EU-Allgemeine Datenschutzrichtlinie

Gruppe Bondioli & Pavesi

Inhaltsverzeichnis

1. VORBEMERKUNGEN

Die Gruppe Bondioli & Pavesi legt großen Wert auf die Einhaltung der Vorschriften zum Schutz der Privatsphäre und der persönlichen Daten für die korrekte Umsetzung seiner Tätigkeit, seines Geschäfts und seines Images auf dem Markt. Der Schutz der persönlichen Daten, die jedes Unternehmen der Gruppe sammelt und speichert, mit elektronischen Systemen oder mit traditionellen Methoden, stellt einen relevanten und strategischen Wert für die Gruppe und für die Entwicklung ihres Geschäfts dar.

Vor diesem Hintergrund stellt die EU-Verordnung Nr. 679/2016 (im Folgenden auch „DSGVO" genannt) den Kern der neuen europäischen Gesetzgebung zum Schutz personenbezogener Daten dar und ist die wichtigste Bezugsgrundlage für Aktivitäten mit personenbezogenen Daten innerhalb der EU.

Aus diesem Grund ist es unerlässlich, eine gemeinsame Datenschutzrichtlinie (nachfolgend „**Richtlinie**") für die unter Punkt 3 genannten Unternehmen mit Sitz in der EU (nachfolgend jeweils „**Unternehmen**" und zusammenfassend „**EU-Gruppe**") zu verabschieden und alle Mitarbeiter sowie diejenigen, die im Namen und Auftrag der einzelnen Unternehmen arbeiten, über die Grundsätze und Regeln zu informieren, die die EU-Gruppe zu befolgen beabsichtigt, um ein einheitliches und hohes Datenschutzniveau zu gewährleisten.

Angesichts der Komplexität der Vorschriften einerseits und der Unternehmensprozesse, die personenbezogene Daten beinhalten, andererseits, ist es zunächst notwendig, eine Datenschutz-Governance-Struktur innerhalb der Unternehmen der EU-Gruppe einzurichten, die die Gliederung der Rollen, Verantwortlichkeiten und Aufgaben in Bezug auf den Schutz personenbezogener Daten definiert.

2. ZWECK

Die vorliegende Richtlinie hat zum Ziel, Folgendes zu beschreiben:

(i). die Grundsätze und Maßnahmen, die jedes Unternehmen bei der Verarbeitung personenbezogener Daten befolgen muss,
(ii). die Datenschutzorganisation, um die Governance der Angelegenheit zu verwalten, und
(iii). die Zuweisung von Aufgaben und Verantwortlichkeiten der verschiedenen betrieblichen Ebenen.

Aus diesem Grund muss die Richtlinie allen Personen, die in den Unternehmen personenbezogene Daten verarbeiten, zur Kenntnis gebracht werden.

3. ANWENDUNGSBEREICH

Diese Richtlinie muss von den folgenden Unternehmen befolgt werden:

- Alle italienischen Unternehmen, die zur Gruppe Bondioli & Pavesi gehören;
- Bondioli & Pavesi GMBH;
- Bondioli & Pavesi France SA;
- Bondioli & Pavesi Iberica SA;

- Bondioli & Pavesi Sp. Zo.o.;
- OM Protivin AS.

Zusätzlich zur Einhaltung der folgenden Richtlinie muss jeder von ihnen natürlich auch die GDPR und die lokalen ergänzenden Vorschriften zum Schutz der Privatsphäre und der personenbezogenen Daten einhalten.

4. DEFINITIONEN

Für die Zwecke dieser Richtlinie geben wir die folgenden, aus der DSGVO abgeleiteten Definitionen in der Reihenfolge ihrer Relevanz an:

- **Personenbezogene Daten**: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („**betroffene Person**") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität identifiziert werden kann.
  Darüber hinaus im Falle von Marketingaktivitäten, die nicht vom Empfänger angefordert wurden (z.B. spontane Zusendung von Werbematerial, Direktverkauf, Marktforschung oder kommerzielle Kommunikation), auch alle Informationen, die sich auf eine juristische Person - einschließlich Körperschaften oder Vereinigungen - beziehen.
  Dazu gehören zum Beispiel: persönliche Daten, Post-, Telefon- und Telematik-Adressen, Identifikationscodes, Bestellungen, Umsätze, Bild, Stimme, Lebenslauf, Kaufgewohnheiten, Systemzugriffsprotokolle und ganz allgemein alles, was auf Papier oder Computer aufgezeichnet wird und mit einer identifizierten oder identifizierbaren Person in Verbindung gebracht werden kann.

