Richtlinienbezeichnung: Data Protection GDPR Policy
Verantwortliche Person: Radosław Bieliński
Genehmigende Person: Radosław Bieliński
Genehmigungsdatum: 12.05.2020
Chief Compliance Officer Überprüfungsdatum: 12.05.2020

VERSION	AUTOR	ÄNDERUNGSBESCHREIBUNG	GENEHMIGT DURCH
16.06.2020	Radosław Bieliński	Einleitung neues Bezeichnungssystem für Richtlinie	Radosław Bieliński

Inhaltsverzeichnis

1. Einleitung

Der Datenschutz ist ein Grundrecht und für unsere Organisation ein wichtiges Anliegen. DYWIDAG, als globale Gruppe, bekennt sich daher zur Einhaltung aller Gesetze, Regelungen und Vorschriften in Verbindung mit dem Datenschutz, die für ihre Tochtergesellschaften gelten, dies schließt insbesondere die Datenschutz-Grundverordnung („DSGVO“) ein.

DYWIDAG sammelt, speichert und verarbeitet personenbezogene Daten, die sich auf verschiedene betroffene Personen wie z. B. Arbeitnehmer, Bewerber, Lieferanten und Dritte beziehen. Die korrekte und rechtmäßige Handhabung von personenbezogenen Daten soll vertrauenswürdig gewahrt bleiben und dem Ansehen der DYWIDAG-Gruppe als sozial verantwortungsbewusster Geschäftspartner und Arbeitgeber entsprechen.

In dieser Richtlinie sind alle Anforderungen in diesem Geltungsbereich dargelegt, die befolgt werden müssen und die international anerkannten Grundsätze des Datenschutzes bilden. Diese Anforderungen gelten für alle Tochterunternehmen von DYWIDAG, ihre Arbeitnehmer, Auftragnehmer, zeitlich befristeten Arbeitnehmer sowie Mitarbeiter von Agenturen – einschließlich aller Personen, mit denen wir zusammenarbeiten oder die in unserem Auftrag handeln und bisweilen Datenzugang benötigen. Die Richtlinie behandelt alle Verarbeitungstätigkeiten, bei denen personenbezogene Daten involviert sind, und hilft Ihnen dabei, personenbezogene Daten sowie Ihre Rechte und Pflichten in Bezug auf solche Daten zu erkennen.

Die Datenschutzrichtlinie von DYWIDAG ergänzt das nationale Datenschutzrecht oder findet Anwendung, wenn nationale Rechtsvorschriften fehlen. Die Tochterunternehmen von DYWIDAG, für die diese Richtlinie aufgrund bestehender Governance-Regelungen (z. B. Joint Ventures) nicht direkt gilt, müssen ihre eigenen Richtlinien und Verfahrensweisen auf der Grundlage der jeweiligen nationalen Rechtsvorschriften und Anforderungen implementieren.

Eine Verletzung der jeweiligen Datenschutzgesetze kann in einem großen Schaden für DYWIDAG in Form eines Ansehensverlusts und großer Bußgelder resultieren und das Vertrauen von Kunden, Arbeitnehmern und der Öffentlichkeit sowie aller sonstigen Interessenträger betreffen. Aus diesem Grund verlassen wir uns darauf, dass Sie die in dieser Richtlinie dargelegten Anforderungen einhalten.

2. Geltungsbereich

Der Geltungsbereich dieser Richtlinie betrifft:

- alle Verarbeitungstätigkeiten bezüglich personenbezogener und sensibler personenbezogener Daten, bei denen DYWIDAG als Datenverantwortlicher fungiert, einschließlich von personenbezogenen Daten in physischer Form, die in einem entsprechenden Aktensystem aufbewahrt werden
- alle Arbeitnehmer, Auftragnehmer, Dritte, Auftragsverarbeiter oder sonstigen Personen, die personenbezogene oder sensible personenbezogene Daten im Auftrag der DYWIDAG-Gruppe verarbeiten
- alle geographischen Gebiete, einschließlich von Drittländern außerhalb der Europäischen Union (EU). Alle Tochterunternehmen von DYWIDAG und ihre Arbeitnehmer müssen personenbezogene Daten mit einem gebührenden Maß an Sorgfalt und in Übereinstimmung mit den rechtlichen Anforderungen sowie dieser Richtlinie verarbeiten.

