Beschreibung des METRO

Datenschutz Management Systems

Datenschutz-Kultur

Datenschutzmission

1. In Sachen Datenschutz hat der Vorstand der METRO AG die organisatorische und aufsichtführende Verantwortung. Um dieser Verantwortung nachzukommen, hat das Corporate Data Protection Department (DPD) ein risikobasiertes Datenschutz Management System (DMS) eingerichtet.

2. Wesentliches Element des DMS ist die Allgemeine Datenschutzrichtlinie der METRO (Datenschutzrichtlinie), die u.a. einen organisatorischen Rahmen für den Datenschutz innerhalb der METRO-Unternehmensgruppe (METRO) schafft und die näheren Verantwortlichkeiten für den Datenschutz festgelegt. Darin werden bestimmte Kriterien für die Schaffung und den Betrieb einer geeigneten Compliance-Organisation in Bezug auf die Behandlung von Datenschutzfragen festgelegt.

Schaffung eines Datenschutzbewusstseins

3. METRO ist der Ansicht, dass für ein wirkungsvolles DMS eine nachhaltig positive Datenschutz-Kultur ausschlaggebend ist. Die Datenschutz-Kultur der METRO kommt zum Ausdruck in der Art und Weise, wie einzelne METRO-Mitarbeiter mit personenbezogenen Daten umgehen, sie schützen und den Umgang bzw. den Schutz von vorneherein nachvollziehbar machen.

4. Datenschutz-Kultur betrifft alle Funktionsbereiche. Eine positive Datenschutz-Kultur hat ihren Ausgang an der Unternehmensspitze: in den Geschäftsführungen der METRO. Führungskräfte sind in der Verantwortung, Vorbilder zu sein, indem sie die Einhaltung datenschutzrechtlicher Vorgaben fördern. METRO sieht diesbezüglich insbesondere die Vorstände und die Geschäftsführungen in der Pflicht. Das gleiche trifft aber auch auf alle Führungskräfte unterhalb der Geschäftsführerebene zu, sowohl in den Hauptverwaltungen als auch in den Märkten.

5. Die wichtigsten Ecksteine der Datenschutz-Kultur der METRO sind der Schutz der Privatsphäre der Mitarbeiter, Kunden und Geschäftspartner. METRO ist bewusst, dass der Schutz deren Grundrechte ein unverzichtbarer Bestandteil der Unternehmenskultur ist und dass die Einhaltung dieser Standards das Selbstverständnis als attraktiver Arbeitgeber sowie die interne und externe Reputation unmittelbar beeinflussen wird. METRO ist ferner bewusst, dass die Einhaltung der Datenschutzbestimmungen ein wesentlicher Bestandteil der gesamten Compliance-Strategie des Konzerns und ein wichtiger Faktor bei der Abwehr von Imageverlust und an-

deren damit verbundenen Gefahren für die METRO und ihre Marken ist. Der Vorstand richtet sich zur Datenschutz-Kultur im Intranet an die Mitarbeiter, verankert den Schutz der Privatsphäre als unverzichtbaren Baustein der Entwicklung der Unternehmenskultur und betont die besondere Verantwortung, die dem Unternehmen in dieser Hinsicht zukommt.

6. METRO beabsichtigt, technische Innovationen kontinuierlich zum Nutzen des Konzerns, seiner Mitarbeiter und Kunden einzusetzen. Im Rahmen ihrer Digitalisierungsstrategie will die METRO die Wertschöpfungskette der personenbezogenen Daten optimieren, den Datenfluss im Konzern straffen und innovative digitale Geschäftsmodelle schaffen. Die Sicherstellung der Nutzbarkeit des bestehenden und neu entstehenden Datenportfolios wird daher eine unverzichtbare Voraussetzung für die künftige Geschäftsstrategie des Konzerns sein, die wiederum nur unter strikter Einhaltung der Datenschutzbestimmungen erreicht werden kann.

7. METRO betrachtet jeden Geschäftsprozess, der mit der Verarbeitung personenbezogener Daten verbunden ist (Verarbeitungstätigkeit), als Chance, um ein besseres Verständnis für die Kunden zu erlangen, die interne Zusammenarbeit und die Leistungsfähigkeit des Unternehmens weiter zu verbessern und neue Marktchancen zu entdecken und zu nutzen.

8. Ob Mitarbeiter sich gemäß den dienstlichen Vorgaben zum Datenschutz verhalten, wird im Rahmen des regulären Beurteilungsprozesses für METRO-Mitarbeiter evaluiert. Etwaige Verstöße gegen die Vorgaben zum Datenschutz werden im Rahmen dieses Prozesses aufgegriffen und bei den regulären Beurteilungen Rechnung getragen.

Datenschutz-Ziele

Definition von Datenschutz-Compliance

1. Das DMS bezweckt, das Unternehmen in Übereinstimmung mit anwendbaren Gesetzen und internen Richtlinien, welche die relevanten Datenschutz-Risikobereiche betreffen, zu führen.

2. Das DMS ist Bestandteil der allgemeinen Compliance-Strategie des Unternehmens zum rechtmäßigen Handeln. Das DMS unterstützt das Unternehmen dabei, sich an die Vorgaben von Recht und Gesetz im Bereich des Datenschutzes zu halten und somit öffentlich-rechtliche Maßnahmen – insbesondere Bußgelder – sowie zivilrechtliche Ansprüche und Reputationsschäden von METRO abzuwenden.

3. Grundpfeiler dabei sind stets die national verbindlichen gesetzlichen Vorschriften zum Datenschutz (innerhalb Deutschlands etwa das Bundesdatenschutzgesetz sowie spezifische Datenschutzvorschriften anderer Gesetze, Rechtsverordnungen und Satzungen), innerhalb der Europäischen Union somit insbesondere die Datenschutz-Grundverordnung 2016/679 der Europäischen Union (DSGVO). Darüber hinaus ist intern die Datenschutzrichtlinie für das gesamte Unternehmen verbindlich, soweit dort nicht ausdrücklich anders bestimmt.

DMS-Konzept

4. Die geltenden gesetzlichen Vorschriften sind vom Datenschutzbeauftragten ständig auf Aktualität und etwaig anstehende Änderungen oder Ergänzungen zu prüfen. Daneben sind auch Stellungnahmen zuständiger Behörden sowie Gerichtsentscheidungen zur Kenntnis zu nehmen und zu überprüfen. Sich daraus eventuell ergebende Änderungsbedarfe fließen in das DMS und die internen Vorgaben zum Datenschutz ein.

5. Jede Verarbeitung personenbezogener Daten ist daher dahingehend zu prüfen, ob sie mit den anwendbaren Gesetzen sowie der Datenschutzrichtlinie vereinbar ist. Dazu ist es zunächst erforderlich, den zugrundeliegenden Sachverhalt aufzuklären und diesen anhand des Maßstabs der genannten Vorgaben zu prüfen. Bei verbleibenden Unsicherheiten und Risiken nach vollständiger Prüfung ist stets eine Abwägung des datenschutzrechtlichen Risikos mit etwaigen unternehmerischen Vor- und Nachteilen vorzunehmen.

Geltungsbereich des DMS

6. Das DMS gilt für alle Konzerngesellschaften der METRO weltweit (METRO-Gesellschaften). Allerdings gelten für Verarbeitungen personenbezogener Daten im Geltungsbereich der DSGVO erhöhte interne Voraussetzungen, die in der Datenschutzrichtlinie ausdrücklich bestimmt sind.

