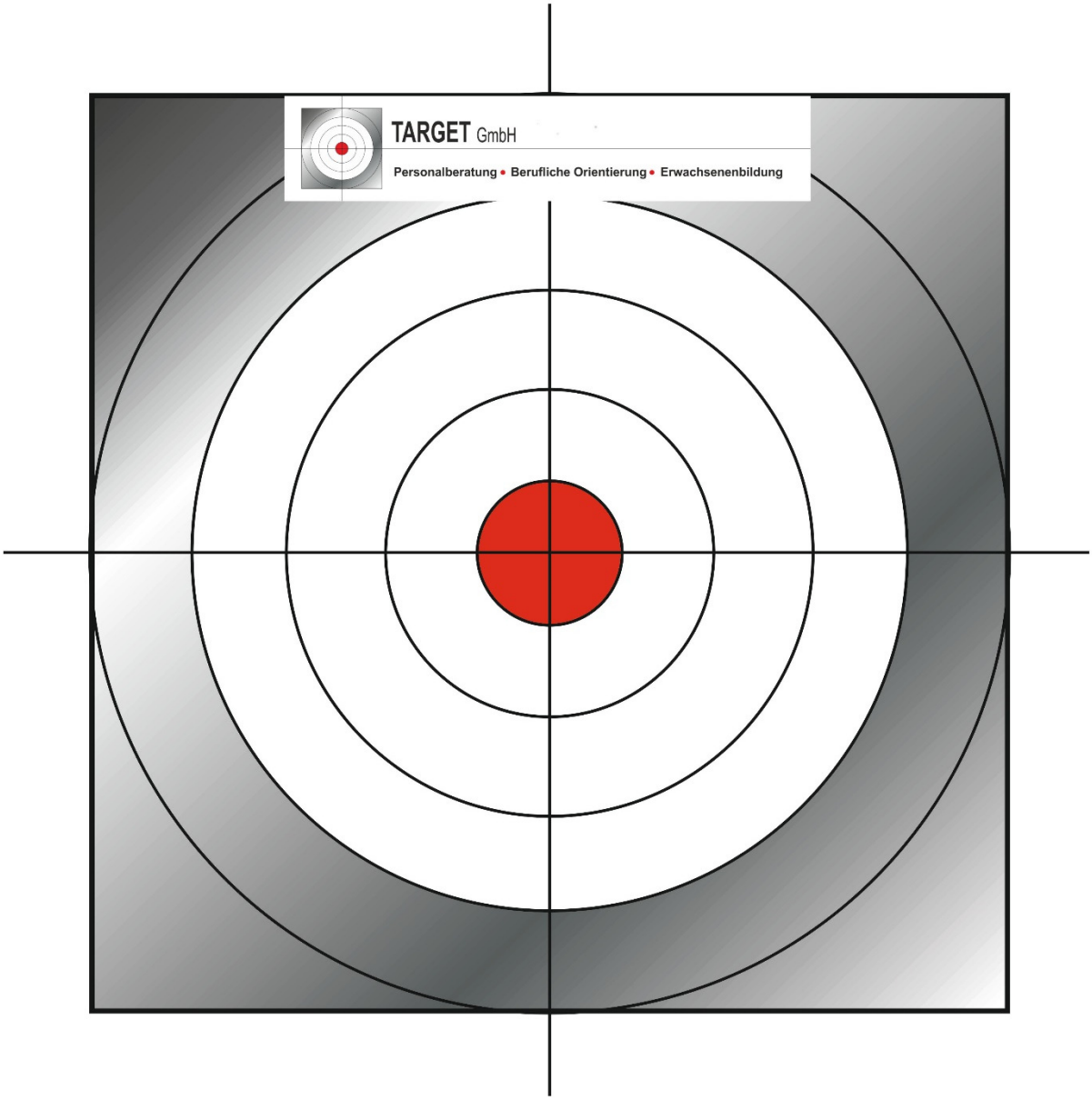

Datenschutzhandbuch der TARGET GmbH Stand 25.05.2018

Vorwort

Die TARGET GmbH setzt zur Durchführung ihrer Aufgaben im Bereich ihrer Projekte moderne IT-Infrastruktur ein und ist zu einem großen Teil davon abhängig. Der effiziente und sichere Betrieb, sowie die vertrauensvolle Verarbeitung der anfallenden Daten setzt voraus, dass alle Mitarbeiter der TARGET GmbH verantwortungsvoll mit den ihnen anvertrauten Daten und dem eingeräumten Handlungsspielraum umgehen.

Durch die Vernetzung von Arbeitsplätzen können absichtliche oder auch unabsichtliche Handlungen Einzelner sehr schnell zu großen Auswirkungen für andere im selben Netzwerk führen. Vor allem wenn dadurch Daten von natürlichen aber auch juristischen Personen berührt werden, kann sehr schnell das Vertrauen in die ganze TARGET GmbH in Mitleidenschaft gezogen werden.

Dieses Datenschutzhandbuch (DS-Handbuch) soll deshalb ein Leitfaden sein, wie die interne Kommunikation miteinander bei der Target GmbH gestaltet sein muss, damit dem einzelnen Mitarbeiter möglichst wenig technische Schranken auferlegt werden müssen.

Im DS-Handbuch finden sich bewusst keine technischen Spezifikationen von Hard- oder Software. Konkrete Umsetzungen, detaillierte Regelungen oder Anforderungen an Geräte oder Programme werden in aktuellen Beschreibungen vom IT Leiter entweder im Intranet oder per Mail veröffentlicht.

Die Grundsätze zur Gewährleistung des vertrauensvollen und verantwortungsbewussten Umgangs mit den der TARGET GmbH anvertrauten Daten finden sich in der Datenschutzerklärung der TARGET GmbH. Dieses Dokument beinhaltet weiter die Erklärung zur Erfüllung der Informationspflicht von Auftraggeberinnen und Auftraggebern von Datenanwendungen gemäß Art. 13 – 20 DSGVO und kann in seiner jeweils gültigen Fassung unter datenschutz@target-gmbh.de angefordert werden.

Das vorliegende Datenschutzhandbuch ist auch als Information und Belehrung zum Thema Datenschutz, die die Target GmbH ihren Mitarbeitern und Mitarbeiterinnen zur Verfügung stellt, zu verstehen. Die bzw. der Datenschutzbeauftragte (DSB, datenschutz@target-gmbh.de) steht darüber hinaus allen Mitarbeitern und Kursteilnehmern der TARGET GmbH gerne für Auskünfte und Erklärungen zum Thema Datenschutz oder dem vorliegenden DS-Handbuch zur Verfügung.

