LOYALTY PARTNER

Datenschutz-Handbuch für die deutschsprachigen Unternehmen der Loyalty Partner Gruppe

Version: 2.0
Stand: Februar 2019

LOYALTY PARTNER

Erstellungshinweise und Verteilerkreis:

Konzeption/ Erstellung durch:	Datenschutzbeauftragten
Weiterentwicklung durch:	Datenschutz-Manager
Beschlussfassung durch:	jeweilige Geschäftsführung
Verteilung an:	Geschäftsführung / Bereichsleiter / Abteilungsleiter
Durchgeführt von:	Datenschutz-Management

Freigegeben und für verbindlich erklärt

Unternehmen	Vertreten durch	Datum	Unterschrift
Loyalty Partner GmbH	Bernhard Brugger	27.02.19	
PAYBACK GmbH	Bernhard Brugger	27.02.19	
PAYBACK Austria GmbH	Walter Lukner	28.02.19	
Loyalty Partner Solutions GmbH	Alexander Glück	28.02.2019	

Historie

Version	Datum	Autor	Kommentar
Version 1.0	August 2011	Dr. Robert Selk, DSB	Erstfassung
Version 2.0	Februar 2019	Anna Rocke (DSM), in Abstimmung mit Dr. Robert Selk (DSB)	Allgemeine Überarbeitung aufgrund der DS-GVO

Inhalt

1. Vorwort

Der Datenschutz spielt in den Unternehmen der Loyalty Partner Gruppe („LP-Gruppe“) eine ganz wesentliche und zentrale Rolle. Die datenschutzrechtlichen Anforderungen sind vielfältig, sowohl betreffend der übergreifenden organisatorischen Datenschutz-Prozesse als auch im Umgang mit personenbezogenen Daten im Einzelfall.

Die LP-Gruppe hat sich daher entschlossen, die Beschreibung der Datenschutz-Organisation in dem hiesigen Datenschutz-Handbuch („DS-Handbuch“) festzuschreiben. In ihm werden die zu erreichenden Ziele vorgegeben, Verantwortlichkeiten sowie Befugnisse festgelegt und übergreifende Datenschutz-Prozesse definiert. Das Dokument ist als zentrales Dokument für den gesamten Datenschutz zu verstehen.

Neben Verarbeitungsverzeichnis und Datenschutzfolgenabschätzungen ist das DS-Handbuch ein zentraler Baustein zur Erfüllung der gesetzlichen Nachweispflichten.

Inhaltlich wurde sich bei der Erstellung des DS-Handbuchs an den Vorgaben der VdS-Richtlinien zur Umsetzung der DS-GVO VdS 10010 : 2017-12 (01) orientiert.

2. Allgemeines

2.1 Inhalte, Geltungsbereich und Aktualisierung des DS-Handbuchs

Das DS-Handbuch wurde von der Geschäftsführung beschlossen. Es gilt verbindlich für alle deutschsprachigen Unternehmen der LP-Gruppe, deren internen und externen Mitarbeiter und für jede Art der Verarbeitung von personenbezogenen Daten. Umfasst sind hiervon auch außerhalb der Geschäftsräume eingerichtete Arbeitsplätze, wie z. B. Heimarbeitsplätze.

Das DS-Handbuch

- definiert die Ziele und den Stellenwert des Datenschutzes in der LP-Gruppe,
- verpflichtet die Unternehmen, die rechtlichen Anforderungen des Datenschutzes umzusetzen,
- definiert sämtliche Positionen für den Datenschutzprozess und weist auf deren Aufgaben hin,
- erläutert das Vorgehen bei der Erstellung von Datenschutz-Vorgaben und
- weist auf die Konsequenzen ihrer Nichtbeachtung hin.

Bei neuen Gesetzen, Änderungen bestehender Gesetze und sonstiger Vorschriften sowie organisatorischen Änderungen werden die Inhalte des DS-Handbuchs entsprechend angepasst. Zudem wird das DS-Handbuch jährlich vom Datenschutzbeauftragten („DSB") auf Aktualität geprüft. Hierbei kann der DSB einzelne Fachverantwortliche des Unternehmens hinzuziehen.