Insbesondere was Organisationen und Datenverarbeitungstätigkeiten anbelangt, die der DSGVO unterliegen, sind zusätzliche Leitlinien und Verfahrensweisen von essenzieller Bedeutung. Diese müssen durch die lokale Geschäftsführung oder durch einen benannten Beauftragten entwickelt und eingerichtet werden, damit die Vorschriften, die seit Mai 2018 zusätzlich zu etwaigen nationalen Gesetzen Anwendung finden, eingehalten werden. Auch Tochterunternehmen, die außerhalb der Europäischen Union operieren, müssen zusätzliche lokale Richtlinien und Leitlinien entwickeln, falls dies notwendig ist, um die entsprechenden nationalen Rechtsvorschriften und Datenschutzgesetze einzuhalten. Tochterunternehmen von DYWIDA, für die keine nationalen Datenschutzgesetze gelten, müssen diese Richtlinie übernehmen und anwenden.

Diese Richtlinie hat ggf. nachrangige Bedeutung, falls durch entsprechende nationale Gesetze Konflikte entstehen oder diese strengere Anforderungen vorsehen. Die Überwachung der nationalen Rechtsvorschriften zum Datenschutz und der entsprechenden Entwicklungen oder Ergänzungen obliegt den lokalen Geschäftsführungen der Organisationen. Falls Ergänzungen nationaler Rechtsvorschriften mit dieser Richtlinie in Konflikt stehen, muss dies dem Chief Compliance Officer mitgeteilt werden.

3. Definitionen

- „Personenbezogene Daten“: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, die sogenannte „betroffene Person“, beziehen.
- „Betroffene Person“: Eine identifizierbare natürliche Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung auf eine Kennung wie Namen, Kennziffern, Standortdaten, Online-Kennungen oder auf einen oder mehrere Faktoren, die spezifisch für die physische, physiologische, genetische, geistige, wirtschaftliche, kulturelle oder sozial Identität der natürlichen Person sind. Informationen über die rassische oder ethnische Herkunft, politischen Ansichten, Glaubensvorstellungen oder ähnliche Vorstellungen, die Mitgliedschaft in einer Gewerkschaft, körperliche oder geistige Erkrankungen oder Beeinträchtigungen, die Gesundheit und das Sexualleben, strafrechtliche Anschuldigungen oder Vergehen gelten als sensibel und zählen zu besonderen Kategorien personenbezogener Daten. Nach nationalem Recht können weitere Datenkategorien als besonders sensibel gelten oder Datenkategorien andere Inhalte haben.

  Anonymisierte Daten und Daten, die sich nicht auf eine natürliche Person beziehen (z. B. Unternehmensdaten wie Namen und Adressen von Unternehmen), unterliegen dieser Richtlinie nicht.
- „Verarbeitung“: Die Verarbeitung personenbezogener Daten bedeutet alle Vorgänge oder Vorgangsreihen, die auf automatisiertem oder nicht automatisiertem Wege an personenbezogene Daten oder Reihen von personenbezogenen Daten durchgeführt werden, darunter z. B. das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, das Abgleichen oder Verknüpfen, die Einschränkung, das Löschen oder die Vernichtung solcher Daten
- Ein „Datenverantwortlicher“: ist eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“
- „Auftragsverarbeiter“: verarbeiten personenbezogene Daten im Auftrag des Datenverantwortlichen (z. B. eine Agentur zur Lohnbuchhaltung, die von DYWIDAG, welche als Datenverantwortlicher fungiert, beauftragt wird)

- „Sicherheitsverletzung“: Vorgänge, die zum unbefugten Zugang zu Daten, Anwendungen, Diensten, Netzwerken und/oder Geräten führen, indem die jeweils zugrundeliegenden Sicherheitsmechanismen umgangen werden.
  Eine Sicherheitsverletzung tritt ein, wenn eine Person oder eine Anwendung unrechtmäßig Zugang zu einem privaten, vertraulichen oder unbefugten logischen IT-Perimeter erlangt. Eine Sicherheitsverletzung wird auch als Sicherheitsverstoß bezeichnet und resultiert potenziell in einer Verletzung des Schutzes personenbezogener Daten.
- „Verletzung des Schutzes personenbezogener Daten“: Eine Verletzung der Sicherheit, die unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust oder zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten, die in elektronischer oder ausgedruckter Form übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, führt, und die potenziell die Vertraulichkeit oder Integrität der Daten gefährdet.
- „Dritte“ bedeutet natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, außer der betroffenen Person, dem Datenverantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Datenverantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