7. Innerhalb einer METRO-Gesellschaft unterfallen sämtliche Geschäftsbereiche und -prozesse dem DMS. Es gibt keine Erleichterungen oder geringeren Anforderungen an „unwesentliche" Prozesse, etwa wenn Daten nur in geringem Umfang verarbeitet werden (geringe Anzahl von Betroffenen). Sobald ein Prozess die Verarbeitung personenbezogener Daten zum Gegenstand hat, muss er sich an den Vorgaben des DMS messen lassen. Lediglich solche Prozesse, die vollkommen ohne die Verarbeitung personenbezogener Daten ablaufen, sind nicht vom DMS umfasst.

8. Ebenso gilt das DMS für alle Arten personenbezogener Daten, unabhängig davon, ob es sich um personenbezogene Daten von Kunden, Lieferanten, Mitarbeitern oder sonstigen Betroffenen handelt. Mitarbeiter unterliegen insoweit der Besonderheit, dass sie zugleich personenbezogene Daten verarbeiten, aber auch von der Datenverarbeitung betroffen sein können.

Datenschutz-Ziele

9. Datenschutz-Ziele sind sowohl die Einhaltung verbindlicher Datenschutzvorgaben geltenden Rechts als auch die Absicht, METRO als verlässlichen Partner für Kunden und Geschäftspartner sowie auch für die eigenen Mitarbeiter darzustellen. Ein weiteres Ziel ist es, personenbezogene Daten – unter Beachtung der Vorgaben des Datenschutzes – für neue Geschäftsstrategien zu nutzen.

10. Die Ziele des DMS werden neben der Datenschutzrichtlinie auch in Handreichungen sowie auf allgemein zugänglichen Informationsseiten im Intranet kommuniziert. Daneben sind sie auch Teil der nichtfinanziellen Erklärung (NFE) von METRO.

11. Die Erreichung der Datenschutzziele wird in jährlichen Datenschutzberichten jeder Gesellschaft festgehalten, die vom jeweiligen Datenschutzbeauftragten der Gesellschaft erstellt und den Geschäftsführungen vorgestellt werden.

Datenschutz-Organisation

Aufbau- und Ablauforganisation

1. Die Datenschutz-Organisation der METRO ist auf strukturelle und operative Effizienz ausgelegt. Innerhalb der Datenschutz-Organisation sind verschiedene Rollen festgelegt.

2. Die Geschäftsführungen der jeweiligen METRO-Gesellschaften sind verpflichtet, alle Maßnahmen zu definieren und umzusetzen, die erforderlich sind, um die Einhaltung der geltenden Datenschutzbestimmungen durch ihre Gesellschaft zu gewährleisten. Die Geschäftsführungen sind für die Einhaltung der geltenden datenschutzrechtlichen Gesetze und Vorschriften in ihrem Betrieb verantwortlich. Sie setzen Vorgaben der Konzernleitung zum Datenschutz unter Berücksichtigung ggf. anwendbarer rechtlicher Abweichungen aufgrund nationalen Rechts um. Die Konzernleitung trifft insoweit eine Unterstützungs- und Überwachungspflicht. Die Geschäftsführungen der METRO-Gesellschaften Konzerngesellschaften stellen innerbetrieblich die erforderlichen personellen, organisatorischen und finanziellen Ressourcen bereit, um ein dem jeweiligen Rechtsrahmen nach angemessenes Datenschutzniveau zu gewährleisten.

3. Jede METRO-Gesellschaft hat hierzu unter den Voraussetzungen der Anlage 2 der Datenschutzrichtlinie einen Datenschutzbeauftragten zu benennen – auch in Fällen, in denen dies gesetzlich nicht gefordert ist. Der Datenschutzbeauftragte erfüllt für die METRO-Gesellschaft sämtliche ihm nach jeweils anwendbarem Recht obliegenden Aufgaben und Pflichten gemäß Anlage 2 der Datenschutzrichtlinie, insbesondere (a.) die Beratung der METRO-Gesellschaft in Datenschutzbelangen, (b.) die Unterstützung der METRO-Gesellschaft bei der Einhaltung der jeweils anwendbaren Datenschutzgesetze, der Datenschutzrichtlinie sowie sonstiger intern verbindlicher Vorgaben der METRO im Bereich des Datenschutzes und (c.) die Überwachung all dieser Vorgaben.

4. Von jedem Datenschutzbeauftragten wird eine enge Zusammenarbeit mit der jeweiligen Geschäftsführung erwartet. Der jeweilige Datenschutzbeauftragte berichtet direkt an die Geschäftsführung und stimmt Datenschutz-Themen eng mit ihr ab, z.B. im Rahmen regelmäßiger Besprechungen mit dem für Datenschutz zuständigen Geschäftsführer.

5. Aufgabe des DPD als zentraler Einheit im Datenschutz ist es, METRO-Gesellschaften und ihre Datenschutzbeauftragten in Datenschutzfragen zu unterstützen und das bestehende Datenschutz-Regelwerk ständig zu aktualisieren und anzupassen.

6. Neben der konzeptionellen DMS-Verantwortung unterstützt das DPD alle METRO-Gesellschaften und deren Datenschutzbeauftragte bei der Umsetzung der DMS-Maßnahmen. Das DPD bietet darüber hinaus eine große Auswahl praktischer Hilfsmittel, Vorlagen und Informationen zur Anwendung im Tagesgeschäft an.

7. Innerhalb des DPD arbeiten mindestens zwei Datenschutz-Manager, die für übergeordnete Datenschutzbelange der METRO zuständig sind. Die Datenschutz-Manager übernehmen u.a. die Aufgabe (a.) der Beratung der Datenschutzbeauftragten in Datenschutzfragen, (b.) die Koordination von Datenschutzfragen mit Bezug zu Konzernbelangen, (c.) die Überwachung der Datenschutzbeauftragten und (d.) die Erstellung regelmäßiger Berichte über den allgemeinen Datenschutzstatus bei METRO. Die Datenschutz-Manager sind berechtigt, von METRO-Gesellschaften Auskunft über sämtliche Prozesse und Umstände des Umgangs mit personenbezogenen Daten zu verlangen. Sie berichten unmittelbar an den Vorstand der METRO AG.

8. Jede METRO-Gesellschaft muss mindestens einen Datenschutzkoordinator ernennen. Sofern es der Datenschutzbeauftragte für erforderlich hält, sind auf seinen Vorschlag hin im gegenseitigen Einvernehmen mit der Geschäftsführung der METRO-Gesellschaft im jeweils angemessenen Umfang weitere Datenschutzkoordinatoren zu ernennen. Aufgabe der Datenschutzkoordinatoren ist im Wesentlichen die Unterstützung des Datenschutzbeauftragten und der Geschäftsführung bei der Einhaltung geltenden Datenschutzrechts einschließlich der Datenschutzrichtlinie und sonstiger intern verbindlicher Vorgaben der METRO im Bereich des Datenschutzes.

9. Die Verantwortlichkeit gegenüber der Geschäftsführung für die datenschutzrechtliche Gesamtkonformität eines Geschäftsprozesses verbleibt beim Prozessverantwortlichen, also der für den jeweiligen Geschäftsprozess operativ zuständigen Person. Der Prozessverantwortliche kann sich hierzu mit dem Datenschutzbeauftragten und den Datenschutzkoordinatoren abstimmen und diese um Hilfe ersuchen. Er ist für die Pflege und Aktualität des Verzeichnisses der Verarbeitungstätigkeiten verantwortlich.