Änderungen des DS-Handbuchs werden im Datenschutz-Lenkungskreis (siehe Kapitel 4.3) besprochen und treten nach Freigabe den Datenschutz-Lenkungskreis in Kraft. Das aktuelle DS-Handbuch steht allen Mitarbeitern im Intranet zur Verfügung.

2.2 Abgrenzung zur Informationssicherheit

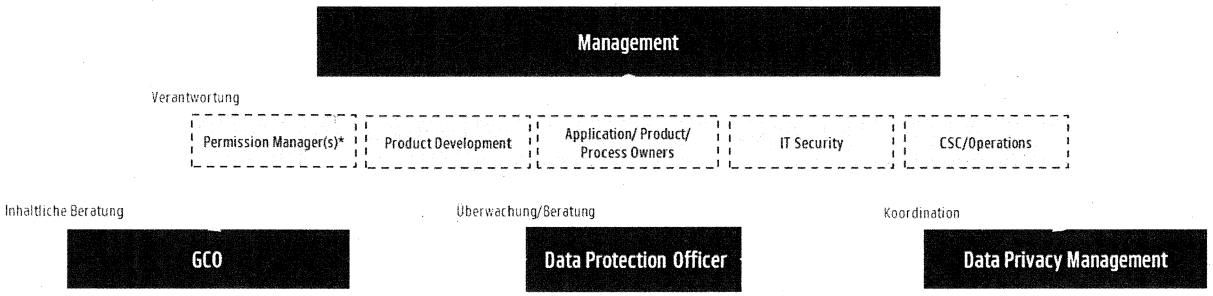
Die Unternehmen der LP-Gruppe unterscheiden gemäß BSI-Grundschutz-Katalog zwischen „Datenschutz" und „Informationssicherheit". Der Datenschutz legt auf Basis des jeweils gültigen Datenschutzrechts fest, unter welchen rechtlichen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen. Die Informationssicherheit steuert das Information Security Management System („ISMS"). Hierdurch werden die technisch-organisatorischen Maßnahmen („TOMs") geplant und umgesetzt, mit denen das Unternehmen die Verfügbarkeit, Vertraulichkeit und Integrität der zu verarbeitenden Daten (unabhängig vom Personenbezug) sicherstellt.

Datenschutz und Informationssicherheit ergänzen sich. Der Datenschutz betrachtet die Maßnahmen der Informationssicherheit als wesentliches Werkzeug, um Datenschutzziele zu erreichen. Umgekehrt betrachtet die Informationssicherheit den Datenschutz bei Verfahren, in denen personenbezogene Daten verarbeitet werden, als eine wesentliche Quelle für Anforderungen, die sie umzusetzen hat.

Aufgrund der hohen Bedeutung beider Bereiche gibt es jeweils eigenständige Dokumentationen und Beschreibungen, wenngleich aufeinander abgestimmt und aufbauend. Das hiesige DS-Handbuch betrifft alleine die datenschutzrechtliche Seite, die Informationssicherheit ist gesondert geregelt (vgl. die „LP Information Security Management Policy").

3. Die datenschutzrechtlichen Verantwortlichkeiten

3.1 Übersicht der Datenschutz-Organisation



3.2 Geschäftsführung

Die Gesamtverantwortung für das Thema „Datenschutz" liegt bei der Geschäftsführung des jeweiligen Unternehmens der LP-Gruppe. Ihr obliegen in diesem Zusammenhang die Wahrnehmung und Übernahme folgender Verantwortlichkeiten:

- Beschluss und Inkraftsetzen der Inhalte des DS-Handbuchs
- Bereitstellen der notwendigen technischen, finanziellen und personellen Ressourcen für den Datenschutz
- Einbetten des Datenschutzes in die Strukturen, Hierarchien und Arbeitsabläufe des Unternehmens

Soweit in diesem DS-Handbuch festgelegt, können bestimmte Aufgaben zum Datenschutz an andere Abteilungen und Personen delegiert werden. Die Verantwortung für die übertragenen Aufgaben verbleibt jedoch bei der Geschäftsführung, sodass diese die Erfüllung und das Ergebnis der delegierten Aufgaben regelmäßig überprüfen muss (Art. 24 Abs. 1 DS-GVO).