- **Verarbeitung**: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten oder einer Reihe personenbezogener Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Übertragung durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, den Abgleich oder die Verknüpfung sowie das Einschränken, Löschen oder Vernichten.
  Dazu gehören z.B.: die Verwaltung der Lohn- und Gehaltsabrechnung und der Anwesenheit von Mitarbeitern, die Vertragsverwaltung, das Versenden von Marketing-Kommunikation, Profilerstellung, Videoüberwachung, etc.

- **Besondere Kategorien personenbezogener Daten**: Personenbezogene Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten über Gesundheit oder Sexualleben oder sexuelle Orientierung der Person. Es handelt sich um eine Untergruppe der personenbezogenen Daten.

Dazu gehören zum Beispiel: Krankenscheine, Gewerkschaftsmitgliedschaften, Gewerkschaftsgenehmigungen, Behinderungen, Verletzungen, Parteizugehörigkeit, Gesundheitszustand usw.

- **Personenbezogene Daten, die sich auf strafrechtliche Verurteilungen und Straftaten beziehen:** (im Folgenden „**Strafrechtliche Daten**"), personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen. Es handelt sich um eine Untergruppe der personenbezogenen Daten.

- **Verantwortlicher für die Datenverarbeitung**: die natürliche oder juristische Person, die Behörde, der Dienst oder eine andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
  Wenn zum Beispiel die Website vollständig von Bondioli & Pavesi S.p.A. verwaltet wird, ist das Unternehmen Verantwortlicher für die Verarbeitung der Daten.
  Jedes Unternehmen wird Verantwortlicher, wenn es selbständig entscheidet, wie die Behandlung durchgeführt wird. Die Verarbeitung von Daten der Mitarbeiter ist zum Beispiel mit der Verantwortung der Datenverarbeitung der einzelnen Unternehmen verbunden.

- **Verantwortlicher für die Datenverarbeitung**: Natürliche oder juristische Person oder Behörde, Dienststelle bzw. sonstige Einrichtung, die personenbezogene Daten im Auftrag des für die Datenverarbeitung Verantwortlichen gemäß Artikel 28 der DSGVO verarbeitet.

- **Zur Datenverarbeitung befugtes Personal**: (auch als Datenverarbeiter bezeichnet) - natürliche Person, die personenbezogene Daten unter der direkten Autorität des Datenverantwortlichen oder des Datenverarbeiters verarbeitet;

- **Betroffene Person** Die identifizierte oder identifizierbare natürliche Person, auf die sich die personenbezogenen Daten beziehen. Darüber hinaus ist für den Fall von Marketingaktivitäten, die vom Adressaten nicht angefordert wurden (z.B. spontane Zusendung von Werbematerial, Direktverkauf, Marktforschung oder kommerzielle Kommunikation), ist die betroffene Person auch die juristische Person - einschließlich Körperschaften oder Vereinigungen - wie in der EU-Richtlinie Nr. 58/2002 (Datenschutzrichtlinie) und nachfolgenden Ergänzungen und Änderungen vorgesehen.
  Dies sind z. B.: Kunden, einschließlich potenzieller Kunden, Mitarbeiter, Bewerber für eine Anstellung, Berater, Lieferanten, Besucher, Webnutzer der Websites des Verantwortlichen usw.

5. DATENSCHUTZ-ORGANISATIONSMODELL DER EU-GRUPPE

Um die Maßnahmen im Bereich des Schutzes personenbezogener Daten innerhalb der Gruppe homogen zu gestalten, hat die EU-Gruppe beschlossen, das folgende Organisationsmodell zu übernehmen:

- **Corporate-Referent:** hat kurz gesagt die Aufgabe, die Angelegenheit auf der Ebene der gesamten UE-Gruppe zu koordinieren und allen innerhalb der EU-Gruppe ernannten Datenschutzreferenten fachliche Anleitung zu geben. Eine detaillierte Auflistung der

zugewiesenen Verantwortlichkeiten und Aufgaben ist in dem Dokument PRCY011 enthalten, Verfügbar im Intranet des Unternehmens;

- **Allgemeiner Referent**: Er hat kurz gesagt die Aufgabe, die Angelegenheit auf der Ebene des einzelnen Unternehmens, das ihn ernannt hat, in seiner Gesamtheit zu koordinieren und alle Funktionsansprechpartner, die innerhalb desselben Unternehmens ernannt werden können, fachlich anzuleiten. Einzelheiten zu den zugewiesenen Verantwortlichkeiten und Aufgaben sind in dem Dokument PRCY012 festgelegt, Verfügbar im Intranet des Unternehmens;
- **Funktionsreferent:** kurz gesagt, ist er für die Koordination der Angelegenheit auf der Ebene der ihm zugeordneten Unternehmensabteilung innerhalb des Unternehmens, das ihn ernannt hat, verantwortlich. Eine detaillierte Auflistung der zugewiesenen Verantwortlichkeiten und Aufgaben ist in dem Dokument PRCY013 enthalten, Verfügbar im Intranet des Unternehmens. Dieser Referent wird nur dann ernannt, wenn dies von dem allgemeinen Referenten als notwendig erachtet wird.

