

Technische und organisatorische Maßnahmen

Datenschutz

Inhaltsverzeichnis

1.	**Einleitung**	**3**
2.	**Datenschutzmaßnahmen**	**4**
2.1.	Governance- und Betriebsmodell	4
2.2.	Richtlinien, Prozesse und Vorgaben	4
2.3.	Datenschutz durch Technikgestaltung	4
2.4.	Datenlandschaft	4
2.5.	Information Lifecycle Management	4
2.6.	Rechte der betroffenen Person	5
2.7.	Grenzüberschreitende Datenübermittlung	5
2.8.	Regulatorische Überwachung	5
2.9.	Schulung und Sensibilisierung	5
2.10.	Sicherheit für den Datenschutz	6
2.11.	Reaktion auf Datenschutzverletzungen und Benachrichtigung	6
2.12.	Third Party Management	6
3.	**Maßnahmen zur Informationssicherheit**	**7**
3.1.	Rollen und Zuständigkeiten im Bereich der Informationssicherheit	7
3.2.	Richtlinien zur Informationssicherheit	7
3.3.	Mobile device management	7
3.4.	Human resources	7
3.5.	Akzeptable Nutzung	7
3.6.	Zugriffskontrollen	8
3.7.	Asset Management und Klassifizierung	8
3.8.	Physische und umweltbezogene Sicherheit	8
3.9.	Betriebssicherheit	9
3.10.	Beschaffung, Entwicklung und Wartung von Systemen	9
3.11.	Third Party Management	9
3.12.	Management von Vorfällen im Bereich der Informationssicherheit	9
3.13.	Business continuity	9
3.14.	Compliance	9

Einleitung

Von strategischer Beratung bis hin zu Spitzentechnologien unterstützt NTT DATA, um Unternehmen zum Erfolg zu führen, Branchen nachhaltig zu verändern und eine bessere Gesellschaft für alle zu gestalten.

Unsere technischen und organisatorischen Maßnahmen beschreiben, wie wir den Schutz personenbezogener Daten auf transparente, faire, ethische und rechtmäßige Weise gewährleisten. Sie basieren auf den Best Practices der Branche und den geltenden gesetzlichen Anforderungen in den Rechtsordnungen, in denen wir tätig sind. Dies unter Berücksichtigung der Art der von uns verarbeiteten Daten und der Implementierungskosten.

Wenn Sie Fragen zu diesen technischen und organisatorischen Maßnahmen oder im Zusammenhang mit unseren Produkten, Dienstleistungen und Lösungen haben, wenden Sie sich bitte an Ihren Servicemitarbeiter.



Unsere technischen und organisatorischen Maßnahmen beschreiben, wie wir den Schutz personenbezogener Daten auf transparente, faire, ethische und rechtmäßige Weise gewährleisten.

Datenschutzmaßnahmen

2.1. Governance- und Betriebsmodell

NTT DATA trifft im Rahmen der Verarbeitung personenbezogener Daten eine Verantwortung. Wir verfügen über die entsprechenden Organisationsstrukturen, Rollen und Verantwortlichkeiten für die Verwaltung und Überwachung der Verarbeitung personenbezogener Daten.

In jeder Jurisdiktion, in der wir tätig sind, sind Organisationseinheiten verpflichtet, angemessene Ressourcen bereitzustellen, um die geltenden Datenschutzgesetze einzuhalten. Dazu gehört die Ernennung qualifizierter Datenschutzressourcen, die die Einhaltung der Vorschriften überwachen, sowie die Einrichtung geeigneter Berichtsstrukturen.

NTT DATA berichtet der Geschäftsleitung regelmäßig über die Gestaltung und betriebliche Wirksamkeit von Datenschutzaktivitäten.

2.2. Richtlinien, Prozesse und Vorgaben

NTT DATA hat Richtlinien, Prozesse, Standards und Vorgaben implementiert und kommuniziert, die detailliert beschreiben, was Mitarbeiter von NTT DATA im Rahmen der Verarbeitung personenbezogener Daten zu beachten haben.

NTT DATA hat Datenschutzhinweise definiert und kommuniziert, die Mitarbeiter, Kunden und andere Interessengruppen darüber informieren, wie personenbezogene Daten verarbeitet werden.