3.3 Datenschutz-Management („DSM")

Aufgrund der hohen Bedeutung und um die kontinuierliche Betreuung der datenschutzrechtlichen Themen sicherzustellen, wurde innerhalb des sog. General Counsel's Organisation („GCO") das „Datenschutz-Management" („DSM") als Einheit etabliert.

DSM koordiniert die datenschutzrechtlichen Prozesse und stellt die Erfüllung der Nachweis- und Dokumentationspflichten sicher. Zu den Aufgaben des DSM gehören insbesondere:

- Erarbeiten konkreter Verbesserungsvorschläge im Datenschutz
- On- und Offboarding sowie Auditierung von Auftragsverarbeitern
- Koordination von Zertifizierungen, z.B. durch den TÜV
- Erstellung, Überprüfung und ggf. Anpassung der Datenschutz-Dokumentation, insbesondere des DS-Handbuchs
- Review der von den Fachbereichen erstellten Handlungsanweisungen
- Untersuchen von datenschutzrelevanten Ereignissen
- Kontinuierliche Information des DSB über datenschutzrechtliche Risiken und Vorfälle
- Einleiten und Steuern von Sensibilisierungs- und Schulungsmaßnahmen
- Koordination der kontinuierliche Aktualisierung des Verarbeitungsverzeichnisse inkl. der rechtlichen Prüfung
- Koordination von Datenschutzfolgenabschätzungen

- Qualitätssicherung der Datenschutzhinweise hinsichtlich inhaltlicher Vollständigkeit und konsistenter Verwendung
- Monitoring der Bearbeitung eingehender Betroffenenanfragen
- Bearbeitung von Anfragen der Behörde sowie Meldung von Datenschutzverletzungen

In enger Abstimmung mit dem DSB berichtet das DSM in regelmäßigen Abständen, mindestens einmal jährlich, dem Management zu aktuellen Themen.

3.4 Rechtsabteilung

Die Rechtsabteilung ist ebenfalls Teil von GCO und hat neben der Bearbeitung allgemeiner juristischer Fragestellungen auch datenschutzrechtliche Aufgaben.

So berät sie die Geschäftsführung und die Fachbereiche aller Gesellschaften bei inhaltlichen Fragestellungen zu datenschutzrechtlichen Vorgaben. Hierzu zählen insbesondere:

- Prüfung von Rechtsfragen des Datenschutzes
- Ansprechpartner bei Projekten mit Datenschutz-Relevanz
- Vertragsgestaltung hinsichtlich datenschutzrechtlicher Themen
- Formulierung von Datenschutzhinweisen und Einwilligungstexten
- Enge Zusammenarbeit mit DSB und DSM

3.5 Datenschutzbeauftragter („DSB“)

Für jede LP-Gesellschaft ist schriftlich ein betrieblicher Datenschutzbeauftragte (kurz. „DSB“) benannt, welcher auch den zuständigen Aufsichtsbehörden für den Datenschutz gemeldet wurde. Der DSB kann in Personalunion für mehrere LP-Gesellschaften tätig sein.

Zugleich ist die Person des DSB gegenüber allen internen und externen Mitarbeitern bekannt zu machen, was auch gegenüber neuen Mitarbeitern gilt. Die Bekanntmachung erfolgt u.a. durch Veröffentlichung im Intranet.

