Technische und organisatorische Maßnahmen

Es ist die Vision von NTT, **durch Technologie und Innovation eine sichere und miteinander verbundene Zukunft** zu ermöglichen. Wir haben technische und organisatorische Maßnahmen (TOM) getroffen, die sicherstellen, dass die Verarbeitung von personenbezogenen Daten durch NTT in einer transparenten, fairen, ethischen und rechtmäßigen Weise erfolgt.

Unsere TOM basieren zum einen auf den höchsten Standards im Markt, auf den jeweiligen rechtlichen Anforderungen in den Ländern, in denen NTT operativ tätig ist und schließlich berücksichtigen sie die jeweiligen zu verarbeitenden Daten in angemessener, effizienter Art und Weise.

Inhaltsverzeichnis

(A) Data Privacy and Protection Measures

1 Corporate Governance und Business-Modell

1.1 Um der Verantwortung und den gesetzlichen Vorschriften bei der Verarbeitung personenbezogener Daten zu entsprechen, hat NTT eine Organisationsstruktur implementiert, die alle Rollen und Verantwortlichkeiten bei der Verarbeitung von personenbezogenen Daten berücksichtigt.

1.2 Um sicherzustellen, dass etwaige Verstöße gegen das Datenschutzrecht, bzw. im Hinblick auf die Datensicherheit durch das zuständige Management innerhalb von NTT unverzüglich überprüft werden, wurde eine Governance-Struktur implementiert. Die oberste Verantwortung für den Datenschutz und die Datensicherheit liegt beim Vorstand bzw. der Geschäftsführung der jeweiligen NTT Gesellschaft, der durch dedizierte Rollen im gesamten Unternehmen, insbesondere bestellte Datenschutzbeauftragte oder gleichwertiger Rollen unterstützt wird, wo dies gemäß den Datenschutzgesetzen erforderlich ist.

2 Anweisungen, Prozesse und Richtlinien

2.1 Richtlinien, Prozesse, Standards und Leitlinien die detailliert beschrieben, wie NTT Mitarbeiter personenbezogene Daten verarbeiten, wurden implementiert und kommuniziert. Dazu gehören folgende Richtlinien:

2.1.1 Datenschutz- und IT-Sicherheitsrichtlinie

2.1.2 Richtlinie zu den Rechten der Betroffenen; und

2.1.3 Richtlinie über die Benachrichtigung Betroffener und Behörden.

2.2 2NTT hat Datenschutzerklärungen definiert und kommuniziert, in denen Mitarbeiter, Kunden und andere Beteiligte darüber informiert und angeleitet werden, wie personenbezogene Daten zu verarbeiten sind.

2.3 NTT wird bei Vorliegen der Voraussetzungen entsprechende Datenschutz-Folgenabschätzungen ("DPIA") durchführen.

3 Datenschutz durch Design

NTT verpflichtet sich, angemessene Maßnahmen zu ergreifen, ihre Kunden bei der Einhaltung der Datenschutzgesetze zu unterstützen. Soweit möglich, werden bei der Entwicklung und Bereitstellung von NTT-Produkten, Dienstleistungen und Lösungen die Grundsätze des Datenschutzes durch Design, also Gestaltung der Lösung und durch entsprechende Voreinstellungen, etwa zur Erfüllung des Grundsatzes der Datensparsamkeit, angewendet.

4 Verfahrensverzeichnisse

4.1 NTT hat Prozesse implementiert, um die persönlichen Daten zu identifizieren, zu erfassen, zu bewerten und zu sichern, die NTT verarbeitet.

4.2 NTT führt Verfahrensverzeichnisse über die verarbeiteten personenbezogenen Daten bzw. Verarbeitungsprozesse in Übereinstimmung mit den geltenden Datenschutzgesetzen.

5 Information Lifecycle Management

5.1 Um sicherzustellen, dass die Verarbeitung (Erfassung, Nutzung, Aufbewahrung, Offenlegung, Vernichtung) von personenbezogenen Daten durchgehend den gesetzlichen Anforderungen entspricht, hat NTT Richtlinien und Prozesse implementiert.