NTT DATA hat in Übereinstimmung mit den geltenden Datenschutzgesetzen Prozesse und Vorlagen für die Durchführung von Risikobewertungen implementiert, einschließlich von Datenschutz-Folgenabschätzungen (DSFA), Bewertungen berechtigter Interessen (LIA) sowie von Bewertungen im Rahmen von Datenübertragungen (Transfer Impact Assessments).

2.3. Datenschutz durch Technikgestaltung

NTT DATA verpflichtet sich, angemessene Maßnahmen zu ergreifen, um die Kunden bei der Einhaltung der Datenschutzgesetze zu unterstützen. Soweit möglich, werden bei der Entwicklung von Produkten, Dienstleistungen und Lösungen von NTT DATA die Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen angewendet.

2.4. Datenlandschaft

NTT DATA hat Prozesse implementiert, um die von ihr verarbeiteten personenbezogenen Daten zu identifizieren, aufzuzeichnen, zu bewerten und zu verstehen.

NTT DATA führt Aufzeichnungen über die verarbeiteten personenbezogenen Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen.

2.5. Information Lifecycle Management

NTT DATA hat Richtlinien und Prozesse implementiert, um sicherzustellen, dass personenbezogene Daten über ihren gesamten Lebenszyklus hinweg angemessen verarbeitet werden (von der Erhebung über die Nutzung, Aufbewahrung, Offenlegung bis hin zur Vernichtung).

NTT DATA hat Richtlinien und Zeitpläne zur Datenaufbewahrung erstellt, die sich an den geltenden Gesetzen orientieren. NTT DATA speichert personenbezogene Daten nur, wenn es einen legitimen Grund dafür gibt. Eine Speicherung erfolgt dann in Übereinstimmung mit den entsprechenden gesetzlichen Verpflichtungen. NTT DATA vernichtet, löscht oder anonymisiert personenbezogene Daten, wenn die Aufbewahrungsfrist abgelaufen ist und kein berechtigtes Interesse an der Aufbewahrung der personenbezogenen Daten für einen längeren Zeitraum besteht.

NTT DATA bewahrt die im Auftrag seiner Kunden verarbeiteten personenbezogenen Daten gemäß den Anforderungen der Kunden und den geltenden Gesetzen auf und wird personenbezogene Daten sicher vernichten, löschen, anonymisieren oder zurückgeben, wenn dies angefordert wird und keine weiteren Verpflichtungen zur Aufbewahrung der personenbezogenen Daten gemäß den geltenden Gesetzen bestehen.

NTT DATA unternimmt alle zumutbaren Anstrengungen, um sicherzustellen, dass die zu verarbeitenden personenbezogenen Daten korrekt, vollständig und aktuell sind.

2.6. Rechte der betroffenen Person

Die Datenschutzgesetze in bestimmten Ländern gewähren den betroffenen Personen bestimmte Rechte in Bezug auf ihre personenbezogenen Daten. NTT DATA verpflichtet sich, diese Rechte zu wahren und auf Anfragen betroffener Personen rechtzeitig, transparent, fair, ethisch und rechtmäßig zu reagieren.

NTT DATA hat angemessene Richtlinien und Verfahren eingeführt, um die Rechte der betroffenen Personen in Übereinstimmung mit den geltenden Datenschutzgesetzen zu wahren.

NTT DATA unterstützt die folgenden Rechte betroffener Personen:

- Recht auf Information
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit
- Recht auf Einschränkung der Nutzung
- Widerspruchsrecht (einschließlich des Rechts, sich vom Direktmarketing und dem Verkauf personenbezogener Daten abzumelden)
- Recht auf Anfechtung automatisierter Entscheidungen
- Recht auf Nichtdiskriminierung
- Recht auf Beschwerde

NTT DATA stellt sicher, dass den betroffenen Personen geeignete Kanäle zur Verfügung stehen, damit sie ihre Rechte in Bezug auf personenbezogene Daten, die NTT DATA über sie verarbeitet, ausüben können.

NTT DATA führt Aufzeichnungen über alle eingegangenen Anfragen betroffener Personen und die Maßnahmen, die als Reaktion auf diese Anfragen ergriffen wurden.

NTT DATA wird Kunden bei der Beantwortung von Anfragen betroffener Personen in Übereinstimmung mit den bestehenden Vereinbarungen in angemessener Weise unterstützen.

