeanlage.....	6
4. Brandmeldeanlage.....	6
III. Allgemeine IT-Sicherungsmaßnahmen (Geräteschutz)	7
1. Computer sperren.....	7
2. Schutz vor Einsicht und Abhören (Spionage)	7
IV. Regelungen zu Innendiensttätigkeiten	8
1. Clean-Desk-Policy	8
2. Verschließen der Büroräume.....	8
3. Ausrichtung der Monitore und Bildschirme.....	8
4. Umgang mit zentralen Druck- sowie Multifunktionsgeräten und mobilen Druckern (Druckrichtlinie).....	9
5. Entsorgung von Papier-Fehlausdrucken und -kopien	9
V. Regelungen zu Außendiensttätigkeiten	10
1. Dokumente, Unterlagen und Akten	10
2. Mobile dienstliche Kommunikationsmittel und Speichermedien.....	10

Inhaltsverzeichnis

VI. Regelungen zu Telearbeitsplätzen (“Home-Office“)	12
1. Dokumente, Unterlagen und Akten	12
2. Mobile dienstliche Kommunikationsmittel und Speichermedien	12
VII. Umgang mit Besuchern	13
1. Anmeldung von Besuchern und Reservierung von Besprechungsräumen	14
2. Privatbesuch	14
3. Umgang mit Dienstleistern und externen Reinigungskräften	14

I. Zweck der Richtlinie

Im Geschäftsalltag ist es unumgänglich, unterschiedlichen Personen (Besuchern) Zugang zum Unternehmen zu gewähren. Zu Besuchern zählen neben Kunden und Geschäftspartnern auch Zulieferer, Praktikanten sowie Dienstleister und sonstige Fremdfirmen.

Die Raumrichtlinie dient der Umsetzung des Besuchermanagements und regelt u.a. den Empfang von Personen, die Zugangsberechtigungen, das Einhalten von diesbezüglichen Sicherheitsvorschriften, das Ein- und Ausbringen von Gegenständen und das Führen von Besucherlisten. Der Datenschutz im Rahmen der Tätigkeiten im Büro, im Außendienst (bei Mandanten) sowie im Home-Office ist dabei zwingend zu gewährleisten. Die Möglichkeiten im Umgang mit Besuchern und Dienstleistern innerhalb des Unternehmens sowie mit Kommunikationsmitteln, Dokumenten in Papierform innerhalb des Unternehmens und im Außendienst sind vielfältig und müssen überwiegend mit organisatorischen und IT-technischen Maßnahmen abgesichert werden. Hierbei sind besonders die Sensibilisierung und die permanente Schulung der Mitarbeiter von Bedeutung.

II. Räumliche Grundschutzmaßnahmen

1. Zutrittskontrolle

Der Zutritt zum und das Verlassen des Verwaltungsgebäudes hat für alle Personengruppen des Geschäftsbereiches Verwaltung (inkl. Mitarbeiter, Lieferanten, Dienstleister, etc.) ausschließlich über den Nebeneingang zu erfolgen. Aktive Mitarbeiter müssen den Eingang in Verbindung mit der zur Erfassung der Arbeitszeit installierten Bedieneinheit bei Beginn und Ende des Arbeitstages; sowie beim Verlassen des Firmengeländes in den Pausen oder während eines Dienstganges; nutzen.

Verwaltungsgebäude:

Der Zutritt im Verwaltungsgebäude ist ausschließlich Montags bis Freitags von 06.00 Uhr bis 19.30 Uhr möglich. Mitarbeitern ist es gestattet, mit der Erlaubnis des zugehörigen Abteilungsleiters, auch Samstags im Zeitraum von 06.00 Uhr bis 19.30 Uhr das Verwaltungsgebäude zu betreten.

Produktionshalle:

Während des 2-Schicht Betriebes ist die Produktionshalle für die Mitarbeiter von 4.30 Uhr bis 24.00 Uhr zugänglich, bei einem 3-Schicht Betrieb rund um die Uhr.