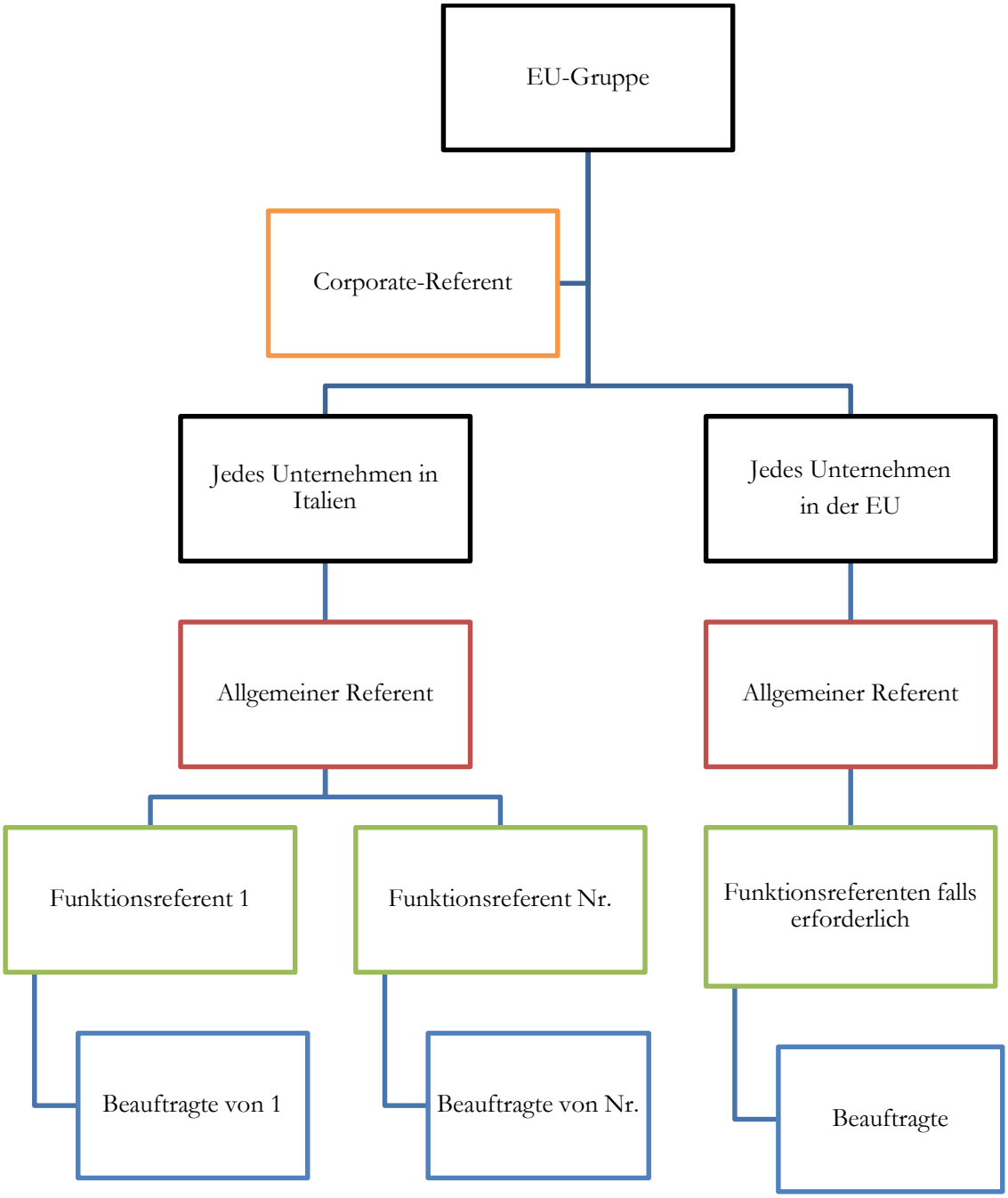
Eine aktuelle Liste aller ernannten Referenten ist unter PRCY015 zu finden.

- **Bevollmächtigter / Beauftragter**: ist die natürliche Person, die die Datenverarbeitungsvorgänge mit Hilfe von Computerwerkzeugen und / oder mit Hilfe von Papiermedien innerhalb der Unternehmensabteilung, der sie zugeordnet ist, durchführt.

  Jedes Unternehmen muss jeden seiner Mitarbeiter, der in Erfüllung seiner Aufgaben personenbezogene Daten verarbeitet, als Datenverarbeiter benennen. Die Ernennungsurkunde zum Beauftragten mit der Definition des Umfangs der zulässigen Verarbeitungen, der erteilten Anweisungen und der übertragenen Aufgaben ist unter PRCY014 zu finden.