4. Rahmenbedingungen und Grundsätze des Datenschutzes

In diesem Abschnitt sind die Rahmenbedingungen und Grundsätze des Datenschutzes beschrieben, die Mindeststandards und Anforderungen für die Organisation unseres Datenschutzes definiert und die Leitlinie zur Gewährleistung, Überwachung und Aufrechterhaltung eines adäquaten Schutzniveaus für personenbezogene Daten enthalten. Im Rahmen der DYWIDAG-Organisation werden persönliche Informationen in transparenter Weise und ausschließlich mit umfassend kooperierenden und informierten Interessenten erhoben. Nach dem Erheben personenbezogener Daten finden die folgenden Grundsätze Anwendung:

Personenbezogene Daten und alle Verarbeitungstätigkeiten werden

- sachlich richtig erfasst und auf dem neuesten Stand gehalten
- ausschließlich zu festgelegten, eindeutigen und legitimen Zwecken erhoben

- nur solange wie nötig und in Übereinstimmung mit den rechtlichen Anforderungen an Aufbewahrungsfirsten gespeichert
- lauter und rechtmäßig verarbeitet
- vor einem unbefugten oder unrechtmäßigen Zugang und Missbrauch durch interne oder externe Parteien geschützt
- dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sein.

Sie werden nicht:

- intern ohne Zweck kommuniziert
- An Organisationen (und Tochterunternehmen), Staaten oder Länder übermittelt, die unzureichende Datenschutzrichtlinien und -vorschriften aufweisen.

Zusätzlich zu den Methoden der Datenhandhabung hat jede Organisation der DYWIDAG-Gruppe direkte Verpflichtungen gegenüber den Personen, denen die Daten gehören. Auf Antrag betroffener Person müssen wir insbesondere Auskunft darüber erteilen, a) welche ihrer Daten verarbeitet werden, b) wie wir diese Daten verarbeiten und c) wer Zugang zu den Informationen hat.

Wir müssen auch

- Vorkehrungen für den Fall verlorener, beschädigter und beeinträchtiger Daten einrichten
- Personen die Möglichkeit geben, die Änderung, Löschung, Reduzierung oder Berichtigung von Daten in unseren Datenbanken zu beantragen.

Um ein adäquates Schutzniveau für die personenbezogenen Daten zu gewährleisten, verpflichten wir uns dazu:

- Den Zugang zu personenbezogenen Daten, insbesondere zu sensiblen personenbezogenen Daten, zu beschränken und zu überwachen
- Transparente Verfahrensweisen für die Datenerhebung zu entwickeln
- Arbeitnehmer im Online-Datenschutz und in Sicherheitsmaßnahmen zu unterweisen
- Sichere Netzwerke zum Schutz von Online-Daten vor Cyberangriffen einzurichten
- Klare Verfahrensweisen zur Meldung von Datenschutzverletzungen oder Datenmissbräuchen zu etablieren

- Vertragsklauseln aufzunehmen, sofern dies für notwendig erachtet wird, oder Erklärungen zu unserem Umgang mit Daten mitzuteilen
- Bewährte Verfahrensweisen (Zugangskontrollen an Gebäuden, Büros und IT-Systemen, Schreddern von Dokumenten, sichere Schlösser, Geräte und Datenverschlüsselung, häufige Sicherungen (Backups), Zugangsberechtigung, Notfallwiederherstellungspläne usw.) einzurichten

Diese Grundsätze sind in den nachstehenden Abschnitten dieser Richtlinie näher beschrieben.