10. Unterstützung bei der Umsetzung von datenschutzrechtlichen Vorgaben in dem IT-System, insbesondere die Mitwirkung bei Umsetzung von Löschkonzepten oder die Berücksichtigung der Vorgaben von „Privacy by Design" und „Privacy by Default", erfolgt durch den Systemverantwortlichen. Systemverantwortlicher ist die zuständige Person für das jeweilige IT-System, welches für die Verarbeitung der personenbezogenen Daten benutzt wird.

11. Für die genannten Rollen in der Datenschutz-Organisation gibt es zentral definierte Qualifikationen in Anlage 2 der Datenschutzrichtlinie, die erforderlich sind, um die Rolle bekleiden zu können.

Datenschutzbeauftragter

12. In jeder METRO-Gesellschaft ist ein Datenschutzbeauftragter zu benennen, wenn sich dies aus den in der Anlage 2 zur Datenschutzrichtlinie festgelegten Kriterien ergibt. Als Datenschutzbeauftragter darf nur berufen werden, wer die in der Stel-

lenbeschreibung in Anlage 2 der Datenschutzrichtlinie beschriebenen Anforderungen erfüllt. Es ist insbesondere sicherzustellen, dass die Person über die erforderliche Qualifikation verfügt, um die Rolle als Datenschutzbeauftragter ausüben zu können. Im Falle einer Aktualisierung der Stellenbeschreibung wird die jeweilige METRO-Gesellschaft prüfen, ob der Datenschutzbeauftragte die Anforderungen weiterhin erfüllt.

13. Jede METRO-Gesellschaft gewährleistet, dass der Datenschutzbeauftragte den ihm obliegenden und in Anlage 2 der Datenschutzrichtlinie definierten Verpflichtungen nachkommen und die ihm zustehenden Befugnisse ausüben kann. Insbesondere ist dem Datenschutzbeauftragten Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zu gewähren. Die Unabhängigkeit und Weisungsfreiheit des Datenschutzbeauftragten ist durch die METRO-Gesellschaft sicherzustellen. Der Datenschutzbeauftragte ist in Entscheidungs- und Informationsprozesse frühzeitig einzubinden.

14. Die Kontaktdaten des Datenschutzbeauftragten werden im Unternehmen sowie extern kommuniziert und der zuständigen Datenschutzbehörde bekannt gemacht.

15. Eine Beratung und Unterstützung des Datenschutzbeauftragten bei der Umsetzung von Maßnahmen, welche die Einhaltung der einschlägigen Datenschutzbestimmungen gewährleistet, erfolgt durch die Datenschutz-Manager. Darüber hinaus ist der Datenschutzbeauftragte befugt, die Rechtsabteilung der jeweiligen METRO-Gesellschaft in rechtlichen Fragen mit Bezug und Relevanz für die datenschutzrechtlichen Belange zu konsultieren und/oder externe Rechtsberatung einzuholen.

16. Durch den zuständigen Datenschutz-Manager wird eine länderübergreifende und einheitliche Beratung der METRO-Gesellschaften sichergestellt.

17. Der Datenschutzbeauftragte sowie die zur Erfüllung der dem Datenschutzbeauftragten obliegenden Tätigkeiten eingesetzten Mitarbeiter sind nachweislich zur Verschwiegenheit zu verpflichten.

18. Die Zusammenarbeit mit und die Koordination von Datenschutzbelangen der METRO-Gesellschaft gegenüber Aufsichtsbehörden und Betroffenen erfolgt durch den Datenschutzbeauftragten.

Integration der Datenschutz-Funktion und Schnittstellen zu weiteren Governance-Funktionen

19. Die mit datenschutzrechtlichen Aufgaben befassten Abteilungen und Funktionen innerhalb der jeweiligen METRO-Gesellschaften stehen zum Zwecke des fachlichen Abstimmungs- und Koordinationsbedarf im Austausch mit verschiedenen anderen Funktionen innerhalb der eigenen Gesellschaft. Dies sind im Einzelnen die folgenden Abteilungen: Compliance, Informationssicherheit, Revision, Mitarbeitervertretung sowie die Rechtsabteilung. Zwischen den einzelnen Abteilungen sowie dem Datenschutzbeauftragten hat ein regelmäßiger gegenseitiger Informationsaustausch zu erfolgen.

Risiken

Datenschutzrechtliches Risikomanagement

1. Das DMS der METRO adressiert verschiedene Risikobereiche, die sich aus den jeweils geltenden datenschutzrechtlichen Vorgaben ergeben. Dazu gehören insbesondere die Dokumentations- und Rechenschaftspflichten, die allgemeinen gesetzlichen Datenschutzgrundsätze, Löschpflichten, Betroffenenrechte sowie die Sicherheit der Datenverarbeitung.

2. Im Rahmen des globalen DMS werden Datenschutz-Risiken adressiert, indem bestimmte strukturelle und operative Maßnahmen definiert werden und diese Maßnahmen von den Datenschutzbeauftragten der METRO-Gesellschaften erfüllt bzw. überwacht werden. Die Definition dieser Maßnahmen erfolgt durch die Datenschutz-Manager im DPD. Die Maßnahmen dienen nur der Erfüllung der Mindestanforderungen. Jede METRO-Gesellschaft, insbesondere die Landesgeschäftsführung und der zuständige Datenschutzbeauftragte, sind angehalten zu erwägen, ob zusätzliche Maßnahmen erforderlich sind, um Datenschutz-Risiken angemessen zu adressieren.

3. Die Erfüllung der Maßnahmen sowie weitere Schlüsselindikatoren werden für jede METRO-Gesellschaft in einer Datenschutz-Reifegrad-Matrix überwacht. Die Reifegrad-Matrix errechnet einen sog. Reifegradwert, dessen bestmöglicher Wert 100% ist und der den Datenschutz-Reifegrad der einzelnen METRO-Gesellschaft widerspiegelt.

4. Maßnahmen müssen angepasst werden, soweit lokale Gesetzgebung einen strengeren Ansatz verlangt.

5. Jede METRO-Gesellschaft nimmt im Rahmen der von der METRO AG konzernweit durchgeführten Risikoinventur eine jährliche Bewertung der Datenschutz- Risiken anhand von Prüfkriterien vor. Hierbei sind bestehende Datenschutz-Risiken bei Bedarf zu aktualisieren und neu hinzugekommene Datenschutz-Risiken zu ergänzen. Die Bewertung dieser erfolgt unter Einbindung des Datenschutzbeauftragten.

6. Die Prozessverantwortlichen führen Risikoanalysen der Verarbeitungstätigkeiten durch, um potentielle neue Datenschutz-Risiken zu identifizieren und – falls notwendig – bestehende Datenschutz-Risiken neu zu qualifizieren. Die Häufigkeit dieser Analysen hängt von der Einstufung des jeweiligen Datenschutz-Risikos ab. Risikoanalysen von Verarbeitungstätigkeiten mit hohem oder sehr hohem Datenschutz-Risiko werden jährlich vorgenommen, sofern nicht aufgrund von behördlichen Vorgaben und/oder Gerichtsentscheidungen eine unterjährige Überprüfung geboten ist.

7. Risikoanalysen bestehen aus bilateralen Gesprächen oder aus einem Workshop-Format, jeweils mit dem zuständigen Mitarbeiter aus der IT-Abteilung sowie dem Datenschutzbeauftragten der jeweiligen Gesellschaft anwesend. Im Falle von konzernübergreifenden Verarbeitungen ist der Datenschutz-Manager in Kenntnis zu setzen und im Einzelfall hinzuzuziehen.