5.2 Die anwendbaren Datenschutzgesetze gewähren den Betroffenen eine Vielzahl von Rechten in Bezug auf ihre persönlichen Daten. NTT wird diese Rechte wahren und stellt sicher, dass Anfragen von Betroffenen in einer transparenten, fairen, ethischen und gesetzeskonforme Weise beantwortet werden.

5.3 Um die Rechte der Betroffenen in Übereinstimmung mit den geltenden gesetzlichen Bestimmungen zu wahren, hat NTT sowohl eine Richtlinie als auch einen Prozess für Informationspflichten des Verantwortlichen und Auskunftsrechte der Betroffenen implementiert.

5.4 NTT dokumentiert eingehende Auskunfts- oder Löschgesuche von Betroffenen und beantwortet diese innerhalb der gesetzlich vorgeschrieben Fristen.

5.5 NTT hat eine Richtlinie zur Datenaufbewahrung implementiert, die sich an den jeweils anwendbaren Gesetzen orientiert, was z.B. Aufbewahrungspflichten angeht. Personenbezogene Daten werden nur dann erhoben, wenn es dafür eine gesetzliche Grundlage gibt. NTT vernichtet bzw. anonymisiert personenbezogene Daten, soweit keine gesetzliche Grundlage mehr besteht, diese Daten länger zu verarbeiten.

5.6 NTT bewahrt die im Auftrag seiner Kunden zu verarbeitenden personenbezogenen Daten in Übereinstimmung mit den gesetzlichen Bestimmungen und den Anforderungen des Kunden auf. Auf Verlangen des Kunden werden die Daten durch NTT ver-

nichtet, gelöscht, pseudonymisiert oder an den Kunden zurückgegeben, soweit keine gesetzlichen Verpflichtungen zur Aufbewahrung dieser personenbezogenen Daten entgegenstehen.

5.7 NTT ergreift alle angemessenen Maßnahmen um sicherstellen, dass personenbezogene Daten richtig, vollständig und aktuell sind.

5.8 NTT verwendet bei der Unterverarbeitung von personenbezogenen Daten durch Konzerngesellschaften und andere Dritte EU-Standardvertragsklauseln und zusätzliche Garantien nach Schrems II, um die rechtmäßige Verarbeitung personenbezogener Daten außerhalb der EU bzw. in Ländern ohne entsprechendes Schutzniveau sicherzustellen.

6 Schulungen zum Datenschutz und zur Datensicherheit

NTT schult in regelmäßigen Abständen ihre Mitarbeiter, insbesondere zu Themen des Datenschutzes und der Datensicherheit. Alle Datenschutz- und Datensicherheitsrichtlinien, -prozesse, -standards und -richtlinien sind den Mitarbeitern zugänglich und werden regelmäßig kommuniziert. Bei Bedarf werden auch spezifische Schulungen durchgeführt, um die Mitarbeiter dabei zu unterstützen, im Einklang mit den Datenschutzanforderungen in bestimmten Ländern, Regionen oder Geschäftsfunktionen zu handeln.

7 Informationssicherheit und Datenschutz

7.1 Die Datenschutz- und Informationssicherheitsteams von NTT arbeiten zusammen, um sicherzustellen, dass ein angemessenes Datenschutz-Niveau und entsprechende Kontrollsysteme implementiert werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten zu schützen.

Die Sicherheitsmaßnahmen von NTT sind an ISO27001 und dem NIST Cyber Security Framework ("CSF") ausgerichtet.

8 Maßnahmen bei Verstößen und Meldungen

8.1 NTT verfügt über Richtlinien, Prozesse und Verfahren zur Identifizierung, Erkennung, Reaktion, Wiederherstellung von Daten und für die Benachrichtigung der entsprechenden Betroffenen für den Fall einer Verletzung des Schutzes personenbezogener Daten. Dies beinhaltet die Durchführung einer Ursachenanalyse und von Korrekturmaßnahmen.

8.2 NTT stellt sicher, dass im Falle der Verletzung des Schutzes von personenbezogen Daten die zuständigen Datenschutzbehörden, die betroffenen Kunden und Personen in Übereinstimmung mit den geltenden Datenschutzgesetzen und den vertraglichen Verpflichtungen benachrichtigt werden.