4.1 Grundsätze für die Verarbeitung personenbezogene Daten

Bei der Verarbeitung personenbezogener Daten gelten die folgenden durchsetzbaren Grundsätze:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz: personenbezogene Daten dürfen ausschließlich zu festgelegten, eindeutigen und legitimen Zwecken in einer nachvollziehbaren und transparenten Weise sowie in Übereinstimmung mit dem geltenden Recht verarbeitet werden. Betroffene Personen müssen über den Umgang mit ihren Daten informiert werden. Grundsätzlich müssen personenbezogene Daten direkt von der betreffenden Einzelperson erhoben werden. Beim Erheben der Daten muss die betroffene Person entweder wissen oder darüber informiert werden, a) welche Identität der Datenverantwortliche hat, b) zu welchem Zweck die Daten verarbeitet werden und c) an welche Dritten oder Kategorien von Dritten die Daten übermittelt werden können.
- Zweckbindung: Personenbezogene Daten dürfen ausschließlich für die Zwecke erhoben und verarbeitet werden, die vor der Erhebung definiert wurden. Die Erhebung und Verarbeitung ist auf ein notwendiges Maß für die Zwecke der Verarbeitung beschränkt und eine Weiterverarbeitung, die mit den ursprünglichen Zwecken unvereinbar ist, ist nicht zulässig.
- Datenminimierung: Personenbezogene Daten müssen angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Personenbezogene Daten dürfen nur dann im Voraus erhoben und für potenzielle zukünftige Zwecke gespeichert werden, wenn die betroffene Person hierzu Ihre Einwilligung erklärt hat oder wenn dies nach nationalem Recht erforderlich oder zulässig ist.
- Richtigkeit: Aufgezeichnete personenbezogene Daten müssen richtig, vollständig und – erforderlichenfalls – aktualisiert werden. Es müssen angemessene Schritte unternommen

werden, um die Löschung, Berichtigung, Ergänzung oder Aktualisierung unrichtiger oder unvollständiger Daten sicherzustellen.

- Speicherfrist und Löschung: Personenbezogene Daten dürfen nur solange und in einer Weise gespeichert werden, als dies für die Erfüllung der beabsichtigten Zwecke der Erhebung und Verarbeitung erforderlich ist. Nach dem Ablauf der rechtlichen oder geschäftsprozessbezogenen Fristen müssen die nicht mehr benötigten personenbezogenen Daten in sicherer Weise gelöscht werden.
- Integrität und Vertraulichkeit, Datensicherheit: Personenbezogene Daten müssen so verarbeitet werden, dass a) eine angemessene Sicherheit der Daten sichergestellt ist; b) Daten unter Verwendung geeigneter, moderner Systeme und Software, die dem neuesten Stand entsprechen, sicher gespeichert werden.

Angemessene technische und organisatorische Sicherheitsmaßnahmen (TOM – z. B. Zugangskontrollen, Passwortregeln, physische Server-Sicherheit, Sicherungsleitlinien usw.) müssen eingerichtet und formal von allen unseren Organisationen beschrieben sein, um unbefugte oder unrechtmäßige Zugänge und Missbräuche, Verarbeitungen oder Weitergaben sowie unbeabsichtigte Verluste, Veränderungen oder Vernichtungen zu verhindern.

Die Einhaltung dieser Grundsätze muss durch ein Verzeichnis von (IT-)Systemen und Verarbeitungstätigkeiten gestützt werden, in dem alle Informationen und Verfahrensweisen in Verbindung mit personenbezogenen Daten dokumentiert sind (z. B. Kategorie der betroffenen Person, Kategorie der personenbezogenen Daten, Zweck der Verarbeitung). Alle Organisationen müssen eine solches Verzeichnis von Verarbeitungstätigkeiten führen, insbesondere Organisation mit Verarbeitungstätigkeiten, die der DSGVO (Art. 30 DSGVO) unterliegen.