Für die Mitarbeiter des Produktionsbereiches ist ein Lesegerät für Schlüsselmarken in der Produktionshalle vorhanden.

Der Verlust von Schlüsselmarken ist unverzüglich, spätestens am nächsten Werktag, bei der IT-Abteilung zu melden. Beim Mitführen ist darauf zu achten, dass kein Rückschluss auf die Gebrüder Meiser GmbH möglich ist.

2. Videoüberwachung

Der Außenbereich des Firmengeländes wird rund um die Uhr durch ein Kamerasystem überwacht.

Weitere überwachte Bereiche sind-

Verwaltung Nebeneingang:

Außerhalb der geschäftlichen Kernarbeitszeiten (Montags bis Donnerstags von 08.00 Uhr – 17.00 Uhr und Freitags von 08.00 Uhr – 16.00 Uhr).

Verzinkerei, Haupteingang, Magazin:

Montags bis Donnerstag 00.00 Uhr - 06.00 Uhr, Freitags von 23.00 Uhr - 6.00 Uhr.

Bearbeitungshalle:

Montags bis Sonntags 22.30 Uhr – 06.00 Uhr

Zur Erfüllung der Transparenzanforderungen und Hinweispflichten sind an den Zugangs- und Zufahrtswegen datenschutzkonforme Hinweisschilder gem. Art. 13 der Datenschutz-Grundverordnung angebracht, auf denen nachfolgende Informationen ersichtlich sind:

- Umstand der Beobachtung (Kamerasymbol)
- Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters
- Kontaktdaten des betrieblichen Datenschutzbeauftragten
- Zwecke und Rechtsgrundlage der Datenverarbeitung
- Berechtigte Interessen, die verfolgt werden
- Speicherdauer oder Kriterien für die Festlegung der Dauer
- Hinweis auf Zugang zu weiteren Pflichtinformationen gem. Art. 13 Abs. 1 und 2 DSGVO

Datenschutzhinweise zur Videoüberwachung nach Art. 13 DSGVO

Hiermit informieren wir Sie über die Verarbeitung Ihrer personenbezogenen Daten durch uns bei der Videoüberwachung und die Ihnen nach den datenschutzrechtlichen Regelungen zustehenden Ansprüche und Rechte.

1. Verantwortlicher und Datenschutzbeauftragter:

Verantwortlich für die Videoüberwachung ist

Gebrüder MEISER GmbH

Edmund Meiser Straße 1

D-66839 Schmelz-Limbach

Tel: +49 (0) 6887 – 309 0

Fax: +49 (0) 6887 – 309 3000

Email: info@meiser.de

Webseite: www.meiser.de

Unseren Datenschutzbeauftragten erreichen Sie unter der E-Mail-Adresse datschutzbeauftragter@meiser.de

2. Zwecke und Rechtsgrundlage der Videoüberwachung:

Die Videoüberwachung erfolgt gemäß Art. 6 Abs. 1 f) Datenschutz-Grundverordnung (DSGVO) i.V.m. § 4 Bundesdatenschutzgesetz (BSDG) insbesondere zu folgenden Zwecken:

- zur Wahrnehmung unseres Hausrechts,
- zum Schutz unseres Eigentums,
- zur Aufklärung von Straftaten und sicherheitsrelevanten Vorfällen.

Eine allgemeine Überwachung des öffentlichen Raums sowie Profiling finden nicht statt.

An Orten, an denen wir Videoüberwachung einsetzen, werden durch ein besonderes Hinweisschild kenntlich gemacht (Muster s.o.).

3. Speicherdauer:

Die Videoaufzeichnungen werden grundsätzlich nach 10 Tagen gelöscht.

4. Empfänger der Videodaten, Weitergabe

Einer Weitergabe der Daten erfolgt an von uns beauftragte Dienstleister, die Überwachungsaufgaben für unser Unternehmen wahrnehmen.

Im Falle des Verdachts von strafbaren Handlungen geben wir die Daten zudem ggf. an Strafverfolgungsbehörden weiter.