8.3 NTT dokumentiert alle Verletzungen des Schutzes personenbezogener Daten und die Maßnahmen, die als Reaktion auf diese Ereignisse ergriffen worden sind.

8.4 Die Maßnahmen von NTT für das Incident-Management zur Identifizierung, Erkennung, Reaktion und Wiederherstellung nach möglichen Verstößen oder Vorfällen sind in Abschnitt B (Informationssicherheit) dieser TOMs beschrieben.

Zusammenarbeit mit Dritten

8.5 NTT ist für die Handlungen seiner Auftragsverarbeiter (d.h. Unterauftragsverarbeiter), die personenbezogene Daten im Auftrag von NTT verarbeiten, nach Maßgabe der gesetzlichen Bestimmungen verantwortlich. NTT bewertet und auditiert ihre Auftragsverarbeiter zum Zeitpunkt der Auswahl und danach in regelmäßigen Abständen.

8.6 Auftragsverarbeiter der NTT sind verpflichtet, entsprechende Vereinbarungen zu unterzeichnen, die die Unterverarbeitung, den Schutz personenbezogener Daten und die Verpflichtung regelt, dass auch Unterauftragnehmer denselben Verpflichtungen unterliegen, die NTT ihrerseits gegenüber ihren Kunden eingegangen ist. NTT wird mit ihren Auftragsverarbeitern entsprechende Datenverarbeitungsverträge abschließen.

9 Zusammenarbeit mit Dritten

9.1 NTT ist für die Handlungen seiner Auftragsverarbeiter (d.h. Unterauftragsverarbeiter), die personenbezogene Daten im Auftrag von NTT verarbeiten, nach Maßgabe der gesetzlichen Bestimmungen verantwortlich. NTT bewertet und auditiert ihre Auftragsverarbeiter zum Zeitpunkt der Auswahl und danach in regelmäßigen Abständen.

9.2 Auftragsverarbeiter der NTT sind verpflichtet, entsprechende Vereinbarungen zu unterzeichnen, die die Unterverarbeitung, den Schutz personenbezogener Daten und die Verpflichtung regelt, dass auch Unterauftragnehmer denselben Verpflichtungen unterliegen, die NTT ihrerseits gegenüber ihren Kunden eingegangen ist. NTT wird mit ihren Auftragsverarbeitern entsprechende Datenverar-

beitungsverträge abschließen.

10 Audits und Scoring

Die jeweiligen NTT-Gesellschaften berichten dem NTT Ltd. Audit and Risk Committee, sowie deren Geschäftsführung über die Gestaltung und operative Effektivität ihrer Datenschutzaktivitäten in regelmäßigen Abständen. Dies umfasst die Berichterstattung z.B. in Form des jährlichen Datenschutzberichtes, Selbsteinschätzungen des Managements, Zertifizierungen, Überprüfungen durch die interne Revision, sowie unabhängige Audits und Bewertungen.

(B) Maßnahmen zur Informationssicherheit

NTT hat sich verpflichtet, ein Informationssicherheitsmanagement zu implementieren und ordnungsgemäß zu verwalten, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten zu schützen, die im Namen und auf Anweisung ihrer Kunden verarbeitet werden. NTT hat ein konzernweites Informationssicherheits-Managementsystem ("ISMS") eingerichtet, das sich an führenden Informationssicherheitspraktiken und -standards aus der ganzen Welt orientiert, darunter die ISO27000-Serie und NIST Cyber Security Framework ("CSF").

11 Informationssicherheit

11.1 Die Rollen, Verantwortlichkeiten und Berichtslinien für die Informationssicherheit wurden innerhalb der NTT-Gesellschaften formell zugewiesen, um die Unabhängigkeit der jeweiligen Funktion gewährleisten. Dies beinhaltet insbesonere die Benennung eines Chief Security Officer ("CSO"), Chief Information Security Officers ("CISO") und Information Security Officers ("ISO").

11.2 NTT-Mitarbeiter sind dafür verantwortlich, dass sie in Übereinstimmung mit den Richtlinien, Prozessen, Standards und Leitlinien zur Informationssicherheit handeln.

11.3 NTT hat Richtlinien zur Informationssicherheit dokumentiert und veröffentlicht, die die Anforderungen des ISMS regeln. Diese Richtlinien und unterstützende Dokumentation werden regelmäßig überprüft.