4.2 Rechtmäßigkeit der Verarbeitung

DYWIDAG muss sicherstellen, dass die Verarbeitung rechtmäßig ist und die Rechtsgrundlagen für die Verarbeitung dokumentieren. Zur rechtmäßigen Verarbeitung personenbezogener Daten ist eine Verarbeitung auf den folgenden Rechtsgrundlagen erforderlich:

- Die Einwilligung der betroffenen Person in die Verarbeitung (z. B. Übermittlung von Lebensläufen durch Stellenbewerber, Marketing-Newsletter)
- die Verarbeitung ist erforderlich, um einen Vertrag mit der betroffenen Person abzuschließen oder zu erfüllen (z. B. Arbeitsvertrag)
- Zur Erfüllung einer rechtlichen Verpflichtung, welcher DYWIDAG und ihre Tochternehmen (die Datenverantwortlichen) unterliegen
- Aufgrund eines berechtigten Interesses von DYWIDAG oder der Partei, welcher die personenbezogenen Daten offengelegt werden (z. B. Benutzerprotokolldateien oder IP-Adressen können vorübergehend gespeichert werden, was dadurch gerechtfertigt ist, dass die angemessene Funktion und Sicherheit des Netzwerks sichergestellt wird)
- Aufgrund eines lebenswichtigen Interesses der Öffentlichkeit und anderer Interessenträger
- Aufgrund öffentlicher Aufgaben und Pflichten.

Die Verarbeitung besonderer Kategorien von personenbezogenen Daten muss gemäß nationalem Recht ausdrücklich zulässig oder vorgeschrieben sein. Darüber hinaus kann eine Verarbeitung zulässig sein, falls dies erforderlich ist, damit die zuständige Behörde ihre Rechte und Pflichten in Bezug auf das Arbeitsrecht erfüllen kann. Arbeitnehmer können auch ausdrücklich in die Verarbeitung einwilligen.

Abgesehen von der Speicherung wird die Verarbeitung unverzüglich eingestellt, sofern es keine Rechtsgrundlagen gibt.

4.3 Rechte betroffener Personen

Auf Antrag einer betroffenen Person muss die entsprechende Organisation Auskunft über die personenbezogenen Daten erteilen, die im Rahmen des geltenden Rechts erhoben wurden. Grundsätzlich haben betroffene Personen das Recht:

- Auskunft über die personenbezogenen Daten zu beantragen, die ein Datenverantwortlicher über sie gespeichert hat
- die Verarbeitung ihrer personenbezogene Daten zu verhindern, der Verarbeitung ihrer personenbezogene Daten zu widersprechen oder die Verarbeitung ihrer personenbezogene Daten (z. B. für Direktwerbungszwecke) zu beschränken
- die Änderung personenbezogener Daten zu beantragen

- Informationen zur Identität des Empfängers oder der Kategorien von Empfängern zu beantragen, falls ihre personenbezogenen Daten an Dritte übermittelt wurden (z. B. unterbeauftragte Auftragsverarbeiter)
- Die Löschung ihrer Daten zu beantragen, falls die Verarbeitung solcher Daten ohne Rechtsgrundlage erfolgt oder falls die Rechtsgrundlage nicht mehr gilt Das Gleiche gilt, wenn der Zweck für die Datenverarbeitung hinfällig ist oder aus anderen Gründen nicht mehr gilt. Rechtliche Speicherfristen können Vorrang vor diesem Recht haben und müssen genau überwacht werden.

Bitte kontaktieren Sie unverzüglich den Chief Compliance Officer, falls Sie einen Auskunftsantrag von einer betroffenen Person erhalten. Diese Anträge müssen baldmöglichst, spätestens jedoch innerhalb von 30 Kalendertagen, bearbeitet und der betroffenen Person auf sicherem Wege mitgeteilt werden.

4.4 Übermittlung personenbezogener Daten und Auftragsdatenverarbeitung (Vertrag)

Übermittlungen personenbezogener Daten innerhalb der Gruppe oder personenbezogene Daten, die im Auftrag eines Datenverantwortlichen („Auftragsverarbeitung“) verarbeitet werden, müssen auf den Grundsätzen basieren, die in den Abschnitten 4.1 bis 4.3 aufgeführt sind, und das geltende Recht sowie die gesetzlichen Anforderungen an den Datenschutz des jeweiligen Landes erfüllen.