Die Einbindung des DSB in datenschutzrechtlich relevante Vorgänge, Anfragen oder Prozesse, sei es auf ein Unternehmen der LP-Gruppe bezogen oder unternehmensübergreifend, erfolgt im Regelfall durch die Rechtsabteilung und/ oder das DSM, um Anfragen bündeln, koordinieren sowie gegebenenfalls selbst bearbeiten zu können. Gleichzeitig haben auch alle Mitarbeiter der LP-Gruppe direkt die Möglichkeit, sich direkt an den DSB zu wenden.

Der DSB berichtet unmittelbar der jeweiligen Geschäftsführung. Zugleich ist übergeordneter Ansprechpartner für den DSB in oberster Instanz einer der Geschäftsführer des jeweiligen Unternehmens.

Der DSB ist im Rahmen seiner Tätigkeit weisungsfrei und unabhängig, also neutral hinsichtlich der Unternehmensinteressen auf der einen Seite und den Betroffeneninteressen auf der anderen Seite. Insofern stellt die jeweilige Geschäftsführung sicher, dass der DSB bei der Erfüllung seiner Aufgaben keine Anweisung bezüglich der Ausführung dieser Aufgaben erhält, insbesondere dadurch, indem sie dies dem Management, Führungskräften und Mitarbeitern kommuniziert.

Der DSB darf von dem jeweiligen LP Unternehmen wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Es gelten ferner die gesetzlichen Regelungen der Art. 37 ff DS-GVO sowie § 38 BDSG iVm § 6 Abs. 4, 5 S. 2 und Abs. 6 BDSG.

Gemäß Art. 39 DS-GVO nimmt der DSB folgende Verantwortlichkeiten wahr:

- Beraten bei der Durchführung der Datenschutzfolgenabschätzungen (DSFA)
- Jährliches Berichten an das Topmanagement über den aktuellen Stand des Datenschutzes im Unternehmen, insbesondere über Risiken und datenschutzrelevante Vorfälle
- Wahrnehmen der Rolle des zentralen Ansprechpartners für Belange des Datenschutzes für betroffene Personen, das Unternehmen und dessen Beschäftigte sowie für die Aufsichtsbehörde
- Unterrichten und Beraten der Geschäftsführung hinsichtlich der geltenden Datenschutzvorschriften
- Regelmäßige Schulung der Mitarbeiter
- Überwachen der Einhaltung der geltenden Datenschutzvorschriften
- Beratung bei Projekten mit Auswirkungen auf den Datenschutz, sowie bei der Einführung neuer Software und IT-Systeme, um sicherzustellen, dass datenschutzrechtliche Aspekte ausreichend beachtet werden

3.6 Mitarbeiter und deren Vorgesetzte

Alle Mitarbeiter müssen die sie selbst oder ihre Tätigkeit betreffenden Maßnahmen und Regelungen zum Datenschutz einhalten.

Mitarbeiter müssen Datenschutzvorfälle unverzüglich der Rechtsabteilung und/ oder dem DSB melden. Hierbei gilt der Grundsatz, dass im Zweifelsfalle vorzugsweise zu oft als zu wenig eine solche Meldung erfolgen soll.

Die Vorgesetzten tragen die Verantwortung für ihre Mitarbeiter und müssen sicherstellen, dass die erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz in Bezug auf die ihnen unterstellten Mitarbeiter umgesetzt sind. Hierzu gehören beispielsweise entsprechende Sensibilisierungsmaßnahmen, Schulungen und Zugriffsbeschränkungen.

3.7 Gesonderte Verantwortlichkeiten

Prozess-, Applikations- und Produktverantwortliche sind dazu verpflichtet, datenschutzrelevante Prozesse proaktiv im Verarbeitungsverzeichnis zu dokumentieren und die Aktualität der Dokumentation sicherzustellen. Zudem sind sie für die Einhaltung der datenschutzrechtlichen Vorgaben in ihrem Zuständigkeitsbereich verantwortlich. Gleiches gilt für Projektverantwortliche.