6. EU-DATENSCHUTZORGANISATIONSSCHEMA

Basierend auf den obigen Ausführungen sieht das Organisationsschema für den Datenschutz wie folgt aus:



7. ANDERE BETEILIGTE PERSONEN

An der Verwaltung personenbezogener Daten können andere Personen beteiligt sein, einschließlich:

- **Verantwortlicher für die Datenverarbeitung**: wie bereits erwähnt handelt es sich um eine externe Person, die die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen durchführt. Eine solche Verarbeitung muss auf der Grundlage eines schriftlichen Vertrags erfolgen, in dem der geregelte Gegenstand, die Dauer der Verarbeitung, die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien der betroffenen Personen sowie die Pflichten und Rechte des für die Verarbeitung Verantwortlichen festgelegt

sind. Im EU-Kontext muss ein solcher Vertrag auch die wesentlichen Elemente enthalten, die in Artikel 28(3) der DSGVO vorgeschrieben sind.
Dienstleistungen, die typischerweise an einen externen Verantwortlichen ausgelagert werden können, sind z. B. die Gehaltsabrechnung, die Verwaltung der Website, der IT-Support usw.

- **DPO**: der Datenschutzbeauftragte (Data Protection Officer) ist eine von der DSGVO in Art. 37 ff. vorgesehene Figur, die ein Unternehmen ernennen muss, wenn:
  - die Haupttätigkeit des für die Datenverarbeitung Verantwortlichen oder des Auftragsverarbeiters aus Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und /oder ihrer Zwecke eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern; oder
  - die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Artikel 9 DSGVO oder von Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Artikel 10 DSGVO in größerem Umfang besteht.

  Seine Hauptaufgaben sind die Überwachung der Einhaltung der DSGVO, die Beratung des Unternehmens, die Überwachung des Betriebs, die Durchführung von Schulungen und die Sensibilisierung zu diesem Thema usw.

  Die Ernennung eines Datenschutzbeauftragten wurde für die Unternehmen nicht als notwendig erachtet, da angesichts der typischen Tätigkeit der Unternehmen, die keine Risiken im Bereich des Schutzes personenbezogener Daten mit sich bringt, angesichts der minimalen Verarbeitung personenbezogener Daten der betroffenen Personen, die mit Sicherheit nicht in großem Umfang stattfindet, und angesichts der Tatsache, dass die Verarbeitung besonderer Datenkategorien im Rahmen des Beschäftigungsverhältnisses keine Haupttätigkeit, sondern eine Nebentätigkeit darstellt (siehe WP29, Leitlinien für den Datenschutzbeauftragten, 2.1.2, S. 9), die oben genannten Voraussetzungen nicht gegeben sind.
  Wenn lokale Richtlinien oder Vorschriften die Ernennung eines Datenschutzbeauftragten für eines der Unternehmen erfordern (außer in Italien), muss dieser Umstand im Voraus an den Corporate-Referenten gemeldet werden.

- **Andere potenzielle Personen**: Lokale Vorschriften können die Notwendigkeit vorsehen, andere Personen zu identifizieren, die für den Schutz personenbezogener Daten relevant sind. Jedes Unternehmen ist verpflichtet zu prüfen, ob es lokale Vorschriften gibt, die ähnliche Verpflichtungen auferlegen.
  In Italien gibt es zum Beispiel die Figur des Systemadministrators, der eine natürliche Person ist, die mit der technischen Verwaltung des gesamten Informationssystems oder auch nur einer seiner Komponenten oder damit verbundenen Aktivitäten betraut ist. Diese Personen müssen eine spezielle Bezeichnung als Systemadministrator und spezifische Anweisungen erhalten.

8. ALLGEMEINE GRUNDSÄTZE

In Bezug auf die Verarbeitung personenbezogener Daten beabsichtigt die EU-Gruppe, alle am besten geeigneten technischen, organisatorischen und logistischen Maßnahmen zu ergreifen, um die wirksame Einhaltung der Garantien für den Schutz personenbezogener Daten zu gewährleisten.
Zu diesem Zweck müssen die Geschäftsprozesse und die Datenverarbeitungsvorgänge, die von den für die Verarbeitung beauftragten Mitarbeitern durchgeführt werden, den folgenden Grundsätzen entsprechen.

8.1. **Rechtmäßigkeit, Korrektheit und Transparenz**
Die Verarbeitung personenbezogener Daten darf nur dann erfolgen, wenn eine der gesetzlich vorgesehenen Voraussetzungen dies zulässt, der Betroffene davon Kenntnis hat und die Verarbeitung dem entspricht, was ihm gegenüber erklärt worden ist.