Inhaltsverzeichniss:

1. Allgemeines

In den verschiedenen Bereichen der TARGET GmbH werden große Mengen von Daten automatisiert verarbeitet und gespeichert. Diese Daten (unter anderem personenbezogene Daten und dem besonderen Schutz unterliegende personenbezogene Daten) müssen sorgfältig geschützt werden, um Datendiebstahl, Datenmissbrauch, Datenverlust und andere Gefährdungen abzuwenden. Die Einhaltung der Datenschutzbestimmungen werden bei der TARGET GmbH gewährleistet, indem die mit der Verarbeitung von Daten betrauten Personen entsprechend aufgeklärt bzw. geschult werden und die Einhaltung der Bestimmungen durch die bzw. den Datenschutzbeauftragten (DSB) kontrolliert wird.

Mit Hilfe dieses DS-Handbuches soll die große Bedeutung des Datenschutzes bei der TARGET GmbH betont werden. Gleichzeitig hat diese Richtlinie das Ziel, eine Überregulierung zu vermeiden und durch den Grundsatz der Verhältnismäßigkeit lebbar und kontrollierbar zu sein. Aus Gründen der einfacheren Lesbarkeit und der Textökonomie werden alle bei der TARGET GmbH mit der Verarbeitung von Daten betrauten Personen (Mitarbeiterinnen und Mitarbeiter, Administratorinnen und Administratoren, Honorarkräfte etc.) im Folgenden als ≫Datenverarbeitende≪ bezeichnet.

2. Verantwortlichkeiten

Alle Datenverarbeitenden bei der TARGET GmbH sind verpflichtet, die im vorliegenden DSHandbuch sowie die in der DSGVO und dem BDSG definierten Bestimmungen in ihrer jeweils gültigen Fassung einzuhalten und die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten der TARGET GmbH bei jedem Vorfall durch den die Sicherheit der verarbeiteten Daten gefährdet ist (auch bei Verdacht), unverzüglich zu kontaktieren. Dies ist insofern wichtig, als dass der Mißbrauch, aber auch der Verlust von Daten für die TARGET GmbH nach geltendem Recht teilweise schwerwiegende Konsequenzen nach sich ziehen kann.

Vorfälle, durch die die Sicherheit verarbeiteter Daten gefährdet werden kann, sind (demonstrativ):

• Virenbefall von Geräten, die im EDV-Netzwerk der TARGET GmbH zur Datenverarbeitung verwendet werden (PCs, mobile Endgeräte und ähnliches, auch im privaten Eigentum).

• Verlust oder Diebstahl von Rechnern, Datenträgern, Passwörtern oder Schlüsseln (insbesondere auch Zugangscodes etc.).

• Sonstige Sicherheitsvorfälle (z.B. Einbruch in Räumlichkeiten der TARGET GmbH).

Alle Datenverarbeitenden der TARGET GmbH haben Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer Tätigkeit bei der TARGET GmbH anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis). Diese Verpflichtung behält auch nach Beendigung des Dienstverhältnisses ihre Gültigkeit.

2.1 Leiterinnen und Leiter von Organisationseinheiten

Als Leiterinnen und Leiter im Sinne dieses DS-Handbuches gelten alle Personen, die eine Organisationseinheit der TARGET GmbH mit Verantwortung für andere Personen (Teilnehmerinnen und Teilnehmer, Mitarbeiterinnen und Mitarbeiter) leiten. Alle Leiter und Leiterinnen tragen die Verantwortung für den Datenschutz in ihrem Zuständigkeitsbereich. Dies umfasst die Verantwortung für die in ihrem Verantwortungsbereich tätigen Personen aber auch für sämtliche zur Verarbeitung von Daten eingesetzte Anwendungen, Dateien und Systeme.
Jede Leiterin und jeder Leiter muss die bzw. den DSB der TARGET GmbH über die Vorgänge in ihrem bzw. seinem Bereich informieren, in denen personenbezogene Daten ermittelt,
verarbeitet oder gespeichert werden, damit der oder die DSB die rechtmäßige Verwendung überprüfen kann.
Informationen zu den Informationspflichten der Leiter und Leiterinnen finden sich in diesem Dokument. Außerdem werden in unregelmäßigen Abständen Informationsveranstaltungen (Mitarbeiter Meetings) abgehalten. Des Weiteren kann bei Unklarheiten bezüglich des Datenschutzes jederzeit der oder die Datenschutzbeauftragte bzw. die Personalabteilung kontaktiert werden.

2.2 Administratorinnen und Administratoren

Administratorinnen und Administratoren bei der TARGET GmbH sind verpflichtet, dafür Sorge zu tragen, dass der Zugriff auf Systeme in ihrem Verantwortungsbereich mit denen personenbezogene Daten verarbeitet oder gespeichert werden, nur dazu berechtigten Datenverarbeitenden und nur im Umfang der persönlichen Rechte dieser Datenverarbeitenden möglich ist. Diese Systeme (Software, Hardware, Räume etc.) sind in jedem Fall mit technisch aktuellen Mitteln gegen Angriffe zu schützen (z.B. durch die Installation von Virenschutzprogrammen und Firewalls).
Änderungen an den zentralen, datenverarbeitenden Systemen müssen der jeweiligen Systemversion zuordenbar dokumentiert werden. Vor dem produktiven Einsatz neuer Komponenten an bei der TARGET GmbH, ist auf deren Tauglichkeit in Bezug auf den Schutz personenbezogener Daten zu achten. Dabei ist auch darauf zu achten, ob eine aktuelle, vollständige und auch für fachkundiges Vertretungspersonal verständliche Dokumentation der Komponente verfügbar ist und die Komponente die erforderlichen Protokollierungsmechanismen zur Verfügung stellt.
Es liegt im Verantwortungsbereich der Administratorinnen und Administratoren für sämtliche in ihrem Verantwortungsbereich eingesetzten Komponenten regelmäßig zu überprüfen, ob neue Sicherheitsupdates verfügbar sind, und deren Beschaffung und Installation zu veranlassen.
Die Administratorinnen und Administratoren der TARGET GmbH sind aufgrund ihrer Tätigkeit notwendigerweise mit großzügigen Rechten ausgestattet. Sie sind deshalb verpflichtet, mit den ihnen zur Verfügung stehenden Administratorrechten besonders sorgfältig umzugehen und für Systeme gezielt, d.h. nur in Fällen, die dies auch erfordern, zu verwenden.
Generell gilt der Grundsatz, dass mit der geringsten benötigten Berechtigungsstufe gearbeitet werden soll.
Vor dem Zugriff auf Sitzungen von angemeldeten Benutzern auf Systemen im Netzwerk der TARGET GmbH (z.B. mittels TeamViewer QS, KVM-Switches oder Konsolen von Virtualisierungssoftware) bzw. auf Geräte die nicht im Eigentum der Target GmbH stehen, muss die Zustimmung der respektive des Datenverarbeitenden bzw. der Eigentümerin respektive des Eigentümers eingeholt werden.