NTT DATA hat Richtlinien und Verfahren für die Beantwortung von Anfragen von Behörden zum Zugriff auf personenbezogene Daten in Übereinstimmung mit den geltenden Gesetzen und vertraglichen Anforderungen festgelegt. NTT DATA führt Aufzeichnungen über diese Anfragen und deren Ergebnisse.

2.7. Grenzüberschreitende Datenübermittlung

NTT DATA trifft bei grenzüberschreitenden Datenübermittlungen angemessene Sicherheitsvorkehrungen (z. B. Berücksichtigung von Angemessenheitsbeschlüssen, Standardvertragsklauseln und andere in den geltenden Rechtsvorschriften festgelegte Instrumente).

Bei der grenzüberschreitenden Übermittlung personenbezogener Daten führt NTT DATA, falls erforderlich, Transfer Impact Assessments (TIAs) durch, um sicherzustellen, dass das Zielland ein gleichwertiges Schutzniveau für die Rechte und Freiheiten der betroffenen Personen bietet wie das Land, in dem die Daten ursprünglich erhoben wurden. Besteht eine solche Gleichwertigkeit nicht, werden wir ergänzende Maßnahmen prüfen und ergreifen, um die Rechte der betroffenen Personen entsprechend mit unseren Richtlinien und gesetzlichen Anforderungen zu unterstützen. Wenn solche ergänzenden Maßnahmen nicht umgesetzt werden können, wird NTT DATA keine personenbezogenen Daten übermitteln.

NTT DATA stützt sich auf Standardvertragsklauseln, um die rechtmäßige Übermittlung personenbezogener Daten außerhalb des Landes, in dem sie ursprünglich erhoben wurden, zu unterstützen. Um solche Übertragungen zu unterstützen, bestehen entsprechende Vereinbarungen mit Tochtergesellschaften, Konzerngesellschaften, verbundenen Unternehmen, Auftragsverarbeitern, Unterauftragsverarbeitern und Kunden von NTT DATA.

2.8. Regulatorische Überwachung

NTT DATA überwacht Änderungen der Datenschutzgesetze in den Ländern, in denen das Unternehmen tätig ist, und hat Prozesse und Tools zur Unterstützung der Compliance implementiert.

2.9. Schulung und Sensibilisierung

NTT DATA hat sich verpflichtet, durch kontinuierliche Schulungen und Sensibilisierungsinitiativen eine Kultur des Bewusstseins und der Compliance zu implementieren. Wir verlangen von allen Mitarbeitern, dass sie die obligatorischen Schulungen zum Datenschutz in regelmäßigen Abständen absolvieren. Schulungsmaterialien und die damit verbundenen Richtlinien, Prozesse, Standards und Richtlinien stehen den Mitarbeitern zur Verfügung und werden regelmäßig kommuniziert. Bei Bedarf werden lokale, regionale oder funktionale Schulungen angeboten, um die Mitarbeiter dabei zu unterstützen, im Einklang mit den Anforderungen in bestimmten Ländern, Regionen oder Geschäftsfunktionen zu handeln.

2.10. Sicherheit für den Datenschutz

NTT DATA hat geeignete technische und organisatorische Maßnahmen ergriffen, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten zu gewährleisten, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und des Zwecks der Verarbeitung personenbezogener Daten sowie der Risiken für die Rechte und Freiheiten der betroffenen Personen.

Die Sicherheitsmethoden von NTT DATA orientieren sich an der ISO 27001 und dem Cybersecurity Framework (CSF) des National Institute of Standards and Technology (NIST).

2.11. Reaktion auf Datenschutzverletzungen und Benachrichtigung

NTT DATA verfügt über Richtlinien, Prozesse und Verfahren zur Identifizierung, Erkennung, Reaktion und Wiederherstellung einer Verletzung des Schutzes personenbezogener Daten sowie zur Benachrichtigung der entsprechenden Interessengruppen im Falle einer solchen Verletzung. Dazu gehören Mechanismen zur Durchführung einer Ursachenanalyse und zur Durchführung von Korrekturmaßnahmen.

NTT DATA setzt sich dafür ein, dass die zuständigen Datenschutzbehörden, betroffene Kunden und betroffene Personen im Falle einer Verletzung des Schutzes personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen und allen vertraglichen Verpflichtungen benachrichtigt werden.