Ansonsten werden die Daten nur weitergegeben, wenn es eine Rechtsgrundlage für die Weitergabe gibt. Dies kann insbesondere der Fall sein, wenn die Polizei oder sonstige Sicherheitsbehörden im Rahmen der sog. Gefahrenabwehr tätig werden und einen Zugriff auf die Daten der Videoüberwachung verlangen.

5. Datenverarbeitung außerhalb der Europäischen Union

Eine Verarbeitung von personenbezogenen Daten findet im Rahmen der Videoüberwachung nicht statt.

6. Rechte der Betroffenen:

Als Betroffener haben Sie das Recht, Auskunft, Berichtigung, Löschung und Sperrung Ihrer Daten zu verlangen. Sie haben darüber hinaus das Recht, der Videoüberwachung zu widersprechen, sofern Sie Gründe haben, die sich aus Ihrer besonderen Situation ergeben.

Ihre Rechte machen Sie bitte gegenüber dem unter Ziffer 1. Genannten Verantwortlichen oder direkt gegenüber dem dort benannten Datenschutzbeauftragten geltend.

7. Beschwerderecht:

Sie haben das Recht, sich bei einer Aufsichtsbehörde zu beschweren.

Beim Zweck der Rechtsgrundlage sollte stehen „Wahrnehmung berechtigter Interessen gemäß Art. 6 Abs. 1 f) Datenschutz-Grundverordnung (DSGVO) i.V.m. § 4 Bundesdaten-schutzgesetz (BSDG)“ und bei den berechtigten Interessen

- zur Wahrnehmung unseres Hausrechts,
- zum Schutz unseres Eigentums,
- zur Aufklärung von Straftaten und sicherheitsrelevanten Vorfällen.

3. Einbruchmeldeanlage

Von Montags bis Freitags ist die Alarmanlage des Verwaltungsgebäudes von 24.00 Uhr bis 05.00 Uhr scharf geschaltet, sowie von Samstags 16.00 Uhr bis Montags 05.00 Uhr. Die Einbruchmeldeanlage überwacht alle Ein- und Ausgangstüren.

4. Brandmeldeanlage

Im Verwaltungsgebäude herrscht ein generelles Rauchverbot. Über das gesamte Bürogebäude verteilt sind Rauchmelder installiert, die eine Rauchentwicklung registrieren und eine Alarmmeldung an die Brandmeldezentrale weiterleiten.

An den zentralen Punkten auf jeder Etage des Bürogebäudes hängen Flucht- und Rettungspläne, auf denen die Standorte der Feuerlöscher ersichtlich und die Sammelpunkte außerhalb des Gebäudes eingezeichnet sind.

III. Allgemeine IT-Sicherungsmaßnahmen (Geräteschutz)

1. Computer sperren

PCs (Desktop-PCs, Thin-Clients, Notebooks) werden bei längerer Abwesenheit automatisch gesperrt. Dabei können alle geöffneten Programme und Dokumente geöffnet bleiben. Nach dem Sperren des PCs zeigt Ihnen das Windows-Dialogfenster "Computer ist gesperrt" an. Ihr System ist jetzt gesperrt und nur Sie oder ein Systemadministrator können die Sperrung aufheben und geöffnete Dateien oder Programme einsehen. Die Aufhebung der Sperrung erfolgt durch die Eingabe Ihres hinterlegten Passworts. Sämtliche zuvor geöffneten Programme und Dokumente stehen Ihnen wieder zur Verfügung. Bei Problemen oder Fragen wenden Sie sich bitte an die Systemadministratoren. Diese finden Sie auf der Startseite des Intranets.

2. Schutz vor Einsicht und Abhören (Spionage)

Für dienstliche Kommunikationsmittel ist eine automatische Bildschirmsperre einzurichten. Dienstliche Kommunikationsmittel sind bereits bei Ausgabe durch die IT-Abteilung mit einer Bildschirmsperre versehen. Achten Sie bei Ihrer dienstlichen Tätigkeit außerhalb des Bürogebäudes auf Überwachungskameras und auf aktive Smart-Konnektivitäten (aktive Smart-TV-Kameras, Spielekonsolen etc.).