2.3 Datenschutzbeauftragte

MitarbeiterInnen und Teilnehmer können sich mit allen Fragen und Angelegenheiten des Datenschutzes jederzeit an den/die DSB wenden. Er/Sie ist nicht berechtigt, verbindliche rechtliche Auskünfte zu geben, wird aber Anfragen dementsprechend weiterleiten und sich dafür einsetzen, anstehende Fragen – in Zusammenarbeit mit z.B. der Geschäftsführung, der Personalabteilung oder Dritten – zu klären. Die bzw. der Datenschutzbeauftragte berät die Geschäftsführung der TARGET GmbH bei Entscheidungen im Bereich des Datenschutzes.
Die bzw. der DSB wird bei ihrer bzw. seiner Tätigkeit vom IT Leiter und der Geschäftsführung der TARGET GmbH unterstützt und arbeitet zur Informationsbeschaffung intensiv mit den zuständigen IT-LeiterInnen, wie z.B. bei Fragen zur Umsetzung von Projekten die die IT-Infrastruktur an der TARGET GmbH betreffen oder der Abteilung für Personal bei rechtlichen Fragen zum Thema Datenschutz zusammen und publiziert die geltenden Grundsätze des Datenschutzes der TARGET GmbH im Datenschutzhandbuch sowie der Datenschutzerklärung.

Die Mitwirkungsbereiche der bzw. des Datenschutzbeauftragten umfassen im Wesentlichen:
- Erstellung, Wartung und Publikation der Datenschutzerklärung und des Datenschutzhandbuches
- Schulung und Kontrolle von Datenverarbeitenden
- Beratung in Datenschutzangelegenheiten
- Bearbeitung von Auskunftsanfragen
- Prüfung von datenschutzrelevanten Vorgängen bei der Target GmbH
- Prüfung und Genehmigung von Ausnahmeregelungen
- Mitgestaltung datenschutzrelevanter Prozesse
- Einhaltung gesetzlicher Pflichten (Meldungen/Genehmigungen).

Der bzw. die Datenschutzbeauftragte hat in seiner bzw. ihrer Funktion keine anderen Zugriffsrechte auf Daten als andere MitarbeiterInnen er/sie kann und darf weder Personalakten, Dateien oder andere personenbezogene Informationen anderer einsehen.
Die meisten Verstöße gegen den Datenschutz werden aus Unwissenheit und fehlenden oder falschen Informationen begangen. Es geht daher darum, durch präventive Maßnahmen, wie Regelungen und die Zurverfügungstellung von Informationen, den Datenschutz und die Datensicherheit zu gewährleisten. Der bzw. die Datenschutzbeauftragte arbeitet daher gemeinsam mit allen am Datenschutz Interessierten miteinander daran, innerhalb der TARGET GmbH einen gesetzeskonformen Umgang mit personenbezogenen Daten zu bewahren und soll als Unterstützung in Hinblick auf Datenschutzrelevanz gesehen werden.

3. Umgang mit personenbezogenen Daten

Zur Wahrung des Grundrechtes auf Geheimhaltung von personenbezogenen Daten (Art. 5 und 6 DSGVO) wurden bei der TARGET GmbH Grundsätze für die Ermittlung, Verarbeitung und Nutzung dieser Daten definiert. Das wichtigste Prinzip dabei ist, dass personenbezogene Daten – sofern sie nicht aus anderen öffentlichen Datenquellen stammen – nur aus gesetzlichen Bestimmungen heraus, oder mit Zustimmung der Betroffenen für einen bestimmten Zweck verwendet werden dürfen und danach den gesetzlichen Bestimmungen folgend schnellst möglich wieder gelöscht werden müssen.

3.1 Verwendung von Daten

Art. 4 DSGVO definiert Daten bzw. personenbezogene Daten als ≫alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen oder zu einem oder mehreren besonderen Merkmalen, die Auskunft der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann.≪. Voraussetzung für die Zulässigkeit der Verwendung von Daten ist gemäß Art. 6 DSGVO, dass Zweck und Inhalt der Datenanwendung von den rechtlichen Befugnissen der TARGET GmbH gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der bzw. des Betroffenen nicht verletzt werden.

Als Kontaktperson für Fragen in Bezug auf die Rechtmäßigkeit der Verwendung von Daten steht Ihnen die bzw. der DSB der TARGET GmbH (datenschutz@target-gmbh.de) gerne zur Verfügung.

3.1.1 Sensible Daten

Sensible Daten, also Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben dürfen bei der TARGET GmbH nur dann verwendet werden, wenn zumindest eines der in Art.9 DSGVO aufgezählten Tatbestandsmerkmale erfüllt ist.

Die Verwendung von Daten bei der TARGET GmbH ist unter folgenden Voraussetzungen zulässig:

- Die bzw. der Betroffene hat die Daten offenkundig selbst öffentlich gemacht.
- Die Daten werden in nur indirekt personenbezogener Form verwendet.
- Die bzw. der Betroffene hat seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt.
- Die Verwendung ist erforderlich, um Rechten und Pflichten auf dem Gebiet des Arbeitsrechts Rechnung zu tragen.

3.1.2 Nicht-sensible Daten

Nicht-sensible Daten dürfen gemäß Art. 6 DSGVO bei der TARGET GmbH unter anderem dann verwendet werden, wenn eine der folgenden Bedingungen erfüllt ist:

- Es wurde eine Zustimmung der bzw. des Betroffenen in Kenntnis der Sachlage für den konkreten Fall erteilt und nicht widerrufen.