NTT DATA führt Aufzeichnungen über alle Verletzungen des Schutzes personenbezogener Daten und die Maßnahmen, die als Reaktion auf diese Ereignisse ergriffen wurden.

Abschnitt 3: Maßnahmen zur Informationssicherheit beschreibt unsere Maßnahmen zum Incident Management zur Identifizierung, Erkennung, Reaktion und Wiederherstellung von Informationssicherheitsvorfällen.

2.12. Third Party Management

NTT DATA ist verantwortlich für die Handlungen von Auftragsverarbeitern und Unterauftragsverarbeitern, die personenbezogene Daten in unserem Auftrag verarbeiten. Wir bewerten die Fähigkeit dieser Auftragsverarbeiter und Unterauftragsverarbeiter, personenbezogene Daten in Übereinstimmung mit den NTT DATA-Standards zu schützen zum Zeitpunkt der Auswahl und danach in regelmäßigen Abständen.

Die Auftragsverarbeiter und Unterauftragsverarbeiter von NTT DATA sind verpflichtet, entsprechende Vereinbarungen zu unterzeichnen, die die Verarbeitung und den Schutz personenbezogener Daten regeln. Diese Vereinbarungen enthalten Anforderungen, die sicherstellen, dass die gleichen Verpflichtungen an alle anderen Auftragsverarbeiter weitergegeben werden, die personenbezogene Daten verarbeiten können.



Maßnahmen zur Informationssicherheit

NTT DATA ist verpflichtet, sicherzustellen, dass die Informationssicherheit implementiert und ordnungsgemäß verwaltet wird, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten zu schützen.

NTT DATA hat geeignete Richtlinien, Prozesse, Verfahren, Standards und Vorgaben eingeführt, um die Sicherheit der von NTT DATA verarbeiteten Daten zu gewährleisten. Die Sicherheitsmethoden von NTT DATA orientieren sich an ISO 27001 und anderen Best Practices der Branche.

3.1. Rollen und Zuständigkeiten im Bereich der Informationssicherheit

Rollen und Verantwortlichkeiten für die Informationssicherheit, einschließlich eines Chief Information Security Officer im gesamten Unternehmen wurden formell mit Berichtslinien, die die Unabhängigkeit der Funktion gewährleisten, zugewiesen.

Die Mitarbeiter von NTT DATA sind dafür verantwortlich, in ihrer täglichen Geschäftstätigkeit in Übereinstimmung mit unseren Richtlinien, Prozessen, Standards und Vorgaben zur Informationssicherheit zu handeln.

3.2. Richtlinien zur Informationssicherheit

NTT DATA hat eine Reihe von Informationssicherheitsrichtlinien dokumentiert und veröffentlicht. Diese Richtlinien und die unterstützende Dokumentation werden regelmäßig überprüft.

3.3. Mobile Device Management

NTT DATA hat ein Zero-Trust-Architektur-Framework für die Implementierung und Aufrechterhaltung von Sicherheitskontrollen für den Zugriff auf und die Interaktion mit NTT DATA-Systemen und Informationsressourcen eingerichtet. Dieser Rahmen umfasst:

- EDM-Richtlinien (End User Device Management) und unterstützende Verfahren.
- Kontrollen und Tools zur Aufrechterhaltung der Sicherheit.
- Vertraulichkeit, Verfügbarkeit und Integrität von Unternehmensdaten. Diese Daten können auf Endgeräten (einschließlich Mobiltelefonen, Tablets und Geräten, die einen Fernzugriff ermöglichen) gespeichert oder über diese zugänglich sein.

3.4. Human Resources

NTT DATA führt Hintergrund- und Beschäftigungsüberprüfungen für seine Mitarbeiter durch, soweit dies nach geltendem Recht zulässig ist, um ihre Eignung für die Einstellung und den Umgang mit Unternehmens- und Kundeninformationen (einschließlich personenbezogener Daten) zu überprüfen. Der Umfang der Überprüfung ist proportional zu den Geschäftsanforderungen und der Klassifizierung der Informationen, auf die der Mitarbeiter Zugriff hat.