11.4 NTT hat Maßnahmen ergriffen, um sicherzustellen, dass mobile Geräte (einschließlich Laptops, Mobiltelefone, Tablets, Geräte mit Fernzugriff und "Bring Your Own Device"-Programme) sowie deren Inhalte geschützt sind. NTT hat angemessene Maßnahmen unternommen, um sicherzustellen, dass die Software für die Verwaltung mobiler Geräte ("MDM") auf allen mobilen Geräten mit Zugriff auf das NTT-Unternehmensnetzwerk installiert ist.

11.5 Telearbeit ist über die NTT-Infrastruktur nur dann möglich, soweit ein Virtual Private Network ("VPN")-Dienste eingesetzt wird und die Sicherheit und Vertraulichkeit von Daten und Informationen dabei sichergestellt ist.

12 Personalwesen

12.1 NTT führt Hintergrundchecks und Beschäftigungsprüfungen durch, soweit dies nach geltendem Recht zulässig und nach Kundenvorgaben im Einzelfall erforderlich ist, um die Eignung für die Einstellung bzw. für den konkreten Einsatz und den Umgang mit Unternehmens- und Kundendaten sicherzustellen.

12.2 NTT verpflichtet seine Mitarbeiter, aber auch jene von Subunternehmern, Zeitarbeitskräften und sonstigen Dritten, die NTT zur Vertragserfüllung einsetzt, die Vertraulichkeit von vertraulichen Informationen und personenbezogenen Daten zu wahren.

12.3 NTT-Mitarbeiter müssen regelmäßig eine Schulung zur Informationssicherheit absolvieren. Informationssicherheitsrichtlinien und unterstützende Verfahren, Prozesse und Richtlinien werden den Mitarbeitern zur Verfügung gestellt. Über die NTT Kommunikationsplattform erhalten Mitarbeiter relevante Informationen über Trends, Bedrohungen und Best Practices.

13 Zugriffskontrollen

13.1 NTT hat eine Richtlinie zur ordnungsgemäßen und effektiven Nutzung und den Schutz von NTT-Unternehmensressourcen, einschließlich Computer- und Telekommunikationsressourcen, Produkten, Dienstleistungen, Lösungen und IT-Infrastruktur erlassen.

13.2 NTT hat eine Richtlinie zur Informationsklassifizierung erlassen, die die entsprechenden technischen und organisatorischen Kontrollen für den Umgang mit Informationen auf der Grundlage ihrer Klassifizierung beschreibt. Informationen und Vermögenswerte werden stets entsprechend der Klassifizierungskennzeichnung geschützt.

14 Verwaltung von Zugriffsrechten

14.1 NTT verfügt über eine Richtlinie zur Zugriffskontrolle, unterstützende Verfahren sowie logische und physische Zugriffsmaßnahmen, um sicherzustellen, dass nur autorisierte Personen auf der Grundlage des Prinzips der geringsten

Privilegien Zugang zu Informationen haben.

14.2 Zugriffsüberprüfungen werden regelmäßig für IT-Assets, Anwendungen, Systeme und Datenbanken durchgeführt, um sicherzustellen, dass nur autorisierte Personen Zugriff haben.

14.3 NTT-Prozessoren (d.h. Sub-Prozessoren) müssen über benannte Accounts auf NTT-Systeme zugreifen. Generische Konten und/oder die gemeinsame Nutzung von Anmeldeinformationen sind verboten, es sei denn, eine Ausnahme wurde ausdrücklich von der Geschäftsleitung oder den Kunden genehmigt.

14.4 NTT hat angemessene Anstrengungen unternommen, um die Anzahl der privilegierten ("Admin") Benutzer auf seinen Anwendungen, Systemen und Datenbanken streng zu begrenzen.