8.2. **Zweckbindung**
Personenbezogene Daten dürfen nur zu Zwecken verarbeitet werden, die der betroffenen Person mitgeteilt werden, und dürfen mit diesen Zwecken nicht unvereinbar sein.

8.3. **Minimierung**
Die Verwendung personenbezogener Daten muss auf ein Mindestmaß beschränkt werden. Wenn die Zwecke ohne die Verwendung personenbezogener Daten erreicht werden können, muss die Verarbeitung daher mit anonymen Daten erfolgen. Anonyme Daten sind Daten, die in keiner Weise mit einer identifizierten oder identifizierbaren betroffenen Person in Verbindung gebracht werden können. Insbesondere müssen personenbezogene Daten dem Zweck entsprechen, für den sie verarbeitet werden, dafür erheblich sein und sich auf das beschränken, was im Hinblick auf die Zwecke, für die sie verarbeitet werden, erforderlich ist.

8.4. **Genauigkeit**
Die verarbeiteten Daten müssen korrekt sein und auf dem neuesten Stand gehalten werden, und die betroffene Person muss die Möglichkeit haben, sie zu überprüfen und zu berichtigen.

8.5. **Begrenzung der Speicherung**
Die verarbeiteten personenbezogenen Daten dürfen nicht für unbestimmte Zeit aufbewahrt werden. Sie müssen gelöscht werden, sobald der Zweck erfüllt ist, daher muss jedes Unternehmen Aufbewahrungszeiten festlegen, die mit dem Zweck vereinbar sind und den örtlichen Vorschriften entsprechen.

8.6. **Integrität und Vertraulichkeit**
Jedes Unternehmen muss personenbezogene Daten so verarbeiten, dass eine angemessene Sicherheit und Vertraulichkeit gewährleistet ist, einschließlich der Verhinderung des unbefugten Zugriffs oder der Nutzung von personenbezogenen Daten und der für die Verarbeitung verwendeten Geräte.

8.7. **Rechenschaftspflicht**
Jedes Unternehmen muss die Einhaltung der oben genannten Prinzipien sicherstellen und muss in der Lage sein, diese Einhaltung nachzuweisen.

9. BETRIEBSVORSCHRIFTEN

In Anwendung der oben beschriebenen Prinzipien und der zusätzlichen Regeln, die in der DSGVO festgelegt sind, muss jedes Unternehmen in Übereinstimmung mit den folgenden Betriebsvorschriften arbeiten.

9.1. Verzeichnisse der Verarbeitungstätigkeiten.

Jedes Unternehmen muss durch seine Referenten Nachweise über die intern von den verschiedenen Unternehmensabteilungen durchgeführten elektronischen und manuellen Verarbeitungen führen. Jedes Unternehmen muss dieser Verpflichtung nachkommen, indem es die in Artikel 30 der DSGVO genannten Verzeichnisse der Verarbeitungstätigkeiten erstellt und sich dabei an die Anweisungen hält, die in jedem Land von den örtlichen Aufsichtsbehörden diesbezüglich erteilt werden.

Die Verantwortung dafür, dass jedes Unternehmen über die von der DSGVO vorgeschriebenen Verzeichnisse verfügt und dass diese ständig aktualisiert werden, liegt bei dem allgemeinen Referenten, der zu diesem Zweck ein spezifisches Verwaltungsverfahren festlegen muss, das die Verantwortlichkeiten und Aufgaben innerhalb des Unternehmens festlegt und, falls vorhanden, die Funktionsreferenten einbezieht.

In jedem Fall müssen die Verzeichnisse mindestens einmal pro Jahr aktualisiert werden.

9.2. **Auskunft und Datenerfassung (Transparenz und Korrektheit).**

In der Regel werden personenbezogene Daten direkt von den betroffenen Personen im Rahmen ihrer normalen Arbeitskontakte und bei der Ausübung der betrieblichen Tätigkeit des Unternehmens oder über die Website zur Verfügung gestellt, sie können aber auch von Dritten erworben werden. Mitarbeiter, die personenbezogene Daten einer betroffenen Person erheben, müssen bei der Erhebung der Daten sicherstellen, dass die betroffene Person angemessen über die Zwecke, für die die Daten erhoben und anschließend verarbeitet werden, informiert wird.

Zu diesem Zweck müssen sie das entsprechende, von dem Unternehmen erstellten „Auskunftsdokument“ vorlegen.

Die Auskunft ist immer fällig, auch wenn es nicht notwendig ist, die betroffene Person um ihre Zustimmung zur Verarbeitung ihrer Daten zu bitten.

Vorgänge, für die keine Auskunft erstellt wurde oder die in der Auskunft selbst nicht beschrieben sind, sind unzulässig und können daher nicht durchgeführt werden.

Der Auskunftshinweis muss „einmalig“ erfolgen und der ersten Datenerhebung bei einer betroffenen Person vorausgehen.