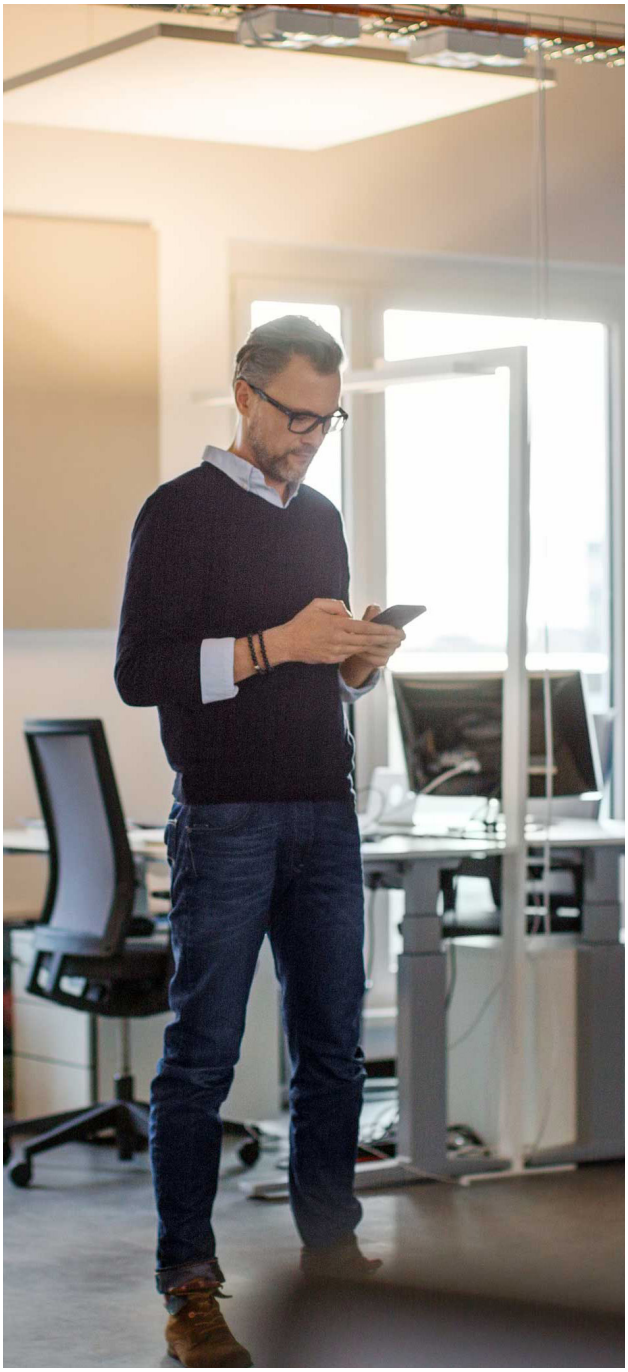
NTT DATA verlangt, dass alle Mitarbeiter (einschließlich Auftragnehmer und Zeitarbeiter) zustimmen, die Vertraulichkeit von Unternehmens- und Kundendaten (einschließlich personenbezogener Daten) zu wahren.

Die Mitarbeiter von NTT DATA sind verpflichtet, Schulungen zum Thema Informationssicherheit und regelmäßige Auffrischungsschulungen zu absolvieren. Informationssicherheitsrichtlinien und unterstützende Verfahren, Prozesse und Richtlinien werden den Mitarbeitern zur Verfügung gestellt. Die Mitarbeiter erhalten außerdem relevante Informationen über Trends, Bedrohungen und Best Practices. Außerdem werden Kampagnen zur Sensibilisierung für das Sicherheitsrisiko regelmäßig durchgeführt, um ein kontinuierliches Bewusstsein zu gewährleisten.

3.5. Akzeptable Nutzung

NTT DATA hat Richtlinien eingeführt, die die ordnungsgemäße und effektive Nutzung der Informationsressourcen unterstützen, zu denen Computer- und Telekommunikationsressourcen, Produkte, Dienstleistungen, Lösungen und IT-Infrastrukturen gehören.

NTT DATA hat Richtlinien zur Informationsklassifizierung eingeführt, um angemessene Kontrollen für den Umgang mit Informationen auf der Grundlage ihrer Klassifizierung zu unterstützen. Informationen und Assets werden gemäß dem jeweiligen Klassifizierungslabel geschützt.



> “Die Sicherheitsmethoden von NTT DATA orientieren sich an ISO 27001 und anderen Best Practices der Branche.”