IV. Regelungen zu Innendiensttätigkeiten

1. Clean-Desk-Policy

Die einfachste und bewährteste Möglichkeit, Daten vor fremder Einsicht zu schützen, ist der aufgeräumte Arbeitsplatz ("Clean-Desk").

Dokumente und Akten (Unterlagen) sowie dienstliche Kommunikationsmittel (Firmennotebooks, -tablets und -handys) und externe Speichermedien (z.B. USB-Sticks und CD) sind beim Verlassen (längere Abwesenheit) des Arbeitsplatzes (z.B. zum Arbeitsende, im Urlaub oder bei der Außendiensttätigkeit) oder bei vorübergehender Abwesenheit (z.B. während der Mittagspause bzw. internen und externen Besprechungen und Schulungen) in den abschließbaren Schränken, Schubladen und Containern zu verstauen, welche beim Verlassen des Arbeitsplatzes zu verschließen sind.

2. Verschließen der Büroräume

Daneben sind die einzelnen Büros beim Verlassen grundsätzlich durch den jeweiligen Mitarbeiter abzusperren. Die Schlüssel zum Büro sowie zu Schränken, Schubladen und Containern dürfen nicht mit einer Aufschrift gekennzeichnet werden und sind vom absperrenden Mitarbeiter sicher zu verwahren, um einen Rückschluss auf die Büroräume und/oder eine räumliche Zuordnung zu vermeiden.

3. Ausrichtung der Monitore und Bildschirme

Bildschirme und Monitore sind vorbehaltlich anderer gesetzlicher Vorgaben so auszurichten, dass der direkte Einblick für Dritte beim Betreten eines Büros oder von außen (Fenster und Glastüren) nicht oder nur bedingt möglich ist.

4. Umgang mit zentralen Druck- sowie Multifunktionsgeräten und mobilen Druckern (Druckrichtlinie)

Bitte lassen Sie keine Ausdrücke und Kopien oder sonstige vertrauliche und datenschutzrelevante Unterlagen in den Bereichen außerhalb Ihres Arbeitsplatzes (z.B. Ablageflächen bei und von zentralen Druckgeräten, Empfangsbereich, Schreibbüro etc.) liegen. Sämtliche Dokumente und Unterlagen sind nach Be- oder Verarbeitung an Ihrem persönlichen Arbeitsplatz aufzubewahren (vgl. auch Ausführungen zu Kap. IV. "Regelungen zu Innendiensttätigkeit" zu Nr. 1 "Clean-Desk-Policy").

Eingescannte Dokumente und Unterlagen werden an die Firmen-Mail-Adresse @Meiser.de des jeweiligen Nutzers gesendet und können von dessen Arbeitsplatz aus weiterverarbeitet werden.

Ausdrücke für private Zwecke und der Ausdruck oder Scan von externen Speichermedien sowie die direkte Versendung per E-Mail an Adressen außerhalb der internen Benutzeradressen sind grundsätzlich untersagt.

5. Entsorgung von Papier-Fehlausdrucken und -kopien

Die Papierkörbe neben den Schreibtischen sind für die Entsorgung von Papieren mit unsensiblen Inhalt (ohne personenbezogene und vertrauliche Daten) gedacht.

Papier-Fehlausdrucke und -kopien mit personenbezogenem oder vertraulichem Inhalt (insbesondere Verträge und Firmeninterna), die nicht mehr benötigt werden, sind vom übrigen Papierabfall getrennt in Ihrem Büro zu sammeln und zeitnah (spätestens zu Feierabend) in den gesonderten Papiertonnen des Entsorgungsdienstleisters zu entsorgen oder über die datenschutzkonformen Aktenvernichter zu vernichten.

Ebenso werden Dokumente in den Körben neben den zentralen Druckgeräten täglich geleert. Es sollte generell vermieden werden, Papier-Fehlausdrucke und -kopien über die Papierkörbe an den Büroarbeitsplätzen und Küchen zu entsorgen.