8. Ungeachtet des ausgewählten Formats muss die Risikoanalyse folgende Elemente umfassen:

   - Risikoidentifizierung auf der Grundlage von Risikoszenarien, die bespielhaft unterschiedliche Arten von Datenschutz-Risiken aufzeigen;

   - Risikoeinschätzung auf der Grundlage von potentiellem Schaden und Eintrittswahrscheinlichkeiten (Formel = Schadenshöhe x Eintrittswahrscheinlichkeit = Risiko).

   - Risikoklassifizierung: Schadenshöhe und Eintrittswahrscheinlichkeit sind in vier Stufen (Klassifizierungen) einzuteilen: „niedrig", „mittel", „hoch" und „sehr hoch". Im Rahmen der Risikoklassifizierung sind die folgenden Kriterien zugrunde zu legen: a) Bewertung/Scoring (inkl. Profiling), b) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung, c) Systematische Überwachung; Vertrauliche Daten oder höchst persönliche Daten, d) Datenverarbeitung in großem Umfang, e) Abgleichen oder Zusammenführen von Datensätzen, f) Daten zu schutzbedürftigen Betroffenen, g) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen, h) Datentransfer außerhalb der EU, i) etwas, dass die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert.

   - Risikosteuerung, um bereits bestehende sowie während der Einschätzung neu identifizierte Risiken angemessen zu behandeln.

9. Die Datenschutz-Risiken sind für jede Verarbeitungstätigkeit im Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren und soweit erforderlich mindestens jedoch bei hohen und sehr hohen Datenschutz-Risiken gegenüber der jeweiligen Geschäftsführung zum Zeitpunkt der Identifikation des Datenschutzrisikos zu kommunizieren. Darüber hinaus hat eine dem Datenschutz-Risiko angemessene Überwachung und Dokumentation der Verarbeitungstätigkeit durch den Datenschutzbeauftragten zu erfolgen.

10. Das DPD vermittelt den mit dem Datenschutz betrauten Fachabteilungen sowie insbesondere dem Datenschutzbeauftragten spezifisches Wissen, insbesondere zur Methodik der richtigen Durchführung von Risikoanalysen und in Übereinstimmung mit den Anforderungen des METRO-Risiko-Managements.

Datenschutz-Folgenabschätzung (DSFA)

11. Verarbeitungen personenbezogener Daten können ein erhöhtes Risiko für die Rechte Betroffener auf Privatsphäre und Datenschutz darstellen. Im Falle eines erhöhten Risikos führt der Prozessverantwortliche der jeweiligen METRO-Gesellschaft eine vorherige Risikoanalyse nach Maßgabe des Art. 35 DSGVO durch.

12. Für die Durchführung der Datenschutz-Folgenabschätzung ist das im Intranet abrufbare Dokument „Datenschutz-Folgenabschätzung" zu verwenden. Dieses be-

rücksichtigt die geltenden gesetzlichen Regelungenwie beispielsweise die Pflicht zur Benachrichtigung der Behörde. Die Datenschutz-Folgenabschätzung soll insbesondere Risikoquellen und -szenarien, Eintrittswahrscheinlichkeiten sowie die Höhe eines möglichen Schadens beinhalten. Die in diesem Dokument enthaltene Prozessbeschreibung ist verbindlich. Die Dokumentation hat im Verzeichnis der Verarbeitungstätigkeiten zu erfolgen.

13. Die Erforderlichkeitsprüfung sowie die Datenschutz-Folgenabschätzung sind vom Prozessverantwortlichen unter Mitwirkung des Datenschutzkoordinators und ggf. des Datenschutzbeauftragten durchzuführen.

Datenschutz-Programm

Richtlinien zum Datenschutz

1. Das Datenschutz-Regelwerk besteht zunächst aus der Datenschutzrichtlinie, deren Anlagen und den darin konkret erwähnten Arbeitsanweisungen. Die Datenschutzrichtlinie wurde vom Vorstand der METRO AG verabschiedet. Darüber hinaus werden weitere Vorgaben durch spezifische Richtlinien und Leitfäden aufgestellt. Aufgrund eines allgemeinen Verweises in der Datenschutzrichtlinie sind diese verbindlich. Das komplette Regelwerk ist via Intranet abrufbar. Die Datenschutzrichtlinie wurde an diejenigen versendet, die gemäß der Konzernrichtlinie „Grundsätze des Regelungsmanagement" dafür verantwortlich sind.

2. Neue Regeln und Änderungen im vorhandenen Regelwerk werden gegenüber den Verantwortlichen bekannt gemacht. Für die Kommunikation, die Aktualität und um die Verbindlichkeit des Regelwerks in den METRO-Gesellschaften sicherzustellen, gibt es mit der Konzernrichtlinie „Grundsätze des Regelungsmanagement" eine eigene Richtlinie mit entsprechenden Vorgaben. Die METRO-Gesellschaften sind aufgrund dessen verpflichtet, das Regelwerk nach den Anforderungen des lokalen Rechts als verbindliche Anweisung in der Gesellschaft zu installieren.

3. Das Regelwerk muss von den METRO-Gesellschaften zur besseren Verständlichkeit auch in der jeweiligen Landessprache angeboten werden.

4. Der Vorstand trägt dafür Sorge, dass das Datenschutz-Management im Rahmen eines periodisch-zyklischen Optimierungsprozesses (Plan-Do-Check-Act) an rechtliche, organisatorische und technische Änderungen betreffend die Verarbeitung personenbezogener Daten jeweils risikogerecht und entsprechend der jeweils anwendbaren gesetzlichen Vorgaben angepasst wird. Das Datenschutz-Regelwerk wird insoweit vom DPD aktualisiert und angepasst, so dass es den derzeitigen rechtlichen Vorgaben entspricht. Dies ist eine der Kernaufgaben des DPD.

Verarbeitungsverzeichnis

5. Jede METRO-Gesellschaft hat ein Verzeichnis von Verarbeitungstätigkeiten zu führen und regelmäßig zu aktualisieren. In diesem Verzeichnis sind alle Verarbeitungstätigkeiten aufzunehmen, in denen eine Verarbeitung personenbezogener

Daten stattfindet. Für die Aufnahme und Pflege eines Prozesses ist der jeweilige Prozessverantwortliche zuständig. Der Datenschutzkoordinator des jeweiligen Geschäftsbereichs unterstützt dabei, dass alle Prozessverantwortlichen in einem Geschäftsbereich die von ihnen verantworteten Verfahren erfassen.

6. Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gilt kraft Datenschutzrichtlinie auch dann, sofern eine solche Pflicht für die jeweilige METRO-Gesellschaft nicht gesetzlich angeordnet ist. Ist die Führung eines Verzeichnisses von Verarbeitungstätigkeiten hingegen gesetzlich angeordnet, gelten die gesetzlichen Bestimmungen zur Art und Weise der Führung des Verzeichnisses von Verarbeitungstätigkeiten vorrangig vor den Vorgaben der Datenschutzrichtlinie, soweit Abweichungen bestehen.

7. Im Anwendungsbereich der DSGVO gelten besondere Vorgaben für die Führung eines Verzeichnisses von Verarbeitungstätigkeiten, die in Anlage 1 der Datenschutzrichtlinie bestimmt sind. Dies dient dazu, die Vorgaben von Art. 30 DSGVO umzusetzen.