4. Kontrollen und Berichtswesen

4.1 Kontrollen zur Einhaltung der datenschutzrechtlichen Vorschriften

Die Definition übergeordneten Datenschutz-Steuerprozesse ist von elementarer Bedeutung für die Nachhaltigkeit und Weiterentwicklung der getroffenen Maßnahmen. Denn es genügt nicht, Maßnahmen einmalig festzulegen und zu implementieren, sondern die Wirksamkeit der ergriffenen Maßnahmen ist regelmäßig zu überprüfen und gegebenenfalls sind Anpassungen vorzunehmen.

Hier werden über einen „Plan-Do-Check-Act"-Zyklus die Umsetzung der getroffenen Datenschutzmaßnahmen kontrolliert. Auch ist die Konformität neuer Verarbeitungstätigkeiten sowie Anpassungen aufgrund etwaiger gerichtlichen Entscheidungen zu überprüfen.

So untersuchen der DSM und der DSB in regelmäßigen Abständen stichprobenartig Geschäftsprozesse, in denen eine Verarbeitung personenbezogener Daten stattfindet. Hierbei wird überprüft, ob die datenschutzrechtlichen Vorgaben eingehalten werden und ob die Ergebnisse mit dem Verarbeitungsverzeichnis übereinstimmen.

Neben diesen internen Kontrollen ist in den LP Gesellschaften PAYBACK Deutschland und PAYBACK Austria ein jährliches externes Datenschutz-Audit, zum Beispiel durch den TÜV oder ähnliche Organisationen, vorgesehen.

4.2 Jahresbericht des DSB an die Geschäftsführung

Einmal jährlich erstellt das DSM gemeinsam mit dem DSB einen Datenschutz- und Tätigkeitsbericht. Dieser wird der Geschäftsführung in einem Termin vorgestellt sowie aktuelle Geschehnisse und Planungen sowie Maßnahmen besprochen.

Teilnehmer in diesem Termin sind neben dem DSB jeweils ein Mitglied der Geschäftsführung eines jeden Unternehmens der LP-Gruppe sowie jeweils ein Mitarbeiter des DSM, der Rechtsabteilung und der Informationssicherheit.

4.3 Regeltermine im Datenschutz-Lenkungskreis

Quartalsweise tagt ein sog. Datenschutz-Lenkungskreis. Das Meeting wird vom DSM organisiert. Weitere Teilnehmer sind der DSB sowie Vertreter der Rechtsabteilung, der Informationssicherheit sowie des Risk-Managements. Jeder Bereich stellt hier wichtige Themen vor und zudem werden aktuelle Vorgänge besprochen.

Darüber hinaus hat der Datenschutz-Lenkungskreis folgenden Funktionen:

- Abstimmung von gesellschaftsübergreifenden Datenschutz-Prozessen und Themen
- Aufarbeitung, Begleitung und Problemlösung von möglichen Datenschutz- und Kompromittierungsvorfällen,
- Funktion einer Schlichtungsstelle bei Meinungsverschiedenheiten in Zusammenhang mit Datenschutzmaßnahmen
- Unterstützung des DSM bei der Planung und Umsetzung von Datenschutzmaßnahmen.

4.4 Ad hoc Termine

Anlassbezogen werden je nach Thema in unterschiedlicher Besetzung ad hoc Termine zur Klärung datenschutzrechtlicher Fragestellungen einberufen.

5. Sensibilisierung und Schulung der Mitarbeiter

5.1 Sensibilisierung

Viele Gefährdungen entstehen aus Unkenntnis oder mangelndem Problembewusstsein, oder werden zumindest durch diese Faktoren verstärkt. Deshalb ist es notwendig, dass das Unternehmen über aktuelles Wissen in Bezug auf Datenschutz verfügt, die Mitarbeiter ihre Verantwortlichkeiten verstehen und sie für ihre Aufgaben geeignet und qualifiziert sind.