- Es handelt sich um zulässigerweise veröffentlichte Daten oder um nur indirekt personenbezogene Daten, bei denen die Identität der bzw. des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmt werden kann.

- Die Verwendung der Daten ist zur Erfüllung einer vertraglichen Verpflichtung zwischen der TARGET GmbH und der Betroffenen bzw. dem Betroffenen erforderlich.

3.1.3 Andere kritische Daten

Bei der TARGET GmbH werden darüber hinaus noch weitere wichtige Daten verarbeitet, die für den Betrieb der TARGET GmbH von großer Bedeutung sind. Dies sind insbesondere nicht personenbezogene vertrauliche Daten (wie z.B. Finanz- oder Strategiedaten), sowie Daten die der TARGET GmbH von Dritten zur Verarbeitung anvertraut wurden. Trotzdem sind die in den nachfolgenden Kapiteln beschriebenen Verhaltensweisen auch auf diese Art von Daten – egal ob personenbezogen oder nicht – anzuwenden.

3.2 Überwiegend berechtigte Interessen

Der Art.1 der DSGVO regelt das Grundrecht auf Geheimnisschutz für alle personenbezogenen Daten. In dieses Grundrecht darf nur aus drei Gründen eingegriffen werden: lebenswichtige Interessen des bzw. der Betroffenen (was in unserem Fall i.d.R. nicht zutrifft), Zustimmung der bzw. des Betroffenen und überwiegend berechtigte Interessen eines bzw. einer Anderen.
Die Zustimmung der Betroffenen wird für die meisten personenbezogenen Daten im Rahmen von Interessenserklärung, Bewerbung und Aufnahme einer Arbeit eingeholt bzw. ergibt sich durch rechtliche Pflichten der TARGET GmbH.
Weiter ist es möglich personenbezogene Daten auch mit dem Argument des ≫überwiegend berechtigten Interesses≪ zu verarbeiten. Hierzu gibt der Gesetzgeber allerdings keine klaren Regelungen, daher ist die Verarbeitung unter dieser Begründung mit Vorsicht und nur nach Rückfrage bei der Personalabteilung oder dem DSB anzuwenden.

3.3 Gewährleistung der Datensicherheit

Die in Art. 32 DSGVO geforderte Gewährleistung der Datensicherheit wird bei der TARGET GmbH durch die in den technisch organisatorischen Maßnahmen (TOM) beschriebenen Maßnahmen sichergestellt. Die Maßnahmen sind unter dem Aspekt der wirtschaftlichen Vertretbarkeit und der Bedingung, dass damit dem Stand der technischen Möglichkeiten Rechnung getragen wird, gewählt und werden laufend dahingehend überprüft.

3.4 Aufbewahrung personenbezogener Daten

Daten werden bei der TARGET GmbH in personenbezogener Form nur solange aufbewahrt, als dies für den Zweck, für den die Daten erhoben wurden, oder aufgrund von gesetzlichen Verpflichtungen (Archivierung), erforderlich ist.

3.5 Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerruf

Jede bzw. jeder hat das Recht auf Auskunft darüber, welche Daten bei der TARGET GmbH über sie bzw. ihn verarbeitet werden, woher diese Daten stammen, wozu sie verwendet werden und an wen sie gegebenenfalls übermittelt werden. Ebenso hat jede bzw. jeder das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässiger Weise verarbeiteter Daten (Art 16-20 DSGVO). Ebenso besteht das Recht, eine bereits erteilte Zustimmung zur Verarbeitung von Daten zu widerrufen (Art. 21 DSGVO).

3.6 Schutz der Daten von MitarbeiterInnen und BewerberInnen

Bewerbungsunterlagen und Daten von potentiellen MitarbeiterInnen, die nicht im Unternehmen tätig werden, sind nach Ablauf von 4 Monaten und wenn kein Einverständnis über das längere Aufbewahren vorliegt zu löschen.

Persönliche Daten werden auch nach einer Tätigkeit nur solange aufbewahrt, wie es für den Verwendungszweck erforderlich ist. Ausgenommen davon sind lediglich diejenigen Daten, die aufgrund einer gesetzlichen Vorschrift aufzubewahren sind. Diese Ausnahme gilt jedoch nur für den jeweils gesetzlich vorgeschriebenen Zeitraum.
MitarbeiterInnen haben Einsichtsrecht über die zur Person gespeicherten Daten und das Recht auf Richtigstellung nicht korrekt erfasster Daten. Die Daten von MitarbeiterInnen sind nur in der Zentrale der TARGET GmbH gespeichert bzw. gesichert aufbewahrt. Außerdem ist sichergestellt, dass nur berechtigte Personen für einen bestimmten und notwendigen Zweck darauf Zugriff haben.

3.6.1 Ausscheiden einer Mitarbeiterin bzw. eines Mitarbeiters

Von der ausscheidenden Mitarbeiterin bzw. dem ausscheidenden Mitarbeiter sind sämtliche Unterlagen, ausgehändigte Schlüssel und zur Verfügung gestellte IT-Geräte (Speichermedien, Laptops Smart-Phones etc.) zurückzugeben.
Es ist sicherzustellen, dass auf den von der TARGET GmbH zur Arbeit zur Verfügung gestellten Geräten zur Datenverarbeitung, unternehmenswichtige Informationen nicht mehr lokal gespeichert sind. Alle notwendigen Daten für die Weiterführung der Arbeit durch eine andere Person müssen dem/der Vorgesetzten bzw. NachfolgerIn übergeben werden, bzw. sich geordnet auf einem zentralen Netzlaufwerk befinden, zu dem diese Personen Zugang haben. Die Daten auf dem bzw. den persönlichen Arbeitsgerät(en) können danach jederzeit gelöscht bzw. zur Sicherung und Durchsicht anderen Mitarbeitern und Mitarbeiterinnen der TARGET GmbH zur Verfügung gestellt werden.
Außerdem sind alle eingerichteten Zugriffsberechtigungen zu entziehen bzw. zu löschen. Auch entsprechende Gruppenmitgliedschaften und damit verbundene Gemeinschaftsrechte sind zu entziehen.
Die ausscheidende Mitarbeiterin bzw. der ausscheidende Mitarbeiter ist nochmals darauf hinzuweisen, dass die eventuell zu Dienstbeginn oder im Laufe von Projekten unterschriebenen Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine im Rahmen der Tätigkeiten erhaltenen geheimen Informationen weitergegeben werden dürfen.
Im Falle einer Änderung des Beschäftigungsverhältnisses (z.B. andere Abteilung, andere Funktion, etc.) sind sofort mit dem Übertritts Datum die Berechtigungen entsprechend zu ändern.