Eine neue Auskunft muss erstellt werden, wenn sich einige der in dem zuvor erstellten Bericht angegebenen Elemente ändern.

9.3. **Bedingungen für die Rechtmäßigkeit der Verarbeitung**

Für jeden in der Auskunft aufgeführten Zweck muss mindestens eine Rechtsgrundlage angegeben werden, die die Verarbeitung rechtmäßig macht.

Die Rechtsgrundlagen sind dieselben wie in Artikel 6 der DSGVO für „gewöhnliche" personenbezogene Daten angegeben, die, zusammenfassend, aus den folgenden Alternativen bestehen:

- Zustimmung
- Erfüllung eines Vertrags
- Erfüllung einer rechtlichen Verpflichtung
- Wahrung lebenswichtiger Interessen
- Aufgabe von öffentlichem Interesse
- Berechtigtes Interesse (sofern nicht die Rechte der betroffenen Person überwiegen)

Im Hinblick auf die Verarbeitung besonderer Datenkategorien sind die Rechtsgrundlagen in Artikel 9 der DSGVO und in Artikel 10 für strafrechtliche Daten festgelegt und restriktiver als für gewöhnliche Daten.

9.4. **Einwilligung der betroffenen Person (Rechtmäßigkeit).**

Unter den Rechtsgrundlagen der Rechtmäßigkeit wird die Einwilligung der betroffenen Person genannt. Die Einwilligung muss nicht eingeholt werden, wenn die Verarbeitung auf einer der anderen Bedingungen für die Rechtmäßigkeit beruht (wie im vorherigen Punkt erwähnt). Bestimmte Verarbeitungen bedürfen jedoch zwingend der Einwilligung als Voraussetzung für die Rechtmäßigkeit. Die Verarbeitungsvorgänge müssen der von der betroffenen Person als Reaktion auf die Auskunft erteilten Einwilligung entsprechen. Die Einwilligung muss von der betroffenen Person aus freien Stücken gegeben werden, darf nur als Reaktion auf eine entsprechende Auskunft eingeholt werden und muss nachweislich und eindeutig sein.
Ist die Einwilligung für die Verarbeitung erforderlich, darf diese nicht durchgeführt werden, wenn sie nicht eingeholt worden ist.

9.5. Datenzugriff und erlaubte Handlungen für das Personal.

Der Zugriff auf personenbezogenen Daten und die Durchführung von Verarbeitungstätigkeiten ist nur Personen gestattet, die ordnungsgemäß bevollmächtigt sind und entsprechende Anweisungen erhalten haben. Diese Auftragsverarbeiter dürfen nur auf die Daten zugreifen, die sie kennen „müssen". Die Daten dürfen ausschließlich zur Erfüllung der jeweils übertragenen Aufgaben und Pflichten verwendet werden.
Wie bereits zuvor erwähnt, wird darauf hingewiesen:

- Vorgänge, für die keine Auskunft vorliegt oder die in der Auskunft selbst nicht ausdrücklich erwähnt werden, dürfen nicht durchgeführt werden;
- es ist nicht erlaubt, Verarbeitungen durchzuführen, für die keine Einwilligung vorliegt, falls erforderlich.

9.6. **Zugang zu besonderen Datenkategorien und kriminellen Daten und Aktivitäten, die dem Personal erlaubt sind.**

Diese Daten dürfen nur von den Auftragsverarbeiter verarbeitet werden, wenn es strikt notwendig ist, für die Erfüllung ihrer Aufgaben unabdingbar ist und sie ausdrücklich dazu ermächtigt wurden.

Zusätzlich zu den zuvor beschriebenen Einschränkungen hinsichtlich der Notwendigkeit von Auskunft und einer eventuellen Zustimmung ist zu beachten, dass die Verarbeitung der Daten auch die Bedingungen und Einschränkungen der lokalen Vorschriften einhalten muss.
In Italien beispielsweise sind die Bedingungen und Einschränkungen in den vom Datenschutzbeauftragten herausgegebenen allgemeinen Genehmigungen festgelegt, die auf der Website des „Garante della Privacy" (www.garanteprivacy.it) zu finden sind.
Daher ist es nicht erlaubt, Verarbeitungen durchzuführen, die nicht den örtlichen Vorschriften entsprechen.

9.7. **Sicherheitsmaßnahmen.**
Alle mit der Auftragsverarbeiter sind verpflichtet, die vom Unternehmen festgelegten Sicherheitsvorschriften einzuhalten, deren Nichteinhaltung erhebliche rechtliche Konsequenzen, manchmal sogar strafrechtlicher Art, nach sich ziehen kann. Die Einhaltung bestimmter Sicherheitsmaßnahmen hängt ausschließlich vom Verhalten der Auftragsverarbeiter ab.