„Auftragsverarbeitung“ bedeutet, dass ein Auftragsverarbeiter im Auftrag und gemäß den Anweisungen eines Datenverantwortlichen, welcher die Zwecke und Mittel für die Verarbeitung personenbezogenen Daten bestimmt, die Verarbeitung personenbezogener Daten durchführt. In anderen Worten: Ein Auftragsverarbeiter wird vom Datenverantwortlichen mit der Verarbeitung der personenbezogenen Daten beauftragt (z. B. Auslagerung von Verwaltung der Lohnbuchhaltung, Auslagerung der IT-Server an einen Host/Cloud-Anbieter).

Innerhalb der EU dürfen Tätigkeiten der „Auftragsverarbeitung“ ohne bindenden schriftlichen Vertrag, in dem der Gegenstand und die Dauer der Verarbeitung, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sowie die Pflichten und Rechte der als Datenverantwortlicher fungierenden DYWIDAG-Organisation (Artikel 28 EU DSGVO) aufgeführt sind, nicht ausgelagert werden. Für den Fall, dass personenbezogene Daten von einer DYWIDAG-

Organisation (Datenverantwortlicher) innerhalb der EU an einen Empfänger (Auftragsverarbeiter) außerhalb der EU (einschließlich von Übermittlungen innerhalb der Gruppe) übermittelt werden, muss der entsprechende Empfänger einwilligen, ein Datenschutzniveau zu gewährleisten, das gleichwertig zu dem Datenschutzniveau in dieser Datenschutzrichtlinie ist.

Der Datenverantwortliche darf ausschließlich Auftragsverarbeiter verwenden, die hinreichend garantieren können, dass angemessene technische und organisatorische Maßnahmen in einer Weise implementiert wurden, dass die Verarbeitung die Anforderungen dieser Richtlinie erfüllt und der Schutz der Rechte betroffener Personen sichergestellt ist.

4.5 Vertraulichkeit der Verarbeitung

Alle personenbezogenen Daten unterliegen dem Datengeheimnis, daher:

- ist jedes unbefugte Erheben und Verarbeiten solcher Daten durch Arbeitnehmer verboten
- ist die Verarbeitung von Daten durch Arbeitnehmer, die nicht im Rahmen ihrer rechtmäßigen Pflichten durchgeführt werden darf, verboten.

Es gilt der „Need-to-know"-Grundsatz: Arbeitnehmer dürfen ausschließlich Zugang zu persönlichen Informationen haben, soweit dies für die Art und den Umfang der betreffenden Aufgabe angemessen ist. Dies erfordert eine sorgfältige Aufgliederung und Unterteilung sowie die Implementierung von Rollen und Verantwortlichkeiten.

Arbeitnehmer dürfen die von uns erhobenen personenbezogenen Daten nicht für private oder gewerbliche Zwecke verwenden oder unbefugten Personen offenlegen; Arbeitgeber müssen ihre Arbeitnehmer zu Beginn des Arbeitsverhältnisses über die Pflicht zum Schutz des Datengeheimnisses informieren und mit dieser Richtlinie vertraut machen (z. B. indem eine schriftliche Bestätigung dieser Richtlinie angefordert wird). Diese Pflicht bleibt auch nach dem Ende des Arbeitsverhältnisses bestehen.

4.6 Sicherheit der Verarbeitung

Personenbezogene Daten müssen vor unbefugtem Zugang und unrechtmäßiger Verarbeitung oder

Offenlegung sowie vor unbeabsichtigten Verlusten, Veränderungen oder Vernichtungen geschützt werden. Dies gilt unabhängig davon, ob die Daten in elektronischer oder in Papierform verarbeitet werden. Diese technischen und organisatorischen Sicherheitsmaßnahmen müssen auf modernen Technologien, die dem neuesten Stand der Technik entsprechen, den Risiken der Verarbeitung und dem Schutz der Sensibilität der Daten basieren. Grundsätzlich müssen DYWIDAG und alle Tochterunternehmen sicherstellen, dass:

- Gebäude und Büroräumlichkeiten angemessen vor einem unbefugten Zugang geschützt sind (z. B. Alarmanlagen, Einlasskontrollen und Anmeldung)
- personenbezogene Daten sicher, unter Verwendung moderner Software, die aktualisiert wird, gespeichert werden
- der Zugang zu personenbezogenen Daten ausschließlich auf Personal beschränkt ist, das Zugang benötigt, und dass angemessene Sicherheitsmaßnahmen eingerichtet sind, um die unbefugte Weitergabe von Informationen zu verhindern
- persönliche Daten ausschließlich auf sicherem Wege (z. B. E-Mail-/Laptop-Verschlüsselung, verschlüsselte USB-Sticks) übermittelt werden
- der Zugang zu personenbezogenen Daten überwacht und protokolliert wird (z. B. Audit-Trails für Dateneingaben, Protokollpfade)
- die Verfügbarkeit und Wiederherstellung von Daten (Sicherung und Notfallwiederherstellungsverfahren, Firewalls, Antivirus-Programme) gewährleistet ist
- das Löschen personenbezogener Daten auf sicherem Wege erfolgt, sodass die Löschung unwiederbringlich ist.
- angemessenen Kontrollen eingerichtet sind, wenn personenbezogene Daten an externe Auftragsverarbeiter ausgelagert werden
- Sicherheitsvorfälle/Datenschutzverletzungen und sonstige Zwischenfälle ordnungsgemäß gemeldet und gehandhabt werden.

Die technischen und organisatorischen Maßnahmen müssen vor der Einführung neuer Methoden für die Verarbeitung personenbezogener Daten, insbesondere neuer IT-Systeme und Anwendungen, definiert und implementiert werden. Die Maßnahmen müssen kontinuierlich im Hinblick auf technische Entwicklungen und organisatorische Veränderungen überprüft und abgeschätzt werden.

4.7 Bewusstsein für den Datenschutz

Die Wirksamkeit der Organisation des Datenschutzes bei DYWIDAG setzt voraus, dass sich alle Tochterunternehmen und ihre Arbeitnehmer, die personenbezogene Daten für DYWIDAG verarbeiten, der Wichtigkeit des Datenschutzes und der Datensicherheit bewusst sind.

Die Geschäftsführungen aller DYWIDAG-Organisationen sind daher dazu verpflichtet, unter allen Arbeitnehmern, die personenbezogene Daten verarbeiten, ein entsprechendes Bewusstsein zu fördern. Beispielsweise durch regelmäßige oder mindestens jährliche Datenschutzschulungen, Unternehmensprogramme für die Bewusstseinsschaffung und Sensibilisierung in Form von Online-Schulungen oder anderen geeigneten Methoden (z. B. Präsenzschulungen).

4.8 Organisationsstruktur

Die Geschäftsführungen aller DYWIDAG-Organisationen sind dafür verantwortlich, ein angemessenes Datenschutzniveau sicherzustellen, das im Hinblick auf alle Tochterunternehmen alle geltenden Gesetze erfüllt und die Implementierung einer angemessenen Organisation des Datenschutzes ermöglicht.

Um ein angemessenes Datenschutzniveau und die Durchsetzung dieser Richtlinie sicherzustellen, ist die Implementierung der folgenden Rollen und Funktionen erforderlich:

- Die lokalen Geschäftsführungen der Organisationen müssen Datenschutzkoordinatoren (Data Protection Coordinator, „DPC“) benennen. Die Datenschutzkoordinatoren sind die Ansprechpartner vor Ort, was den Datenschutz betrifft. Sie können Überprüfungen durchführen und müssen die Arbeitnehmer über die Inhalte dieser Datenschutzrichtlinie informieren.
- Datenschutzbeauftragte (Data Protection Officer, „DPO“), sofern das geltende Recht dies erforderlich macht.

In nationalen Rechtsvorschriften können weitere Rollen und Aufgaben definiert sein. Die regionale und/oder lokale Geschäftsführung einer Organisation stellt sicher, dass DPO und DPC:

- hinreichend und rechtzeitig in alle Sachverhalte bezüglich des Schutzes personenbezogener Daten miteinbezogen werden
- Zugang zu allen Prozessen erhalten, welche die Verarbeitung personenbezogener Daten betreffen
- direkt dem Chief Compliance Officer Bericht erstatten können
- im Hinblick auf ihre Tätigkeiten in Übereinstimmung mit dem geltenden Recht zur Vertraulichkeit und Nichtoffenlegung verpflichtet sind.