15 Zugangskontrollen

NTT hat angemessene und geeignete Maßnahmen in Übereinstimmung mit der Richtlinie zur physischen Sicherheit umgesetzt, um Unbefugten physischen Zugriff, Beschädigung oder Störung von NTT-Informationen oder Anwendungen, Systemen, Datenbanken und Infrastrukturen in den folgenden Bereichen zu verwehren:

15.1 Physische Zugangskontrollen

15.2 Überwachung und Auditierung des physischen Zugangs

15.3 Schutz vor Umweltgefahren

15.4 Sichern von Sachwerten

15.5 Verkabelungssicherheit

15.6 Umgang mit physischen und informativen Assets

15.7 Wartung und Entsorgung von Sachanlagen

15.8 "Clean Desktop" Policy und Vorschriften, den Arbeitsplatz beim Verlassen zu sichern (Bildschirm sperren, Schränke verschließen)

15.9 Zugangskontrolle für und Überwachung von Besuchern, z.B. Aufenthalt nur in Begleitung von NTT-Mitarbeitern.

16 Operative Sicherheit

16.1 Die Funktion NTT Information and Technology ("I&T") ist verantwortlich für das Management von NTT-Anwendungen, Systemen, Datenbanken und Infrastruktur. I&T dokumentiert, pflegt und implementiert alle IT-Betriebsrichtlinien und -verfahren, die sich an COBIT- und ITIL-Standards orientieren.

16.2 NTT hat eine Richtlinie und unterstützende Verfahren für die Behandlung von Änderungen an seinen Geschäftsprozessen, Anwendungen und Systemen, Datenbanken und Infrastruktur implementiert. NTT hat Governance-Strukturen eingerichtet, um alle Änderungen nach Reichweite und Umfang der Änderung zu überprüfen und zu genehmigen. Alle Anfragen und deren Ergebnisse werden protokolliert und dokumentiert.

16.3 NTT hat ein Bedrohungs- und Schwachstellenmanagement-Programm eingerichtet, das anerkannten Regeln der Technik entspricht und Standardwerkzeuge zur Identifizierung, Verwaltung und Minderung von Risiken für Unternehmensinformationen, einschließlich der persönlichen Daten von Mitarbeitern und Kunden implementiert. Dazu gehört die jeweils aktuellste Generation von Endpoint Detection and Response ("EDR") für Anti-Viren- und Anti-Malware-Tools, regelmäßiges Scannen von Umgebungen, Patching-Protokolle und Verwaltung von Behebungs- und Verbesserungsmaßnahmen.

16.4 Der Kapazitätsbedarf wird kontinuierlich überwacht und regelmäßig überprüft. Systeme und Netzwerke werden im Einklang mit diesen Überprüfungen verwaltet und skaliert.

16.5 Die Systemverfügbarkeit umfasst Architektur, Hochverfügbarkeitsdesign und Back-Ups, die auf den Risiko- und Verfügbarkeitsanforderungen für jedes System basieren. Die Methode zur Aufrechterhaltung der Systemverfügbarkeit oder Wiederherstellung, einschließlich des Umfangs und der Häufigkeit der Back-Ups wird auf der Grundlage der Geschäftsanforderungen von NTT, einschließlich der Kundenanforderungen und der Kritikalität der Informationen festgelegt. Die Überwachung von Back-Ups wird durchgeführt, um den erfolgreichen Abschluss zu gewährleisten, da sowie die Verwaltung von Problemen und Ausnahmen oder Fehlern bei der Datensicherung.

16.6 NTT unternimmt angemessene Maßnahmen, um eine Audit-Protokollierung für Anwendungen und Systeme zu erstellen. Protokolle werden regelmäßig überprüft und sind für Unternehmenszwecke verfügbar. Der Zugriff auf die Protokolle ist streng auf autorisiertes Personal beschränkt.

17 Systembeschaffung, Entwicklung und Wartung

17.1 NTT hat eine Sicherheitsarchitektur- und Designrichtlinie, sowie unterstützende Standards und Verfahren implementiert um sicherzustellen, dass die „Security by Design" - Prinzipien bereits bei der Entwicklung von Lösungen und Software angewendet werden.

17.2 NTT erlaubt keine Verwendung von Produktions-, Kun-

den-, persönlichen Daten oder anderen vertraulichen Informationen zu Testzwecken. In Ausnahmefällen dürfen Produktions- oder Kundendaten mit Genehmigung des jeweiligen Kunden, bzw. Geschäftsinhabers verwendet werden.