8. Die Erfassung der Verfahren erfolgt softwaregestützt, derzeit über die Softwareanwendung „PrIME". Jeder Prozessverantwortliche erhält vom Datenschutzbeauftragten der jeweiligen Gesellschaft einen web-basierten Fragebogen, in den er alle für das Verfahren relevanten Angaben einpflegen kann. Die Antworten werden automatisch in „PrIME" übertragen.

9. Die Prozessverantwortlichen werden durch Musterfragebögen sowie durch Instruktionen (Tutorials) beim Ausfüllen der Fragebögen unterstützt. Zudem können sie sich an die Datenschutzkoordinatoren und/oder den Datenschutzbeauftragten wenden. Zudem stehen weitere Materialien zur Unterstützung der Prozessverantwortlichen zur Verfügung. Für Verarbeitungen, die auf einer Einwilligung basieren, stellt das DPD neben den Vorgaben der Datenschutzrichtlinie beispielsweise ein Muster-Einwilligungsdokument im Intranet zur Verfügung, das die Pflichtvorgaben einer wirksamen Einwilligung beinhaltet, inklusive einer Formulierung sowie von (Platzhalter-)Kontaktdaten zum Widerruf.

10. Die Angaben im Verzeichnis der Verarbeitungstätigkeiten sind bei Änderungen der Verarbeitungstätigkeit anlassbezogen zu aktualisieren. Eine anlassbezogene Änderung kann etwa bei Zweckänderungen der Verarbeitung erforderlich sein. Ob und wann dies der Fall ist, ergibt sich aus einer im Intranet veröffentlichten Arbeitsanweisung zum Umgang mit Zweckänderungen. Ansonsten werden die Prozessverantwortlichen vom Datenschutzbeauftragen regelmäßig (derzeit einmal jährlich) zur Überprüfung des Verfahrens aufgefordert, indem ihnen der Fragebogen des bestehenden Verfahrens zur Überprüfung zugesendet wird.

11. Jeder Datenschutzbeauftragte hat Zugriff auf das Verzeichnis der Verarbeitungstätigkeiten der Gesellschaft, für die er bestellt ist und überwacht die Vollständigkeit und Aktualität des Verzeichnisses der Verarbeitungstätigkeiten. Im Rahmen der Überwachung prüft er die jeweilige Verarbeitungstätigkeit auch im Hinblick auf die Zulässigkeit der Verarbeitung.

12. Die jeweiligen Datenschutz-Manager national/international haben Zugriff auf die Verfahren aller Gesellschaften, die von ihnen betreut werden.

Technische und Organisatorische Maßnahmen

13. Jede METRO-Gesellschaft hat erforderliche technische und organisatorische Maßnahmen (TOM) zum Schutz personenbezogener Daten zu treffen.

14. Die Erforderlichkeit der technischen und organisatorischen Maßnahmen bestimmt sich anhand einer risikobezogenen Abwägung. Zu bewerten sind hierbei insbesondere die Zwecke der Verarbeitung sowie die unter Berücksichtigung des jeweils aktuellen Stands der Technik aus Art, Umfang und Umständen der Verarbeitung resultierende Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten Betroffener als auch die Implementierungskosten für etwaige technische und organisatorische Maßnahmen.

15. Sämtliche bei METRO eingesetzte IT-Systeme sind in einem Online-Tool dokumentiert. Dort ist jeweils die Funktion des IT-Systems beschrieben. Zudem ist der Verantwortliche genannt, an den man sich bei Fragen zum IT-System wenden kann.

16. Jeder Prozessverantwortliche ist dazu verpflichtet, erforderliche technische und organisatorische Maßnahmen für von ihm verantwortete Verarbeitungstätigkeiten umzusetzen und diese im Verzeichnis der Verarbeitungstätigkeiten abzubilden. Die Berücksichtigung und Umsetzung von technischen und organisatorischen Maßnahmen für bestimmte Verfahren erfolgt im Zusammenspiel zwischen Prozessverantwortlichen, Systemverantwortlichen und Datenschutzbeauftragten.

17. Für METRO-interne Verarbeitungstätigkeiten gibt es einen METRO TOM-Standardkatalog, der standardmäßige technische und organisatorische Maßnahmen, die quer über alle Verfahren in der METRO IT-Infrastruktur vorhanden sind, abbildet.

18. Der METRO TOM-Standardkatalog basiert auf der internen METRO IT-Security-Richtlinie, die umfangreich und in detaillierter Form IT-Sicherheitsmaßnahmen im Unternehmen beschreibt. Diese Richtlinie wird von der Abteilung IT-Security verantwortet und regelmäßig (die IT Security Management Prinzipien jährlich, die Richtlinie regelmäßig im Rahmen geplanter Intervalle sowie bei Bedarf) aktualisiert. Aktualisierungen der Richtlinie werden anschließend zwischen der Abteilung IT-Security und dem DPD hinsichtlich ihrer Implikationen in Bezug auf den Datenschutz besprochen und sodann bei Bedarf im METRO TOM-Standardkatalog reflektiert. Eine neue Fassung des METRO TOM-Standardkatalogs wird gemeinsam von der Abteilung IT Security und dem DPD verabschiedet und wird in dieser Form als TOM-Standardkatalog im Verzeichnis von Verarbeitungstätigkeiten hinterlegt, nachdem die Maßnahmen von IT Security und dem DPD als angemessen und wirksam beurteilt wurden.

Privacy by Design und Privacy by Default

19. Bei der Berücksichtigung und Umsetzung von technischen und organisatorischen Maßnahmen werden insbesondere die datenschutzrechtlichen Grundsätze des „Privacy by Design" und „Privacy by Default" angewendet. Es gibt hierzu in Anlage 4 der Datenschutzrichtlinie umfassende Regeln, die geeignete Unternehmensabläufe festlegen, um sicherzustellen, dass die Grundsätze befolgt werden. Die Regeln gelten insbesondere für die Neuentwicklung und Weiterentwicklung bestehender IT-Systeme bzw. Anwendungen.

Betroffenenrechte und Informationspflichten

20. Die von der Verarbeitung personenbezogener Daten durch METRO Betroffenen sind im Einklang mit den gesetzlichen Vorgaben über die Verarbeitung personenbezogener Daten zu informieren. Personenbezogene Daten sind dabei grundsätzlich unmittelbar beim Betroffenen selbst zu erheben. Die Datenerhebung bei Dritten gemäß der Datenschutzrichtlinie bedarf einer gesetzlichen Erlaubnis.

21. Jeder Betroffene ist zumindest über die Identität der erhebenden METRO-Gesellschaft, den Verarbeitungszweck sowie weitere Empfänger seiner Daten und seine Rechte im Zusammenhang mit dieser Verarbeitung zu informieren. Im Geltungsbereich der DSGVO gelten besondere Anforderungen hinsichtlich der transparenten Information von Betroffenen, sie sich insbesondere aus den Art. 12 bis 14 DSGVO ergeben. Die Sicherstellung der Einhaltung der Informationspflichten obliegt dem Prozessverantwortlichen. Dieser kann bei Bedarf den Datenschutzkoordinator sowie den Datenschutzbeauftragten um Unterstützung bitten. Zudem wird vom Datenschutzbeauftragten ein Musterdokument für die Erteilung der Pflichtinformationen bereitgestellt, das Anweisungen dazu enthält, in welcher Form die Informationen zu erteilen sind.