3.7 Schutz der Daten der TARGET GmbH

Bei der TARGET GmbH werden vielfach Anfragen um Überlassung von Daten (statistischeDaten, Finanzen etc.) gerichtet. Beispielhaft können sich solche Anfragen beziehen auf

• Unternehmenskennzahlen (Umsatz, Betriebsaufwand, Anzahl der MitarbeiterInnen, Investitionen etc.)

• Statistische Daten zur Projektumsetzung bei der Target GmbH oder an einzelnen Maßnahmen (Quantitative und qualitative Angaben über Dozenten, Lehrveranstaltungen, Teilnehmer, Drop-Out-Zahlen, Entwicklungsprojekte für Lehrangebote etc.)

• Statistische Daten zur Entwicklung bei der TARGET GmbH (Auftragslage, Auftragseingang, Projektdaten, Informationen über FördergeberInnen und Fördervolumina u.ä.).

Manche der angefragten Daten sind öffentlich einsehbar, andere Daten sind Gegenstand von Veröffentlichungen der TARGET GmbH. Bestimmte Daten sind nur zur Kenntnisnahme für einen bestimmten, eingeschränkten Personenkreis (z.B. Gesellschafter) bestimmt, viele Daten sind gar nicht zur Veröffentlichung bestimmt und daher geheim zu halten.
Um sicherzustellen, dass keine geheimhaltungsbedürftigen Daten an Externe weitergegeben werden, muss die Beantwortung derartiger Anfragen von der Geschäftsführung autorisiert werden. Die Entscheidung, welche Daten an den jeweiligen Anfragesteller weitergegeben werden können, fällt in die ausschließliche Zuständigkeit der Geschäftsführung der TARGET GmbH und daher sind Anfragen an die GF weiter zu leiten.
Die Anfrage sowie ein Vorschlag zur Beantwortung ist daher möglichst rasch an die Geschäftsführung —via eMail oder als Hardcopy — weiter zu leiten. Die Geschäftsführung entscheidet darüber ob die Anfragebeantwortung direkt frei gegeben wird. Die Freigabe eines Antwortvorschlages erfolgt formlos durch die Geschäftsführung.

4. IT Sicherheit

Die aktuellen Regeln und Richtlinien zur Nutzung der IT-Infrastruktur der TARGET GmbH können im Intranet über die Seiten der IT & Logistik, insbesondere in der Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz, in ihrer jeweils gültigen Version abgerufen werden und sind zu befolgen. Im Folgenden werden daher nur die wichtigsten Grundsätze hinsichtlich der Gewährleistung einer sicheren Nutzung der IT-Infrastruktur in Bezug auf die Sicherheit von personenbezogenen Daten beschrieben.
Die nachfolgenden Abschnitte beziehen sich auf alle datenverarbeitenden Geräte, die im Netzwerk der TARGET GmbH betrieben werden. Geräte im Bereich der IT Administration stehen unter deren Verantwortung. Mitarbeiter und Mitarbeiterinnen die Geräte mit eigenen lokalen Administrationsrechten verwalten, sind für die entsprechende IT-Sicherheit wie sie in den nachfolgenden Abschnitten beschrieben wird selbst verantwortlich und haben für eine äquivalente Sicherheit wie die IT Leitung zu sorgen.

4.1 Arbeitsplatz- und Datensicherung

4.1.1 Ablage von Daten

Wichtige Dokumente und Dateien insbesondere alle Daten die Personen bezogen sind oder laufende Maßnahmen betreffen dürfen nicht auf lokalen Laufwerken (z.B. C: oder D:) der Rechner der TARGET GmbH gespeichert werden, da diese nicht gesichert werden und außerdem für sämtliche Benutzerinnen und Benutzer ohne großen technischen Aufwand einsehbar sind.
Solche Daten sind ausschließlich in StepNova (TOM) zu speichern!!
Bei Betriebssystemen, bei denen die Dateinamenserweiterung eine wichtige Rolle spielt, ist die Anzeige so einzustellen, dass der Typ einer Datei (ausführbares Programm, Textdatei, etc.) sofort anhand der Namenserweiterung erkannt werden kann. Damit kann ein versehentliches Ausführen von z.B. als Textdatei getarnten, bösartigen Programmen leichter vermieden werden.

• Nutzen Sie Ihr persönliches Laufwerk SPS (Z:) (gesicherter USB Stick) zur Ablage Ihrer persönlichen Dokumente und Dateien.

4.1.2 Benutzerinnen- bzw. Benutzerkennung und Passwort

Die von der IT Leitung der TARGET GmbH vergebene Benutzerinnen- bzw. Benutzerkennung sowie das von der jeweiligen Benutzerin bzw. dem jeweiligen Benutzer selbst gewählte Passwort für StepNova (TOM) und Intranet sind geheim zu halten und dürfen keinesfalls weitergegeben werden. Ebenso darf die Funktion ≫Kennwort speichern≪ für Kennwörter auf Rechnern der TARGET GmbH sowie in installierten Programmen nicht verwendet werden, wenn dies vermeidbar ist. Das ist erforderlich, um zu verhindern, dass unbefugte Personen auf personenbezogene Daten oder andere vertrauliche Daten zugreifen können, da in vielen Fällen damit das Passwort im Klartext auf dem lokalen Rechner gespeichert werden würde.
Das Passwort ist entsprechend der in der von der IT Leitung veröffentlichten Passwortrichtlinie definierten Passwort-Konventionen zu wählen (mindestens 12 Zeichen, Groß- und Kleinschreibung, Sonderzeichen, Zahlen müssen enthalten sein) und in den dort vorgeschriebenen Abständen (mindestens einmal im Quartal) zu erneuern. Das bei der TARGET GmbH verwendete Passwort und auch die Benutzerkennung dürfen – soweit auswählbar – auf Systemen außerhalb der TARGET GmbH nicht verwendet werden (z.B. für Dienste im WWW, private Computer, Webplattformen, etc.), um auch Angriffe von außen zu erschweren.
Auch die eMail-Adressen von Benutzerinnen und Benutzern der TARGET GmbH dürfen nur für Diensttätigkeiten verwendet werden, da ansonsten auch damit das Spam- und Angriffsaufkommen erhöht wird.