18 Zusammenarbeit mit Drittanbietern

18.1 NTT verfügt über eine Sicherheitsrichtlinie und unterstützende Verfahren für die Zusammenarbeit mit Drittanietern um sicherzustellen, dass Informationen geschützt werden. Dies beinhaltet Anforderungen an die Sorgfaltspflicht für die Informationssicherheit durchzuführende Risikobeurteilungen um sicherzustellen, dass:

18.1.1 Die Anforderungen an die Informationssicherheit in den Vereinbarungen sind klar formuliert sind;

18.1.2 NTT-Drittanbieter das gleiche Maß an Schutz und Kontrolle wie NTT gewährleisten;

18.1.3 Auftragsverarbeiter verpflichtet werden, alle vermuteten oder tatsächlichen Vorfälle im Bereich der Informationssicherheit zeitnah an NTT zu melden.

18.2 NTT hat angemessene Vorkehrungen unternommen, um sicherzustellen, dass Vereinbarungen mit Auftragsverarbeitern bestehen, die Zugang zu Datenbanken, Infrastruktur, Informationen, Anwendungen und Systemen von NTT haben. Diese Vereinbarungen beinhalten NTT-Informationssicherheitsstandards zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von NTT-Informationen.

19 Management von Informationssicherheitsvorfällen

19.1 NTT hat Richtlinien, Prozesse und Verfahren zur Identifizierung, Erkennung, Reaktion und Wiederherstellung von möglichen Sichterheitsvorfällen, sogenannte „Incidents“, etabliert um die Benachrichtigung der entsprechenden Beteiligten im Falle eines Informationssicherheitsvorfalls, einschließlich persönlicher Datenverletzungen zu informieren. Dies beinhaltet Mechanismen zur Durchführung einer Ursachenanalyse und die Durchführung von Abhilfemaßnahmen.

19.2 NTT hat konzernweite Maßnahmen zur proaktiven Überwachung und Verwaltung aller Netzwerk- und Computeranlagen etabliert. Dies wird durch technische Tools für Reaktion auf Informationssicherheitsvorfälle und Wiederherstellung sichergestellt.

20 Geschäftskontinuität

NTT hat Maßnahmen ergriffen, um Business-Continuity- und Disaster-Recovery-sicher zu stellen. NTT hat einen mehrstufigen Ansatz gewählt, um die Verfügbarkeit ihrer Systeme und Daten sicherzustellen.

21 Compliance

21.1 NTT hat Funktionen und Verantwortlichkeiten für die rechtzeitige Erkennung von neuen Gesetzen und Vorschriften bzw. derer Änderungen festgelegt, die sich auf Geschäftsbetrieb von NTT und ihrer Kunden auswirken. Verantwortlichkeiten für die Einhaltung von Gesetzen und Vorschriften sind auf Konzern- und Regionalebene festgelegt, um sicherzustellen, dass NTT die globalen und lokalen Anforderungen erfüllt.

21.2 NTT verfolgt einen einheitlichen Ansatz für die Informationssicherheit in allen Geschäftsbereichen. NTT-Produkte, -Dienstleistungen und -Lösungen sind auf den ISO 27001-Standard ausgerichtet und werden, sofern sie gemäß der Kundenvereinbarung zertifiziert sind, jährlich gemäß diesem Standard auditiert.

22 Compliance

22.1 NTT hat Funktionen und Verantwortlichkeiten für die rechtzeitige Erkennung von neuen Gesetzen und Vorschriften bzw. derer Änderungen festgelegt, die sich auf Geschäftsbetrieb von NTT und ihrer Kunden auswirken. Verantwortlichkeiten für die Einhaltung von Gesetzen und Vorschriften sind auf Konzern- und Regionalebene festgelegt, um sicherzustellen, dass NTT die globalen und lokalen Anforderungen erfüllt.

22.2 NTT verfolgt einen einheitlichen Ansatz für die Informationssicherheit in allen Geschäftsbereichen. NTT-Produkte, -Dienstleistungen und -Lösungen sind auf den ISO 27001-Standard ausgerichtet und werden, sofern sie gemäß der Kundenvereinbarung zertifiziert sind, jährlich gemäß diesem Standard auditiert.

Bei Fragen wenden Sie sich bitte an das Privacy Office unter **privacyoffice@global.ntt**

Together we do great things