22. Anfragen von Betroffenen hinsichtlich der ihnen zustehenden Rechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragung und Widerspruch) werden von METRO unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang der Anfrage, beantwortet.

23. Für den internen Umgang mit Betroffenenanfragen besteht ein Musterprozess der in einer im Intranet zur Verfügung gestellten Arbeitsanweisung sowie in einem Leitfaden (Datenübertragbarkeit) abgebildet ist, die im Einzelnen beschreiben, welche Schritte nach Eingang einer Anfrage bis zu ihrer Beantwortung zu berücksichtigen sind und welche Stellen im Unternehmen welche Teilschritte umzusetzen haben.

24. Bei der Beantwortung von Betroffenenanfragen ist sicherzustellen, dass die Identität des Betroffenen feststeht. METRO stellt den einzelnen Gesellschaften dazu ein Musterverfahren zur Identifizierung des Betroffenen zur Verfügung, das unter Berücksichtigung des nationalen Rechts einzusetzen ist.

25. Für die Beantwortung der Anfragen werden zudem Musterantworten im Intranet bereitgestellt, die der Antwort zugrunde gelegt werden sollen.

26. Die Verwendung personenbezogener Daten zur vollständig automatisierten Entscheidungsfindung (z.B. Scoring) ist nicht gestattet, es sei denn, es liegt ein gesetzlich definierter Ausnahmefall vor.

27. Der Umgang mit Betroffenenrechten sowie mit Informationspflichten unterliegt der ständigen Überprüfung durch den Datenschutzbeauftragten. Bei gesetzlichen Änderungen oder aufgrund Entscheidungen von Datenschutzbehörden und/oder Gerichten werden die Vorgaben bei Bedarf entsprechend angepasst.

Löschkonzept

28. Für jede Verarbeitungstätigkeit ist jeweils vor Inbetriebnahme durch den Prozessverantwortlichen ein Löschkonzept zu erstellen und anschließend zu implementieren.

29. Durch die Implementierung geeigneter Maßnahmen ist das Folgende sicherzustellen:

    - Dokumentation von Lösch- und Sperrfristen sowie Sperrungen im Verzeichnis der Verarbeitungstätigkeiten;

    - Regelung der Verantwortlichkeiten im Hinblick auf das Lösch- und Sperrkonzept;

    - Regelmäßige, mindestens jährliche, stichprobenhaften Überprüfung des Lösch- und Sperrkonzepts;

    - Protokollierung und Überwachung der Löschung/Sperrung.

30. Einzelheiten zur Organisation und Umsetzung eines Löschkonzeptes als wesentlicher Baustein des DMS sind in der Anlage 2 der Datenschutzrichtlinie verbindlich geregelt.

Notifikationsprozess, Datenschutzverletzungen und Hinweisgebersystem

31. Datenschutzverletzungen können zu einem Risiko für die Rechte und Freiheiten Betroffener führen und sind daher umgehend zu identifizieren, um schnelle Abhilfe sowie fristgerechte Meldung an Aufsichtsbehörden und Betroffene gemäß Art. 33 und 34 DSGVO zu ermöglichen.

32. Alle Mitarbeiter der METRO sind verpflichtet, Datenschutzverletzungen, sobald diese ihnen bekannt werden, zu melden, selbst wenn es sich hierbei nur um einen Verdacht einer Datenschutzverletzung handelt. Zu melden sind auch Datenschutzverletzungen, die den Mitarbeitern durch andere (Auftragsverarbeiter, Dritte) gemeldet werden. Hierauf werden alle Mitarbeiter in Schulungen sowie durch Flyer und Informationen im Intranet aufmerksam gemacht. Informationen zur Identifizierung eines Vorfalls sowie zu dessen Meldung stehen allen im Intranet zur Verfügung.

33. Eine Meldung kann per E-Mail an das Funktionspostfach des Datenschutzbeauftragten, telefonisch oder mündlich an diesen erfolgen. Mitarbeiter können Datenschutzverletzungen ebenso an Datenschutzkoordinatoren und Datenschutz-Manager melden. Diese sind verpflichtet, die Meldung unverzüglich an den zuständigen Datenschutzbeauftragten der betroffenen METRO-Gesellschaft(en) weiterzuleiten.

34. Auftragsverarbeiter sind vertraglich verpflichtet, Datenschutzverletzungen umgehend an den Datenschutzbeauftragten der betroffenen METRO-Gesellschaft zu melden. Alle Vereinbarungen zur Auftragsverarbeitung, die METRO abschließt, benennen das Funktionspostfach des zuständigen Datenschutzbeauftragten, an den die Meldung zu erfolgen hat.

35. Eine Meldung durch Dritte kann jederzeit über das Funktionspostfach des Datenschutzbeauftragten, das in allen Informationen für Betroffene gemäß Art. 13, 14 DSGVO zu benennen ist, erfolgen.

36. Zur Meldung von Datenschutzverletzungen stehen Mitarbeitern und Datenschutzbeauftragten der METRO Formulare zur Verfügung, die die Erfassung notwendiger Informationen zum Datenschutzvorfall erleichtern.

37. Dem Datenschutzbeauftragten obliegt es, alle Informationen zur Ermittlung der Datenschutzverletzung, des dadurch entstandenen Risikos für die Rechte und Freiheiten der Betroffenen sowie Bewertung getroffener und zu treffender risikominimierender Maßnahmen zusammenzutragen sowie eine Risikobewertung vorzunehmen.

38. Der Datenschutzbeauftragte hat die notwendigen Fachabteilungen bei der Ermittlung und Behebung des Datenschutzvorfalls einzubinden. Hierzu steht allen Datenschutzbeauftragten der METRO ein Strukturdiagramm zur Verfügung, das notwendige Schritte zur Einbindung der zuständigen Fachabteilungen erläutert.

39. Datenschutzverletzungen, die zu einem Risiko für die Rechte und Freiheiten Betroffener führen können, werden gemäß Art. 33 DSGVO innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde gemeldet. Die rechtzeitige Meldung obliegt dem Datenschutzbeauftragten der betroffenen METRO-Gesellschaft. Zur Sicherstellung der Fristwahrung ist dem Datenschutzbeauftragten Zugang auf das Funktionspostfach auch auf mobilen Geräten zu geben und bei Abwesenheit ein Stellvertreter zu benennen, dem Zugriff auf das Funktionspostfach (zumindest für die Dauer der Abwesenheit des Datenschutzbeauftragten) zu gewähren ist.

40. Datenschutzverletzungen, die zu einem hohen Risiko für die Rechte und Freiheiten Betroffener führen können, sind den Betroffenen gemäß Art. 34 DSGVO bekannt zu geben. Können nicht alle Betroffenen direkt benachrichtigt werden, ist die Abteilung Unternehmenskommunikation zwingend einzubinden, ebenso, wenn das Bekanntwerden der Datenschutzverletzung einen Reputationsschaden der METRO zur Folge hat oder haben könnte. Zur Benachrichtigung Betroffener kann der Datenschutzbeauftragte zur Verfügung gestellte Formulare und Musterbriefe verwenden.