DPC und DPO können andere Aufgaben, Pflichten und Funktionen erfüllen, wenn diese mit ihrer Tätigkeit als DPC oder DPO nicht in Konflikt stehen. DPC und DPO können für mehrere Organisationen einer Region oder eines Landes benannt werden, falls eine solche Benennung keinen Interessenkonflikt darstellt.

4.9 Datenschutzvorfälle

Die folgenden datenschutzrelevanten Vorfälle müssen den jeweils verantwortlichen lokalen DPC und/oder DPO wie auch dem Chief Compliance Officer und der Rechtsabteilung unverzüglich durch die regionale oder lokale Geschäftsführung einer Organisation gemeldet werden:

- Alle gemeldeten, voraussichtlichen oder potenziellen Datenschutzverletzungen (z. B. E-Mail an falsche Empfänger gesendet, personenbezogene Daten unbefugten Personen offengelegt, eine Sicherheitsverletzung resultiert üblicherweise in einer Datenschutzverletzung)
- Datenschutzbeschwerden, Forderungen und Anschuldigungen von betroffenen Personen (z. B. Arbeitnehmer, Kunden, Lieferanten)
- Datenschutzanträge durch betroffene Personen (z. B. ein Kunde verlangt Auskunft über Verarbeitungstätigkeiten bezüglich seiner personenbezogenen Daten)
- Verletzungen oder potenzielle Verletzungen von Datenschutzgesetzen sowie Verletzungen dieser Datenschutzrichtlinie
- Bußgelder, die durch Datenschutzbehörden auferlegt werden

- Audits, zu denen Datenschutzbehörden raten
- Sicherheitsverletzungen oder -vorfälle bezüglich IT-Systemen (z. B. kompromittierte Systeme, Systemausfälle, Hackversuche, Eindringen in Systeme, unbefugte Zugriffsversuche), die in einer Datenschutzverletzung resultieren können.

Der Verlust oder Diebstahl von Mobilgeräten (Laptops, Mobiltelefonen, Tablets, USB-Sticks) kann in einer
potenziellen Datenschutzverletzung resultieren und muss daher auch dem lokalen DPC/DPO, Chief Compliance Officer und dem Global Head of IT gemeldet werden.

Darüber hinaus muss die lokale Geschäftsführung:

- ein Verzeichnis über alle oben erwähnten Vorfälle und Ereignisse führen
- alle relevanten Dokumente, Mitteilungen und ergriffenen Maßnahmen in Verbindung mit solchen Vorfällen in einer separaten Datei erfassen und auf Antrag zur Verfügung stellen können

Die kompletten Kontaktdetails aller benannten DPO und DPC sowie alle nachfolgenden Änderungen müssen dem Chief Compliance Officer und/oder der Rechtsabteilung der Gruppe mitgeteilt werden.

5. Verantwortlichkeiten und Pflichten, Audit

Die Geschäftsführung der Gruppe und die lokale Geschäftsführung ist dafür verantwortlich, dass alle relevanten organisatorischen, HR- und technischen Maßnahmen eingerichtet sind, damit die Verarbeitung aller personenbezogenen Daten in Übereinstimmung mit den nationalen Datenschutzgesetzen erfolgt. Die Befolgung und Einhaltung dieser Anforderungen obliegt allen betreffenden Arbeitnehmern.

Alle Arbeitnehmer (einschließlich von zeitlich befristeten Arbeitnehmern und Leiharbeitskräften), Führungskräfte und Dienstleister von DYWIDAG, die in den Räumlichkeiten von DYWIDAG personenbezogene Daten verarbeiten, Datenverarbeitungssysteme und -ausrüstung von DYWIDAG verwenden oder in diesem Zusammenhang tätig sind, sind zur Einhaltung dieser Richtlinie verpflichtet.

Über vor Ort oder extern durchgeführte Datenschutz- und/oder IT-Sicherheitssystemüberprüfungen oder ähnliche Abschätzungen wird in regelmäßigen Abständen die Einhaltung dieser Datenschutzrichtlinie durch die Abteilung für gruppeninterne Audits (Group Internal Audit) überprüft. Zur Erfüllung dieser Aufgabe kann die Abteilung für gruppeninterne Audits externe Prüfer oder Sachverständige in diesem Bereich beauftragen.