Verwenden Sie nach Möglichkeit auch bei externen Webanwendungen überall verschiedene und komplexe Passwörter. Es ist besser, schwierige Passwörter zu notieren oder zu speichern, als überall einfach das gleiche zu verwenden.
Stellen Sie sicher, dass diese Passwörter – aber auch Inhalte anderer Möglichkeiten der BenutzerInnen Authentifizierung wie bei Public-Key-Verfahren o.ä. – gesichert (versperrt) und für andere unzugänglich verwahrt werden.
Bei der Verwendung eines Passwort- oder Key-Managers muss das Master-Passworts mindestens den Passwort-Konventionen der TARGET GmbH genügen.
Für Fragen und Anliegen zu diesem Thema steht der IT Leiter der TARGET GmbH jederzeit gerne zur Verfügung.

4.1.3 Arbeitsplatzsicherung

Alle Benutzerinnen und Benutzer haben sich auf Systemen der TARGET GmbH mit ihrer persönlichen Kombination aus Benutzerinnen- bzw. Benutzerkennung und Passwort anzumelden. Beim Verlassen des Arbeitsplatzes ist dieser zu sperren, beim Verlassen der TARGET GmbH oder des Arbeitsplatzes insbesondere wenn noch Teilnehmer im Raum sind, sollte sich die jeweilige Benutzerin bzw. der jeweilige Benutzer auch abmelden (bzw. aus ökologischen und ökonomischen Gründen auch den Rechner herunterfahren). In Bereichen mit Publikumsverkehr sind Monitore, Drucker, Faxgeräte, aber auch Dokumentenablagen so aufzustellen, dass das Risiko der Einsichtnahme Unbefugter möglichst ausgeschlossen ist.

• Mit Hilfe von Tastenkombinationen (Windows: ≫Windowstaste+L≪, Linux: z.B. ≫STRG+ALT+L≪) können Rechner schnell und einfach gesperrt werden.
• Wenn nicht bereits von der IT Leitung installiert, verwenden Sie zusätzlich Bildschirmschoner, die nach einer fix definierten Wartezeit automatisch aktiviert werden und die nur mittels Passworteingabe wieder deaktiviert werden können.

4.1.4 Versehentliche Dateneinsicht

Benutzerinnen oder Benutzer, die aufgrund einer Störung oder Fehlbedienung Zugang zu Daten oder Mitteilungen erhalten, die nicht für sie bestimmt sind, dürfen diese nicht einsehen, kopieren, manipulieren oder weiterleiten.
Sollten Sie versehentlich Einsicht in nicht für Sie bestimmte Daten erlangen, informieren Sie bitte umgehend die IT Leitung der TARGET GmbH sowie ggf. die Absenderin bzw. den Absender der Daten über das Versehen.

4.2 Internet und eMail

Die Benutzerinnen und Benutzer sind berechtigt, das eMail System sowie den Internet-Zugang der TARGET GmbH zu verwenden, solange dabei nicht gegen geltendes ¨Deutsches Recht verstoßen und zusätzlich die Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz der TARGET GmbH eingehalten wird.
Die Arbeitsplätze, über die auf das Internet zugegriffen wird, müssen mit einem aktuellen, aktiven Virenscanner ausgestattet sein. Der verwendete Browser muss so konfiguriert sein, dass ein möglichst hohes Maß an Sicherheit gewährleistet ist. Dies gilt insbesonders für Viren- und Malware-gefährdete Systeme wie Windows.

Bei der Übermittlung von personenbezogenen oder vertraulichen Daten per eMail oder über das Internet müssen entsprechende Sicherheitsvorkehrungen getroffen werden (z.B. sichere, Verschlüsselte Datenübertragung).
Auch ist dabei zu beachten, dass eine automatisierte Weiterleitung von eMails an externe Anbieter dazu führen kann, dass die DSGVO verletzt wird, indem z.B. personenbezogene Daten, die unverschlüsselt und vermeintlich intern versendet werden, dadurch an einen Anbieter in Übersee weitergeleitet und dort gespeichert werden.
Die IT Leitung der TARGET GmbH behält sich das Recht vor, Details zum eMail Verkehr (Absender, Empfänger, Zeitstempel und Größe, keinesfalls jedoch die Nachrichten selbst), sowie die Adressen besuchter Websites (ohne deren Inhalt und ohne einen direkten Personenbezug) zu Statistikzwecken und um mögliche Angriffe zu detektieren zu protokollieren.

Eine Archivierung und Löschung von eMails wird durch den IT Leiter vorgenommen.
Führen Sie regelmäßig die von den Betriebssystemherstellern veröffentlichten Sicherheitsupdates durch.
Deaktivieren Sie nach Möglichkeit aktive Inhalte (z.B. ActiveX) und Skriptsprachen (z.B. Visual Basic Script) in Ihrem Browser und nutzen Sie dessen Sicherheitsfunktionen.
Bei Problemen mit dem Zertifikat einer vermeintlich sicheren Website (Information durch den Browser) stoppen Sie im Zweifelsfall bitte die geplante Transaktion und wenden Sie sich an den Helpdesk der IT Leitung der TARGET GmbH (service@target-gmbh.de).
Klicken Sie nur auf Links in eMails und öffnen Sie nur dann eMail Attachments, wenn Ihnen die wahre Absenderin bzw. der wahre Absender bekannt ist oder Sie die eMail bzw. das Attachment erwarten.
Um Adressdatenmissbrauch zu vermeiden, verwenden Sie das Feld ≫BCC≪ anstelle des Feldes ≫An≪, wenn Sie ein E-Mail an mehrere, einander unbekannte Empfängerinnen bzw. Empfänger verschicken. Die Empfängerinnen bzw. Empfänger erhalten dadurch keine Information über weitere Empfängerinnen bzw. Empfänger derselben Nachricht.

4.3 Software

Allen Benutzerinnen und Benutzern ist es ausdrücklich untersagt, Software ohne Berechtigung oder von zweifelhaften Quellen zu installieren oder zu kopieren, sowie Software ohne gültige Lizenz auf Geräten der TARGET zu verwenden. Software aus zweifelhaften Quellen ist sehr oft mit Viren oder Spyware versehen, die heutzutage eine der größten Gefahren im Internet darstellen.