V. Regelungen zu Außendiensttätigkeiten

1. Dokumente, Unterlagen und Akten

Lassen Sie an Ihrem Tätigkeitsort im Außendienst keine Dokumente, Unterlagen und Akten bei vorübergehender Abwesenheit (z.B. während der Mittagspause oder beim Besuch von Ansprechpartnern) sowie bei längerer Abwesenheit (z.B. während Besprechungen oder mehrtägiger Tätigkeit) offen bzw. geöffnet auf dem Tisch liegen, auch wenn die Räumlichkeiten bei Verlassen abgeschlossen werden. Dokumente, Unterlagen und Akten müssen bei längerer Abwesenheit (z.B. während Besprechungen oder mehrtägiger Tätigkeit) in verschließbaren Behältern (z.B. Schränken, Schubladen, Container etc.) aufbewahrt werden, um die Einsichtnahme, Diebstahl oder Beschädigung durch Unbefugte zu verhindern. Dies gilt auch generell für Dokumente, die Sie nicht permanent im Zugriff haben.

Sorgen Sie für einen sicheren Transport der Dokumente, Unterlagen und Akten zwischen Firmengebäude und Außendiensttätigkeit, d.h. schützen Sie diese vor der Einsicht und dem Zugang Unbefugter.

Dokumente und Unterlagen sollten unmittelbar nach Beendigung einer Außendiensttätigkeit oder eines Besprechungstermins im Firmengebäude unter Verschluss gehalten werden. Bitte lassen Sie generell keine Dokumente und Unterlagen oder Arbeitsmittel (Notebooks) längere Zeit unbeaufsichtigt in Fahrzeugen.

Entsorgen Sie keine Unterlagen mit personenbezogenen oder vertraulichen Daten, die nicht mehr benötigt werden, über die Entsorgungsmöglichkeiten (Mülleimer, Papierkörbe, Aktenvernichter, Mülltonnen, Container etc.) im Außendienst. Sammeln und verwahren Sie nicht mehr benötigte Unterlagen, wenn möglich an einem abschließbaren Platz oder Raum, und entsorgen Sie diesen bei Ihrem nächsten Büroaufenthalt.

2. Mobile dienstliche Kommunikationsmittel und Speichermedien

Mobile dienstliche Kommunikationsmittel und Speichermedien sind bei der Nutzung außerhalb der Büroräume und beim Transport gegen Diebstahl zu schützen und sollten generell niemals unbeaufsichtigt gelassen werden.

Bei längerer Außendiensttätigkeit sind mobile dienstliche Kommunikationsmittel und Speichermedien nicht über Nacht im Fahrzeug zu lassen und sollten immer im Kofferraum (nicht sichtbar im Innenraum) transportiert werden.

Die Reservierung eines notwendigen Präsentationsequipments (z.B. Beamer, Laptop etc.) für den Einsatz im Außendienst ist im Vorfeld frühzeitig bei der IT-Abteilung im Geltungsbereich dieser Richtlinie (vgl. Datenschutz-Grundlagen Kapitel II. "**Umsetzung / Review**", Nr. 4 "**Geltungsbereich der Richtlinie**") zu melden.

VI. Regelungen zu Telearbeitsplätzen ("Home-Office")

Beim Einsatz von sogenannten Telearbeitsplätzen sind neben den vorgenannten einige zusätzliche sicherheitstechnische Anforderungen zu beachten. Es ist sicherzustellen, dass am Arbeitsplatz des Telearbeiters und bei der Kommunikation zwischen Kanzlei und Telearbeitsplatz die Vertraulichkeit der Daten gewährleistet ist.

1. Dokumente, Unterlagen und Akten

Bewahren Sie die Dokumente, Unterlagen und Akten in verschließbaren Behältern (z.B. Schränken, Schubladen, Container etc.) auf, um die Einsichtnahme, Diebstahl oder Beschädigung durch Unbefugte zu verhindern.

Entsorgen Sie keine Unterlagen mit personenbezogenen oder vertraulichen Daten, die nicht mehr benötigt werden, über den Hausmüll.