41. Jeder Verdacht auf eine Datenschutzverletzung ist aufzunehmen und inklusive aller Kommunikation mit Meldenden, Fachabteilungen, Aufsichtsbehörden und Betroffenen zu dokumentieren. Ebenso sind alle geplanten und getroffenen Maßnahmen zur Eindämmung, Risikominimierung und Behebung des Datenschutzvorfalls durch den Datenschutzbeauftragten zu dokumentieren. Führen solche Maßnahmen zur Änderung technischer und/oder organisatorischer Maßnahmen, ist die entsprechende Dokumentation (siehe oben) anzupassen. Führen solche Maßnahmen zu einer Änderung im Verzeichnis von Verarbeitungstätigkeiten, ist dieses ebenfalls anzupassen. Die Anpassung wird durch den zuständigen Datenschutzbeauftragten überwacht.

42. Alle Fachabteilungen sind verpflichtet, zum Ende eines jeden Geschäftsjahres die Anzahl der sich in ihrer Abteilung ereigneten Datenschutzvorfälle dem zuständigen Datenschutzbeauftragten zu melden. Lagen keine Datenschutzvorfälle vor, ist eine Null-Meldung zu erstatten. Der zuständige Datenschutzbeauftragte ist verpflichtet, alle sich in dem Geschäftsjahr ereigneten Datenschutzvorfälle in seinem jährlichen Tätigkeitsbericht aufzuführen.

Auftragsverarbeiter und Umgang mit externen Dienstleistern

43. METRO schließt mit allen Auftragsverarbeitern entsprechende Vereinbarungen ab. Das DPD stellt Muster zur Verfügung, die von den Fachabteilungen in Absprache mit dem zuständigen Datenschutzbeauftragten zu nutzen sind. Abweichungen von Mindestinhalten des Art. 28 DSGVO sind nicht zulässig. Weitere Anforderungen gibt die Anlage 1 zur Allgemeinen Datenschutzrichtlinie der METRO vor. Die Überwachung des Abschlusses aller notwendigen Vereinbarung zur Auftragsverarbeitung mit entsprechenden Mindestinhalten obliegt dem zuständigen Datenschutzbeauftragten.

44. Auftragsverarbeiter, mit denen eine Vereinbarung geschlossen werden soll, müssen vor Vertragsabschluss eine aussagekräftige Auskunft über die von ihnen getroffenen dem Verarbeitungsrisiko angemessenen technischen und organisatorischen Maßnahmen zur Verfügung stellen. Dem zuständigen Datenschutzbeauftragten obliegt es die Angemessenheit dieser Maßnahmen zu prüfen. Hierzu kann er weitere Fachabteilungen einbinden und sich der vom DPD zur Verfügung gestellten Arbeitsanweisungen zur Überprüfung der Angemessenheit von technischen und organisatorischen Maßnahmen bedienen. Nach Freigabe der zu vereinbarenden und durch den Auftragsverarbeiter zugesicherten technischen und organisatorischen Maßnahmen durch den zuständigen Datenschutzbeauftragten werden bei METRO Vereinbarungen zur Auftragsverarbeitung geschlossen.

45. METRO-Gesellschaften überprüfen und inspizieren Auftragsverarbeiter, die in ihrem Auftrag personenbezogene Daten verarbeiten. Überprüfungen und Inspektionen erfolgen risikoorientiert und werden in Bezug auf Datenschutz durch den Datenschutzbeauftragten angeregt und begleitet.

46. Alle Vereinbarungen zur Auftragsverarbeitung der METRO-Gesellschaften sind so aufzubewahren, dass der Zugang zu ihnen jederzeit sichergestellt ist. Die Sicherstellung der Aufbewahrung obliegt der jeweiligen METRO-Gesellschaft. Dem Datenschutzbeauftragten der jeweiligen METRO-Gesellschaft sowie dem zuständigen

Datenschutz-Manager ist jederzeit Zugang zu und Zugriff auf die Vereinbarungen zu gewähren.

Drittstaatenübermittlung

47. METRO ist ein international tätiger Konzern mit Kunden und Partnern weltweit. METRO stellt sicher, dass personenbezogene Daten bei der Übermittlung zu anderen METRO-Gesellschaften im Ausland durch technische und organisatorische Maßnahmen vor Fremdzugriffen, Verlust und Veränderung geschützt sind. Alle METRO-Gesellschaften müssen ein angemessenes Datenschutzniveau garantieren und die Vorgaben der Datenschutzrichtlinie umsetzen.

48. Bei Übermittlung personenbezogener Daten an Dritte in Drittstaaten vergewissert sich METRO, dass ein angemessenes Datenschutzniveau im Empfängerstaat gegeben ist. Die Prüfung obliegt dem zuständigen Datenschutzbeauftragten. Sollte kein angemessenes Datenschutzniveau gemäß Art. 45 DSGVO gegeben sein, ist zu prüfen, ob geeignete Garantien mit dem Empfänger gemäß Art. 40, 42, 46, 47 DSGVO vorliegen oder zu treffen sind oder zu prüfen, ob ein Ausnahmefall gemäß Art. 49 DSGVO vorliegt.

49. Eine Überprüfung der Übertragung von personenbezogenen Daten in Drittstaaten erfolgt gemeinsam mit der Überprüfung des jeweiligen Verfahrens und des Verzeichnisses der Verarbeitungstätigkeiten wie oben beschrieben.

Kommunikation

Kommunikationsmaßnahmen zum Thema Datenschutz

1. METRO ist bestrebt, alle Mitarbeiter für den Datenschutz zu sensibilisieren. Hierfür sind sichere und erreichbare Kommunikationswege und -maßnahmen essentiell.

2. METRO stellt allen Mitarbeitern regelmäßig Informationen zum Umgang mit personenbezogenen Daten im Intranet, per E-Mail, Teams sowie in gedruckter Form zur Verfügung. So soll sichergestellt werden, dass alle Mitarbeiter jederzeit über die Möglichkeit verfügen, sich zum Thema Datenschutz zu informieren. Die Datenschutzrichtlinie inklusive aller Anhänge, Schulungsunterlagen, Muster, Flyer sowie Updates und Neuigkeiten, die alle Mitarbeiter der METRO betreffen, werden im Intranet kommuniziert und stehen dort dauerhaft allen Mitarbeitern zur Verfügung. Datenschutzbeauftragte der METRO-Gesellschaften sind angehalten, eigene Seiten im Intranet zu unterhalten, auf denen landesspezifische Informationen zum Datenschutz bekannt zu machen sind. Datenschutzbeauftragten der METRO-Gesellschaften steht es darüber hinaus frei, zusätzliche, den lokalen Gegebenheiten entsprechende Kommunikationsmittel zu nutzen, um Mitarbeiter der Gesellschaften für das Thema Datenschutz zu sensibilisieren.

3. METRO unterstützt den Austausch von Datenschutzbeauftragten und Datenschutzkoordinatoren im Konzern und stellt diesen neben den allgemein zugänglichen In-

formationen im Intranet zusätzliche Informationen in Microsoft Teams, inklusive einer dedizierten Plattform zum Austausch zur Verfügung.

4. Zur Sicherstellung der Erreichbarkeit aller Datenschutzbeauftragten, richten die METRO-Gesellschaften Funktionspostfächer ein und gewähren den Datenschutzbeauftragten und ihren Stellvertretern Zugriff darauf. Die Adresse des Funktionspostfachs ist in allen Datenschutzerklärungen der jeweiligen Gesellschaft zu veröffentlichen und allen Mitarbeitern bekannt zu machen.

5. Mitarbeiter können sich jederzeit persönlich, telefonisch oder per E-Mail an den Datenschutzbeauftragten wenden. Kunden steht zur Kontaktaufnahme der elektronische Weg über die Funktionsadresse, die telefonische Kontaktaufnahme oder der Postweg offen.