Nutzen Sie die vom jeweiligen Softwareprodukt angebotenen Sicherheitsfunktionen (z.B. Vergabe von Passwörtern für den Zugriff, automatische Speicherung von Zwischenergebnissen oder Verschlüsselungsmechanismen).
Lassen Sie veröffentlichte Sicherheitsupdates für die eingesetzten Softwareprodukte – wenn möglich automatisch – installieren.

4.4 Virenschutz

Zum Schutz vor Viren sind alle Arbeitsplätze der TARGET GmbH mit Windows als Betriebssystem mit Virenscannern des Herstellers Panda ausgestattet, die bei jedem Startvorgang automatisch mit gestartet werden und nicht deaktiviert werden dürfen. Alle Benutzerinnen und Benutzer sind dafür verantwortlich, Vireninfektionen zu verhindern.
Von Viren befallene Wechselmedien dürfen an Arbeitsplätzen der TARGET GmbH nicht verwendet werden (Prüfung vor Verwendung). Ebenso sind Dateien beim Download aus dem Internet, sowie per eMail erhaltene Dateien, besonders zu prüfen. Bitte wenden Sie sich im Zweifelsfall an service@target-gmbh.de.

Überprüfen Sie sämtliche nicht selbst erstellte Dateien bzw. Datenträger vor der Verwendung mit Hilfe eines Virenscanners, wenn dies nicht der Virenscanner schon selbständig durchführt (≫On-Access-Scanning≪).
Bei Problemen mit der Beseitigung von Viren mittels Virenscanner oder bei Verdacht einer Vireninfektion kontaktieren Sie umgehend den IT Leiter der TARGET GmbH.

4.5 Remote Access

Die TARGET GmbH stellt den Benutzerinnen und Benutzern in Ausnahmefällen einen externen Zugang zum Netzwerk der TARGET GmbH zur Verfügung. Die Benutzerinnen und Benutzer sind verpflichtet, bei der bzw. durch die Nutzung dieses Zugangs nicht gegen geltendes ¨Deutsches Recht zu verstoßen und den Zugang keinesfalls betriebsfremden Personen zugänglich zu machen. Der verwendete PC muss mit einem aktuellen, aktiven Virenscanner – insbesondere bei Windows-Computern – entsprechend der Vorgaben der IT Leitung der TARGET GmbH, sowie allen aktuellen Sicherheitsaktualisierungen ausgestattet sein.

4.6 Elektronische Akte

Die TARGET GMBH führt über jeden Teilnehmer eine elektronische Akte unter Verwendung der Anwendung StepNOVA der Firma Ergovia. Es wurde mit dieser Firma ein entsprechender Auftrags-Datenverarbeitungsvertrag geschlossen. Alle Teilnehmer Daten sind von den TARGET Mitarbeitern ausschließlich hier zu hinterlegen.

4.7 Öffentliche Cloud-Services

Viele Firmen bieten im Internet sogenannte Cloud-Services an. Zu den Anbietern gehören Firmen wie Google, Ubuntu, Dropbox, Microsoft, etc. Die angebotenen Dienste können – bei kleineren Datenmengen in den meisten Fällen sogar kostenlos – unter anderem zum Speichern von Office-Dokumenten, Dateien, persönlichen Kontaktdaten usw. verwendet werden. Mit der Möglichkeit der Freigabe dieser Dokumente für andere ergeben sich sehr einfache Möglichkeiten der Kooperation.
Probleme ergeben sich dadurch, dass hierbei die Daten an Dritte (in den meisten Fällen im Ausland, größtenteils in den USA) weitergegeben werden. Personenbezogene Daten dürfen jedoch laut DSGVO – vereinfacht gesagt – nicht, oder nur mit Zustimmung der Betroffenen weitergegeben werden.

Somit ist das Speichern von personenbezogenen Daten bei Cloud-Services den Mitarbeitern der TARGET GmbH untersagt!!

4.8 Videoaufzeichnungen

Die TARGET GmbH führt an keinem Standort eine Videoaufzeichnung als Zutrittskontrolle durch.
Sollte an einem Standort durch einen Mitarbeiter festgestellt werden das eine Kamera den Eingangsbereich überwacht oder für diese Zwecke neu installiert wurde ist umgehend der IT Leiter der TARGET GmbH zu informieren.

4.9 Datenentsorgung / Vernichtung

Alle Datenträger (z.B. Festplatten, USB-Sticks, Papier etc.) die personenbezogene oder andere kritische Daten enthalten, dürfen nicht ohne vorherige Unkenntlichmachung der darauf befindlichen Daten entsorgt werden, oder müssen geschreddert bzw. einer Fachfirma zur Vernichtung übergeben werden.
Für alle elektronischen Speicher die von der TARGET GmbH verwaltet werden, geschieht dies durch die IT Abteilung. Dies gilt auch für mobile Datenträger (USB-Sticks, externe Festplatten).
Größere Papiermengen können in über die Zentrale der TARGET GmbH entsorgt werden, kleinere Mengen sind mittels Dokumentenvernichter zu entsorgen.
Austauschbare Datenträger (CDs, DVDs etc.) sind deutlich zu beschriften um einen eventuell kritischen Inhalt leichter erkennen zu können.

5. Telefonkontakte

Grundsätzlich haben die Beratenden bei jedem Telefonat dafür Sorge zu tragen, dass Gespräche nicht von unberechtigten Dritten mitgehört werden können. Dies bedeutet, dass das Telefonat von den Mitarbeitern der TARGET GmbH zwingend in einem vor fremden Zuhörern geschützten Raum stattzufinden hat. Im Umkehrschluss ist auch den Teilnehmern anzuraten, dass diese Telefonate mit den Mitarbeitern der TARGET GmbH nicht in öffentlichen Bereichen (Park, Café, Zug, Supermarkt etc.) geführt werden. Um dies zu unterstützen, werden die Mitarbeiter der TARGET GmbH zu Beginn eines jeden Telefonates erfragen, ob die Teilnehmer sich an einem für das Telefonat geeigneten Ort aufhalten.