9.8. **Weitergabe von Daten und Übermittlung von Daten an Dritte.**
Personenbezogene Daten dürfen innerhalb der Unternehmen der EU-Gruppe regelmäßig an diejenigen mit der Verarbeitung betrauten Personen weitergegeben werden, die diese Daten zu Arbeitszwecken kennen müssen (*need to know*) und die diesbezüglichen Anweisungen erhalten haben. Sie dürfen jedoch nicht an Dritte außerhalb des EU-Konzerns übermittelt - oder jedenfalls zugänglich gemacht - werden, es sei denn, es liegt einer der folgenden Fälle vor:

- die Übermittlung an Dritten ist erforderlich, um eine gesetzliche Verpflichtung oder eine behördliche Anordnung zu erfüllen;
- die Übermittlung an Dritten ist erforderlich, um Verpflichtungen aus einem Vertrag mit der betroffenen Person, auf die sich die personenbezogenen Daten zurückführen lassen, zu erfüllen;
- wenn der Dritte als Verantwortlicher für die Datenverarbeitung gemäß Art. 28 DSGVO ernannt wurde und die Daten für die Erbringung der ausgelagerten Dienstleistung erforderlich sind;
- die Person, zu der die Daten zurückverfolgt werden können, hat ihre ausdrückliche Zustimmung zur Übermittlung der betreffenden Daten an diesen Dritten gegeben.

Die Übermittlung von Daten an Dritte aus anderen als den oben genannten Gründen bedarf der schriftlichen Zustimmung des allgemeinen Referenten des Unternehmens.

In jedem Fall gehört es nicht zur Politik der EU-Gruppe, aus welchem Grund und zu welchem Zweck auch immer, die Weitergabe von Listen, Verzeichnissen oder Adressen in Form einer Kommerzialisierung von personenbezogenen Daten vorzunehmen.

9.9. **Neue Verarbeitung und Verarbeitung mit hohen Risiken.**
Ohne vorherige Genehmigung dürfen keine neuen Verarbeitungsvorgänge begonnen werden, die ein hohes Risiko darstellen, wie es in der Richtlinie des Unternehmens bezüglich der Bewertung der Auswirkungen der Verarbeitungsvorgänge auf den Schutz personenbezogener Daten (Datenschutz-Folgenabschätzung oder **DSFA**) definiert und geregelt ist. Die wichtigsten zu

bewertenden Elemente, die ein hohes Risiko für die betroffenen Personen darstellen können, sind folgende:

- Bewertung, Einstufung oder Erstellung von Profilen
- Automatisierte Entscheidungsfindung, die rechtliche Auswirkungen hat oder natürliche Personen in ähnlicher Weise erheblich beeinträchtigt
- Systematische Überwachung
- Verarbeitung besonderer Kategorien von Daten
- Großflächige Datenverarbeitung
- Vergleichen oder Kombinieren von Datensätzen
- Verarbeitung von Daten über schutzbedürftige Personen
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
- Verarbeitung, die als solche „die betroffenen Personen daran hindert, ein Recht auszuüben oder eine Dienstleistung oder einen Vertrag in Anspruch zu nehmen"

Außer diesen Elementen könnten lokale Vorschriften zusätzliche Risikofälle oder Fälle vorsehen, in denen eine DSFA obligatorisch ist. In Italien hat der Datenschutzbeauftragte festgelegt, dass die DSFA in einer Reihe von Fällen obligatorisch ist, z. B. bei der nicht anlassbezogenen Verarbeitung von Daten über schutzbedürftige Personen, der systematischen Verarbeitung biometrischer Daten usw.

9.10. **Verletzung personenbezogener Daten (Data breach)**

Eine Verletzung des Schutzes personenbezogener Daten ist definiert als „eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Verbreitung oder zum Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt" (im Folgenden auch als „**Datenverletzung**", Data Breach, bezeichnet).

Im Falle einer Datenverletzung ist es zwingend erforderlich, die Aufsichtsbehörde (lokaler Garant) innerhalb von 72 Stunden nach Bekanntwerden der Verletzung zu informieren.

Die EU-Gruppe hat eine Richtlinie für den Umgang mit Datenschutzverletzungen verabschiedet, die allen Verantwortlichen bekannt und zugänglich sein muss, die sie bei Eintreten der beschriebenen Situation unverzüglich an ihren eigenen Funktionsreferenten oder, falls dieser nicht anwesend ist, an den allgemeinen Referenten mitteilen müssen, um die Meldebedingungen einzuhalten.

9.11. **Privacy by Design und Privacy by Default**

Die EU-Gruppe hat eine „Privacy by Design"- und eine „Privacy by Default"-Richtlinie verabschiedet, die bei der Entwicklung neuer Anwendungen und neuer Verarbeitungsvorgänge befolgt werden muss und die allen Mitarbeitern, die an der Konzeption und Entwicklung solcher Anwendungen und Verarbeitungsvorgänge beteiligt sind, zur Kenntnis gebracht werden muss.