3.6. Zugriffskontrollen

NTT DATA hat Zugriffskontrollrichtlinien, unterstützende Verfahren sowie logische und physische Zugriffsmaßnahmen eingeführt, um sicherzustellen, dass nur autorisierte Personen Zugriff auf Informationen haben, basierend auf den Prinzipien der geringsten Rechte.

NTT DATA setzt branchenübliche Verschlüsselung im Ruhezustand und bei der Übertragung von Daten ein, um sicherzustellen, dass personenbezogene Daten vor unbefugtem Zugriff oder unbefugter Offenlegung geschützt sind.

Zugriffsüberprüfungen werden regelmäßig durchgeführt, um sicherzustellen, dass nur autorisierte Personen Zugriff auf die Systeme und Informationsressourcen von NTT DATA haben.

NTT DATA hat angemessene Anstrengungen unternommen, um die Anzahl der Benutzer zu begrenzen, die privilegierten Zugriff auf die Systeme und Informationsressourcen von NTT DATA haben.

NTT DATA gestattet die Weitergabe von Konten oder Anmeldedaten nicht, es sei denn, dies wurde durch den entsprechenden Ausnahmeverwaltungsprozess genehmigt.

3.7. Asset Management und Klassifizierung

NTT DATA hat Richtlinien festgelegt, die die Klassifizierung und den Umgang mit physischen und informativen Assets regeln, einschließlich der sicheren Entsorgung, um sicherzustellen, dass die Informationen auf angemessene Weise geschützt sind.

Assets basieren auf der Geschäftskritikalität, um Vertraulichkeitsanforderungen zu bestimmen. Branchenleitlinien für den Umgang mit personenbezogenen Daten bilden den Rahmen für technische, organisatorische und physische Schutzmaßnahmen. Zu diesen Sicherheitsvorkehrungen können Themen wie Zugriffsverwaltung, Verschlüsselung, Protokollierung, Überwachung sowie Datenvernichtung gehören.

3.8. Physische und umweltbezogene Sicherheit

NTT DATA hat angemessene Maßnahmen in Übereinstimmung mit unseren physischen Sicherheitsrichtlinien ergriffen, um unbefugten physischen Zugriff oder Beschädigung oder Beeinträchtigung von Informationen, Anwendungen, Systemen, Datenbanken und Infrastrukturen zu verhindern. Dazu gehören:

- Physische Zugangskontrollen
- Überwachung und Auditierung des physischen Zugangs
- Schutz vor Umweltgefahren
- Sicherung physischer Assets
- Umgang mit physischen Assets
- Instandhaltung und Entsorgung von Hardware
- Klare Schreibtisch- und Bildschirmvorgaben
- Zugang und Betreuung von Besuchern

3.9. Betriebssicherheit

NTT DATA hat entsprechende Spezialistenteams zusammengestellt, die für das Management und den Schutz der Informationssysteme und der Infrastruktur von NTT DATA verantwortlich sind.

NTT DATA hat Richtlinien und unterstützende Verfahren für den Umgang mit Änderungen an Geschäftsprozessen, Informationssystemen und der Infrastruktur eingeführt. NTT DATA hat mehrere Governance-Strukturen eingerichtet, um Änderungen auf der Grundlage der Größe und des Umfangs der Änderung und der strategischen Ziele zu überprüfen und zu genehmigen. Alle Anfragen und deren Ergebnisse werden protokolliert und dokumentiert.

NTT DATA hat Programme für das Threat- und Vulnerabilitymanagement entwickelt, die von branchenüblichen Tools unterstützt werden, um Risiken für Unternehmensinformationen, einschließlich der personenbezogenen Daten von Mitarbeitern und Kunden, zu identifizieren, zu verwalten und zu mindern. Dazu gehören Endpoint Detection and Response (EDR) der nächsten Generation für Antiviren- und Antimalware-Tools, regelmäßige Scans von Umgebungen, das Patchen von Protokollen und das Management von Abhilfe- und Verbesserungsaktivitäten.

Der Kapazitätsbedarf wird kontinuierlich überwacht und regelmäßig überprüft. Systeme und Netzwerke werden in Übereinstimmung mit diesen Überprüfungen verwaltet und skaliert.