2. Mobile dienstliche Kommunikationsmittel und Speichermedien

Schützen Sie mobile dienstliche Kommunikationsmittel vor Unbefugten (z.B. gegenüber Familienangehörigen, Freunden und Handwerkern), wenn möglich in einem abschließbaren Raum.

Nutzen Sie vorhandene Schutzmöglichkeiten und Sicherheitsmaßnahmen der mobilen dienstlichen Kommunikationsmittel (z.B. Sperrung des Laptops beim Verlassen).

VII. Umgang mit Besuchern

Der Empfang von Besuchern und die Reservierung eines entsprechenden Besprechungsraums, ein notwendiges Catering, der Bedarf von Präsentationsequipment (z.B. Beamer, Laptop etc.) ist im Vorfeld frühzeitig bei der Zentrale ("Empfang") zu melden. Besucher werden grundsätzlich durch den/die Mitarbeiter der Zentrale in Empfang genommen. Der Empfang ist bei offener Eingangstür niemals unbesetzt zu lassen. Zu kurzfristigen Vertretungen (z.B. i.R.d. Mittagspause) kann auf Auszubildende zugegriffen werden. Besucher sind grundsätzlich nicht unbeaufsichtigt zu lassen. Datenschutzrelevante Bereiche sind für Besucher gänzlich unzugänglich und durch Schloss gesichert.

Besuchern ist der Zutritt zum Gebäude nur über den Haupteingang und ausschließlich während der gewöhnlichen Geschäftszeiten Montags bis Donnerstags von 8.00 Uhr bis 17.00 Uhr und Freitags von 8.00 Uhr bis 16.00 Uhr möglich. Alle Besucher werden unmittelbar nach dem Eintreten in das Firmengebäude am Empfang unter folgenden Angaben in der Besucherdatenbank festgehalten:

- Datum
- Erfasser
- Vor- und Nachname
- Ggf. Firma
- Ggf. besuchte Person
- Grund des Besuchs
- Uhrzeit (von und bis)
- Einwilligung des Besuchers

Besuchereinträge dürfen nachträglich nicht gelöscht werden und sind zumindest für ein Jahr aufzubewahren.

Während der Meldung der Ankunft der/des Besucher/s an den Empfänger (per E-Mail oder Telefon) sind die Besucher angehalten, im Wartebereich (in Sichtweite des Empfangs) Platz zu nehmen oder werden durch einen Mitarbeiter der Zentrale in den vorgesehenen Besprechungsraum begleitet.

1. Anmeldung von Besuchern und Reservierung von Besprechungsräumen

Besprechungen mit Besuchern (mit Ausnahme von Dienstleitern bzw. Wartungsfirmen) sind ausschließlich in separaten Besprechungsräumen im Erdgeschoss abzuhalten und finden niemals in den Büroräumen statt.

2. Privatbesuch

Der Empfang von betriebsfremden Personen zu privaten Zwecken während oder außerhalb der Arbeitszeit ist nur in dringenden Fällen gestattet.

Ausnahmen bedürfen der vorherigen Genehmigung durch die Unternehmensleitung. Ein Besuch in den Büro- oder Arbeitsbereichen ist grundsätzlich nicht zulässig.

3. Umgang mit Dienstleistern und externen Reinigungskräften

Dienstleister und externe Reinigungskräfte sind während ihrer Einsatztätigkeit in datenschutzrelevanten Bereichen des Bürogebäudes nicht unbeaufsichtigt zu lassen. Mitarbeiter werden über den bevorstehenden Einsatz von Dienstleistern (z.B. Technikereinsätze) oder externen Reinigungskräften (z.B. Fensterputzer) informiert.

Außerhalb der gewöhnlichen Geschäftszeiten sind nur solche Räumlichkeiten zugänglich, in denen sich zumindest noch ein Mitarbeiter befindet oder sämtliche datenschutzrelevante Unterlagen in den Aktenschränken und Schubladen verschlossen wurden (vgl. auch Ausführungen in Kap. IV. "**Regelungen zu Innendiensttätigkeiten**" zu Nr. 1 "**Clean-Desk-Policy**").