9.12. **Verwaltung der Rechte betroffener Personen**

Die DSGVO erkennt die folgenden Rechte der betroffenen Personen an:

- Recht auf Zugang zu ihren persönlichen Daten (Art. 15);

- Recht auf Berichtigung (Art. 16);
- Recht auf Löschung (Recht auf Vergessenwerden) (Art. 17);
- Recht auf Einschränkung der Verarbeitung (Art. 18);
- Recht auf Datenübertragbarkeit (Art. 20);
- Recht auf Widerspruch (Art. 21);
- Recht auf Widerspruch gegen eine Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung beruht (Art. 22);
- Recht auf jederzeitigen Widerruf der erteilten Einwilligung, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird (Art. 7.3);

Die EU-Gruppe hat eine Richtlinie für die Verwaltung von Anträgen auf Ausübung der oben genannten Rechte verabschiedet, die ihren Inhalt veranschaulicht. Die Richtlinie muss jeder Person, die am Prozess der Verwaltung solcher Anfragen beteiligt ist, bekannt und zugänglich sein. Es wird darauf hingewiesen, dass bei nicht ordnungsgemäßer Bearbeitung der in der Richtlinie genannten Anfragen der Betroffene das Recht hat, eine Beschwerde beim Datenschutzbeauftragten einzureichen oder rechtliche Schritte zum Schutz seiner Rechte einzuleiten.

10. SCHULUNGEN

Die DSGVO schreibt die Verpflichtung vor, die Auftragsverarbeiter auf die mit der Verarbeitung personenbezogener Daten verbundenen Risiken hinzuweisen. Jedes Unternehmen muss daher sicherstellen, dass die Auftragsverarbeiter durch eine der Aufgabe angemessene Schulung dafür sensibilisiert werden.
Die Schulung kann keine einmalige Veranstaltung sein, sondern muss in regelmäßigen Abständen wiederholt werden, insbesondere bei gesetzlichen Änderungen oder neuen Auslegungsrichtlinien.
Für Schulungszwecke können auch Dokumente und Präsentationen zur Veranschaulichung der wichtigsten Aspekte der Vorschriften, E-Learning-Programme, Unterrichtsstunden und Informationsveranstaltungen usw. zur Verfügung gestellt werden.

Solche Schulungsaktivitäten müssen dokumentiert werden (gemäß dem Prinzip der Rechenschaftspflicht). Jeder Mitarbeiter ist verpflichtet, sein Wissen über das Gebiet zu vertiefen, um in voller Übereinstimmung mit den Vorschriften, dieser Richtlinie und den zum Thema Datenverarbeitung erteilten Anweisungen zu arbeiten. Weiterer Schulungsbedarf muss den Funktionsreferenten (oder, in deren Abwesenheit, dem allgemeinen Referenten) gemeldet werden, der die Anfragen weiterverfolgt.

11. REGELMÄSSIGE ÜBERPRÜFUNGEN

Jedes Unternehmen veranlasst in Erfüllung seiner Pflichten gemäß der DSGVO regelmäßige Überprüfungen, auch durch die intern benannten Referenten (allgemeiner Referent und etwaige Funktionsreferenten), hinsichtlich der Einhaltung der Bestimmungen der DSGVO, der lokalen Vorschriften und der EU-Konzernrichtlinien sowie der erteilten Anweisungen zur Datenverarbeitung.
Die Überprüfungen müssen dokumentiert werden. Die Auftragsverarbeiter werden um größtmögliche Kooperation gebeten, um die Überprüfungen zu erleichtern.

12. SANKTIONEN

Ein teilweiser oder vollständiger Verstoß gegen die Bestimmungen der Datenschutzvorschriften kann straf-, zivil- und verwaltungsrechtliche Sanktionen nach sich ziehen, die für eine rechtswidrige oder nicht mit den Vorschriften konforme Verarbeitung vorgesehen sind.
In den schwerwiegendsten Fällen wird darauf hingewiesen, dass das gemäß Artikel 83 Absatz 5 der DSGVO anwendbare Bußgeld bis zu 20.000.000 Euro bzw. für Unternehmen bis zu 4 % des gesamten weltweiten Jahresumsatzes des Vorjahres betragen kann, je nachdem, welcher Betrag höher ist.

Rechtswidriges Verhalten oder Verhalten, das nicht im Einklang mit dieser Richtlinie, den Richtlinien der EU-Gruppe und den zur Verarbeitung personenbezogener Daten erlassenen Anweisungen steht, kann disziplinarische Maßnahmen nach sich ziehen, die der Schwere des Sachverhalts entsprechen.

*** *** ***