5.1. Erstkontakt zur Vereinbarung eines persönlichen Besprechungstermins

Bei der Kontaktaufnahme via Telefon zum Zwecke der Vereinbarung eines Beratungsgespräches können die Mitarbeiter der Target GmbH von Teilnehmern den Namen und die Kontaktdaten aufnehmen. Soweit Teilnehmer ihre Kontaktdaten ungefragt äußern und um eine Rückmeldung bitten, handelt es sich um eine unaufgeforderte Mitteilung. Eine solche Mitteilung ist als Einwilligung im Sinne des Art. 6 DSGVO (1) c. zur Erhebung der persönlichen Daten durch die Target GmbH zu qualifizieren. Die Mitarbeiter der TARGET GmbH sollten dennoch die Ratsuchenden hierauf hinweisen und explizit

erfragen, ob sie dieser Datenverarbeitung durch die TARGET GmbH zustimmen. Kontaktdaten sind: Name, Vorname, Anschrift, Telefonnummer, Emailadressen.

Weitere Daten werden die Mitarbeiter der TARGET GmbH während der ersten Kontaktaufnahme zu Vereinbarung eines Besprechungstermins nicht erheben!!!

Bei der ersten telefonischen Kontaktaufnahme können die Teilnehmer den Mitarbeitern der TARGET GmbH bereits umreißen, um welche Fragestellung es sich handelt und wie ihre persönliche Situation aussieht. Hierüber werden die Beratenden sich keine Aufzeichnungen machen!!

5.2. Erstkontakt mit Beratung am Telefon

Ein Erstkontakt mit sofortiger Beratung am Telefon ist nach DSGVO nicht zulässig da keine schriftliche Einwilligung in die Datenerfassung des Teilnehmers vorliegt. Und eine Beratung somit nicht dokumentiert werden kann.

5.3. Folgekontakte am Telefon

Ist der Teilnehmer in die Maßnahme aufgenommen werden der Teilnehmer und der Mitarbeiter der TARGET GmbH sich auf ein Kennwort zur Authentifizierung einigen. Dieses wird auch dem Stellvertreter oder der Stellvertreterin der MitarbeiterInn der TARGET GmbH bekannt gegeben.

6. Persönliche Gespräche in den TARGET Räumen

Durch die Mitarbeiter der TARGET GmbH ist sicherzustellen, dass das Gespräch vertraulich stattfindet. Die TARGET Mitarbeiter werden in der ersten Beratungssituation persönlich den Teilnehmern eine Einwilligungserklärung im Sinne dieses Datenschutzhandbuches übergeben und diese auch über die Datenschutzerklärung und den Datenschutz hinweisen sowie ihnen eine ausgedruckte Version der Datenschutzerklärung oder auf Wunsch eine elektronische Version (barrierefreie PDF) übersenden, so dass diese ohne weitere Barrieren die Möglichkeit haben, sich über die Datenschutzerklärung und das Datenschutzhandbuch zu informieren.
Erscheinen die Teilnehmer in Begleitung und sind Kontaktdaten von der Begleitperson als Ansprechpartner notwendig, ist von der Begleitperson eine datenschutzrechtlich relevante Einwilligung für die Speicherung, Erhebung und Verarbeitung sowie Nutzung der personenbezogenen Daten in Bezug auf die Kontaktaufnahme notwendig.
In dem Beratungsgespräch sind die Teilnehmer sowie deren Begleitung darauf hinzuweisen, dass die Mitarbeiter der TARGET GmbH als auch deren ständige Vertretung eine Verschwiegenheitsverpflichtung gegenüber der Target GmbH abgegeben haben.
Sie weisen ausdrücklich die Teilnehmer darauf hin, dass die Gesprächsinhalte im Rahmen des Beratungsprozesses nicht an Dritte weitergegeben werden und vor dem Zugriff unberechtigter Dritter geschützt werden, soweit personenbezogene Daten aufgenommen werden.

7. Umgang mit Twitter und Facebook

Eine Kontaktaufnahme seitens der Mitarbeiter der TARGET GmbH via Twitter, Faceboook, LinkedIN, XING oder anderen öffentlichen Plattformen im Internet in Richtung eines Teilnehmers ist strikt untersagt!!

8. Umgang mit WhatsApp

WhatsApp ist auf den Dientshandys der TARGET Mitarbeiter die eine aufsuchende Maßnahme begleiten eingerichtet zum Zwecke der Kontaktaufnahme des Teilnehmers in Richtung des Target Mitarbeiters um z.B. einen Termin absagen zu können. Es werden via WhatsApp keinerlei Daten übertragen, dies geschieht ausschließlich via eMail.
Eine Kommunikation der TARGET Mitarbeiter untereinander ist möglich, allerdings ist darauf zu achten das nur dienstliche Zwecke kommuniziert werden und auf keinen Fall personenbezogene Daten von Teilnehmern.

Änderungen des DS-Handbuches und mitgeltende Dokumente

Die Erstellung, Wartung und Publizierung dieses DS-Handbuches liegt im Verantwortungsbereich der bzw. des Datenschutzbeauftragten (DSB) der TARGET GmbH. Änderungswünsche sollen der bzw. dem DSB mitgeteilt werden (datenschutz@target-gmbh.de). Sie werden von der bzw. dem DSB geprüft und gegebenenfalls eingearbeitet. Die jeweils gültige Fassung der Datenschutzrichtlinie wird von der bzw. dem DSB im Intranet der TARGTET GmbH veröffentlicht.
Weiterführende Informationen zu den bei der TARGET geltenden Grundsätzen in Bezug auf IT-Sicherheit und den Umgang mit personenbezogenen Daten finden sich in den nachfolgend gelisteten Dokumenten. Die Dokumente können in ihrer jeweils geltenden Fassung über das Intranet der TARGET GmbH bzw. das Internet bezogen werden.

Regelungen und Richtlinien der TARGET GmbH

- Datenschutzerklärung der TARGET GmbH
- Dienstanweisung für Mitarbeiter der TARGET GmbH: Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz
- Technisch- Organisatorische Maßnahmen zum Datenschutz bei der TARGET GmbH
- Sonstige Anleitungen, Regelungen und Richtlinien

Geltende Gesetze:

- Datenschutz Grundverordnung der Europäischen Union vom 22.11.2016
- Gesetz zur Anpassung des Datenschutzrechts an die Verordnung EU 216/679 und zur Umsetzung der Richtlinie EU 2016/680 (Datenschutzanpassungsgesetz – DSAnpUG-EU) vom 30.06.2017 auch Bundesdatenschutzgesetz neu genannt.
- Telemediengesetz (TMG) vom 26.02.2007
- Gesetz gegen den unlauteren Wettbewerb (UWG) vom 03.03.2010