6. Vorgaben zum Datenschutz werden via Intranet verfügbar gemacht und per E-Mail verbreitet. Für die Kommunikation von Vorgaben stehen zahlreiche weitere Kommunikations-Tools zur Verfügung. E-Mail- und Dokumentvorlagen, Vertragsmuster, Checklisten und Broschüren zu den wichtigsten Datenschutzthemen werden zur Verfügung gestellt. Weiteres ergibt sich aus Schulungen, Schulungsunterlagen und individuellen Empfehlungen der Verantwortlichen.

Schulungskonzept

7. Alle Mitarbeiter sind zum allgemeinen Umgang mit personenbezogenen Daten zu schulen. Die Schulung von Mitarbeitern, Datenschutzkoordinatoren und Prozessverantwortlichen obliegt dem Datenschutzbeauftragten der jeweiligen METRO-Gesellschaft. Die Teilnahme an solchen allgemeinen Schulungen ist für alle Mitarbeiter verpflichtend. Dem Datenschutzbeauftragten obliegt es sicherzustellen, dass Mitarbeiter, die zur Teilnahme verpflichtet sind, an dieser teilnehmen. Der Datenschutzbeauftragte hat ausreichend Schulungstermine für Mitarbeiter anzubieten, um allen eine Teilnahme zu ermöglichen. Bei mehrfacher Nichtteilnahme von Mitarbeitern sind deren Vorgesetzte zu informieren. Eine dauerhafte Teilnahmeverweigerung kann arbeitsrechtliche Maßnahmen zur Folge haben. Allgemeine Schulungen sind alle zwei Jahre zu wiederholen.

8. METRO DPD stellt sowohl allgemeine als auch spezifische Schulungsinhalte zur Verfügung. Deren Vermittlung obliegt dem Datenschutzbeauftragten der jeweiligen METRO-Gesellschaft.

Berichterstattung

9. Datenschutzbeauftragte sind verpflichtet, jährlich nach Abschluss des Geschäftsjahres über ihre Tätigkeit und den Stand der Umsetzung des Datenschutzes in ihrer Gesellschaft an ihre Gesellschaft und an den für sie zuständigen Datenschutz-Manager Bericht zu erstatten.

10. Der zuständige Datenschutz-Manager hat jährlich nach Abschluss des Geschäftsjahres über seine Tätigkeit und den Stand der Umsetzung des Datenschutzes in allen Gesellschaften, für die sie/er zuständig ist an den Vorstand der METRO AG zu berichten.

11. Daneben müssen Datenschutzbeauftragte die Geschäftsführungen der METRO-Gesellschaften, in denen sie benannt sind, regelmäßig sowie anlassbezogen über Risiken und den Umsetzungsstand informieren und beraten.

Überwachung und Verbesserung

Monitoring und Überwachungskonzept

1. Die Überwachung des Datenschutzes obliegt der Konzernleitung und der Geschäftsführung der jeweiligen METRO-Gesellschaft. Diese können diese Pflichten an Datenschutz-Manager und Datenschutzbeauftragte delegieren, bleiben aber für die Überwachung und Kontrolle der delegierten Tätigkeiten gemäß Anhang 2 der Datenschutzrichtlinie verantwortlich.

2. Die Überwachung der Tätigkeiten der Datenschutzbeauftragten erfolgt durch den jeweils zuständigen Datenschutz-Manager. Hierzu kann der Datenschutz-Manager Datenschutzbeauftragte anweisen, regelmäßig zum Umsetzungsstand der anwendbaren Datenschutzvorschriften Bericht zu erstatten. Hierbei trägt der zuständige Datenschutz-Manager dem Risiko eines Schadens durch mangelnde Umsetzung der anwendbaren Datenschutzvorschriften durch die betroffenen METRO-Gesellschaften Rechnung.

3. Der Datenschutzbeauftragte überwacht die Einhaltung der anwendbaren Datenschutzbestimmungen durch die benennende METRO-Gesellschaft. Der Datenschutzbeauftragte führt zu diesem Zweck unter anderem und je nach Bedarf periodische Effizienzprüfungen und/oder Stichprobenkontrollen der implementierten technischen und organisatorischen Maßnahmen und des zugrundeliegenden Konzepts, der Aufzeichnung der Verarbeitungstätigkeiten, etwaiger Verträge mit Auftragsverarbeitern und gegebenenfalls weitere relevante Dokumente durch. Bei Bedarf kann der Datenschutzbeauftragte den zuständigen Datenschutz-Manager in die Prüfung einbinden. Über das Ergebnis der Prüfung erstattet der Datenschutzbeauftragte Bericht wie im Abschnitt zur Berichterstattung vorgesehen.

4. Unabhängige Audits der Internen Revision oder durch Prüfungsgesellschaften stellen eine unabhängige Überprüfung der Tätigkeiten des Datenschutzbeauftragten und des Datenschutz-Managers sicher.

5. Haben Audits der Internen Revision nicht die Überprüfung des gesamten DMS zum Ziel, sondern fokussieren sie sich auf andere Tätigkeiten der Gesellschaft, aber berühren auch anwendbare Datenschutzvorschriften, ist der Datenschutzbeauftragte und der zuständige Datenschutz-Manager in die Planung, Vorbereitung und Durchführung des Audits einzubinden. Die Auswahl der zu auditierenden Bereiche obliegt der Internen Revision. Der Bericht ist nach Abschluss des Audits auch dem Datenschutzbeauftragten und dem zuständigen Datenschutz-Manager zur Kenntnis zu geben. Die Überwachung der Umsetzung der empfohlenen Maßnahmen obliegt dem Datenschutzbeauftragten.

6. Erkenntnisse aus Audits und regelmäßigen Überprüfungen durch Datenschutz-Manager und Datenschutzbeauftragten werden zur Anpassung und Verbesserung des DMS genutzt.

Weiterentwicklung des DMS und Analyse von Verbesserungspotentialen

7. Im Rahmen des periodisch-zyklischen Optimierungsprozesses (Plan-Do-Check-Act) für das Datenschutz-Management wird das Datenschutz-Regelwerk an rechtliche, organisatorische und technische Änderungen fortlaufend angepasst.

8. Erkenntnisse aus der erforderlichen Dokumentation für einen Prozess, der damit zusammenhängenden Risikoanalyse, Datenschutzverletzungen, aktuellen Fortbildungen, Veröffentlichungen und sonstigen Quellen werden genutzt, um Folgemaßnahmen zu definieren. Folgemaßnahmen dienen der Verbesserung im Hinblick auf den Datenschutz und können Schulungen, Arbeitsunterlagen, neue zu implementierende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten oder eine Änderung des Datenschutz-Regelwerks umfassen. Sie werden von den Datenschutz-Managern oder den Datenschutzbeauftragten unmittelbar an die jeweiligen Verantwortlichen gerichtet (siehe Aufbau- und Ablauforganisation) und entsprechend überwacht.

9. Die Geschäftsführungen sind in den Prozess zur Überwachung und Verbesserung eingebunden. Die von den jeweils Verantwortlichen definierten Maßnahmen können auch unmittelbar an die Geschäftsführung gerichtet werden. Insofern können die Geschäftsführungen auch selbst Adressat der Maßnahmen sein. Darüber hinaus werden Missstände und nötige Verbesserungen im mindestens jährlichen Report an die Geschäftsführung ausgewiesen.

Düsseldorf, 30. April 2020

* *