Die Systemverfügbarkeit umfasst Architektur, Hochverfügbarkeitsdesign, Disaster Recovery und/ oder Backups basierend auf den Risiko- und Verfügbarkeitsanforderungen für jedes System. Die Methode zur Aufrechterhaltung der Systemverfügbarkeit oder -wiederherstellung, einschließlich des Umfangs und der Häufigkeit von Backups, wird durch die Geschäftsanforderungen von NTT DATA, einschließlich der Kundenanforderungen, sowie durch die Kritikalität der Informationen bestimmt. Notfallwiederherstellungspläne werden regelmäßig getestet. Backup-Prozesse werden überwacht, um den erfolgreichen Abschluss von Backups sicherzustellen und Backup-Probleme, Ausnahmen oder Fehler zu verwalten.

NTT DATA unternimmt angemessene Anstrengungen, um die Audit-Protokollierung von Anwendungen und Systemen aufrechtzuerhalten. Die Protokolle werden regelmäßig überprüft und stehen zu Untersuchungszwecken zur Verfügung. Der Zugriff auf die Protokolle ist streng auf autorisiertes Personal beschränkt.

3.10. Beschaffung, Entwicklung und Wartung von Systemen

NTT DATA hat ein Zero-Trust-Architektur-Framework entwickelt, um das Design, den Erwerb, die Entwicklung und die Wartung von Informationssystemen und -architekturen zu steuern.

Es gibt Architektur- und Designrichtlinien sowie unterstützende Standards und Verfahren, um sicherzustellen, dass die Security-by-Design-Prinzipien innerhalb des Softwareentwicklungszyklus angewendet werden.

3.11. Third Party Management

NTT DATA hat Richtlinien und Praktiken für das Management von Drittanbietern festgelegt, um sicherzustellen, dass Informationsressourcen geschützt sind, wenn NTT DATA Drittanbieter und/oder Auftragsverarbeiter beauftragt. Dazu gehören Anforderungen an die Sorgfaltspflicht im Bereich der Informationssicherheit und an Risikobewertungen der Informationssicherheit, die durchgeführt werden müssen, um sicherzustellen, dass:

- die Anforderungen an die Informationssicherheit in Übereinstimmung mit den Informationssicherheitsstandards von NTT DATA klar formuliert und dokumentiert werden.
- Dienstanbieter und Auftragsverarbeiter von NTT DATA das gleiche Maß an Schutz und Kontrolle wie NTT DATA implementieren.
- Dienstleister und Auftragsverarbeiter verpflichtet sind, vermutete oder tatsächliche Vorfälle der Informationssicherheit rechtzeitig an NTT DATA zu melden.

3.12. Management von Vorfällen im Bereich der Informationssicherheit

NTT DATA verfügt im Rahmen von Informationssicherheitsvorfällen über Richtlinien, Prozesse und Verfahren für die Identifizierung, Erkennung, Reaktion und Wiederherstellung einschließlich der Fälle von Verletzungen des Schutzes personenbezogener Daten sowie die Benachrichtigung der entsprechenden Betroffenen im Falle eines solchen Vorfalls. Dazu gehören Mechanismen zur Durchführung einer Ursachenanalyse und zur Durchführung von Korrekturmaßnahmen, um ein erneutes Auftreten zu verhindern.

NTT DATA hat unternehmensweite Sicherheitsabläufe eingerichtet, um alle Netzwerk- und Computerressourcen proaktiv zu überwachen und zu verwalten. Diese Vorgänge werden durch technische Tools für Information, Sicherheit, Incident, Response und Recovery unterstützt.

3.13. Business Continuity

NTT DATA hat Pläne für Business Continuity und Disaster Recovery erstellt. NTT DATA hat einen mehrschichtigen Ansatz für die Geschäftskontinuität gewählt, um die Verfügbarkeit von Systemen und Daten sicherzustellen.

3.14. Compliance

NTT DATA hat Rollen und Verantwortlichkeiten für die Identifizierung von Gesetzen und Vorschriften festgelegt, die sich auf unsere Geschäftstätigkeit auswirken. Die Verantwortung für die Einhaltung von Gesetzen und Vorschriften wird auf Konzern- und regionaler Ebene festgelegt, um sicherzustellen, dass NTT DATA die globalen und lokalen Anforderungen erfüllt.


NTT DATA