Daher wird bereits bei der Einstellung neuer Mitarbeiter auf deren Vertrauenswürdigkeit geachtet. Zudem werden bei der Einarbeitung diese DS-Handbuch sowie etwaige datenschutzrechtlichen Vorgaben und für die entsprechende Tätigkeit relevante Handlungsanweisungen bereitgestellt.

Besonderes Augenmerk wird bei der LP-Gruppe auf die persönliche Kommunikation gelegt. So werden in zahlreichen ad hoc Meetings die Fachbereichsvertreter intensiv durch den DSB, das DSM oder die Rechtsabteilung bzgl. der datenschutzrechtlichen Vorgaben sensibilisiert.

Sämtliche datenschutzrelevante Themen werden entsprechend vorstehendem Absatz in Zusammenarbeit mit dem DSB bekannt gemacht. Dies können sowohl Themen zum Mitarbeiter- wie auch Kundendatenschutz sein. Bekanntmachungen um Thema „Datenschutz" können durch Aushang, Rundschreiben und/ oder im Intranet, etc. erfolgen. Darüber hinaus ist die Position des jeweiligen DSB samt Namen und Erreichbarkeit allen Mitarbeitern fortlaufend zugänglich.

5.2 Schulung

Der DSB und/oder das DSM führen in der LP-Gruppe regelmäßig Datenschutzschulungen für die Mitarbeiter durch. Es soll mindestens eine Datenschutz-Schulung pro Jahr gehalten werden, je nach Bedarf auch mehrere Schulungen. Die Details sind im Datenschutz-Schulungs-Konzept festgelegt.

Wenn möglich, sollen sich Schulungen betreffend dem Datenschutz im Allgemeinen und speziellen Datenschutzschulungen zu bestimmten Themen bzw. für bestimmte Fachabteilungen abwechseln. Für Mitarbeiter der IT-Abteilungen und der Personalabteilung sowie den Beschäftigten weiterer datenschutzsensibler Bereiche werden beispielsweise spezifische datenschutzrechtliche Anforderungen definiert.

Neben den vorgenannten Schulungen sind datenschutzrechtlich relevante Punkte bei Einführungsveranstaltungen für neue Mitarbeiter, gegebenenfalls in den regelmäßigen Mitarbeitergesprächen und/oder Zielvereinbarungen auf allen Ebenen, aufzunehmen.

5.3 Verpflichtung auf Vertraulichkeit

Alle Mitarbeiter der LP-Gruppe (angestellte und selbstständige Mitarbeiter) werden im Rahmen ihrer Aufgabenstellung auf Vertraulichkeit gem. DS-GVO verpflichtet. Der Verpflichtungserklärung liegt ein Merkblatt zum Datenschutz bei.

Die Verpflichtung erfolgt bei Neuanstellung und wird in regelmäßigen Abständen und bei wesentlichen/relevanten Gesetzesänderungen erneuert. Dies liegt in der Verantwortung der Personalabteilung. Die unterzeichneten Original-Verpflichtungserklärungen werden in der Personalakte aufbewahrt.

6. Erstellung von sog. „Datenschutz-Vorgaben“

6.1 Zielsetzung

In der LP-Gruppe wird zwischen sog. „Datenschutz-Vorgaben“ und Handlungsanweisungen unterschieden:

- Datenschutz-Vorgaben („DS-Vorgaben“) sind solche, die für alle Verarbeitungen personenbezogener Daten gelten und für die gesamte Unternehmensgruppe verbindlich sind;
- Handlungsanweisung dagegen beschäftigten sich im Schwerpunkt mit *speziellen* Fallgestaltungen (etwa dem Auskunftsersuchen eines Betroffenen),

Sowohl DS-Vorgaben als auch Handlungsanweisungen sind Maßnahmen im Sinne von Art. 24 DS-GVO. Die DS-Vorgaben stehen zudem allen Mitarbeitern im Intranet zur Verfügung.

6.2 Inhaltliche Anforderungen an Datenschutz-Vorgaben und Handlungsanweisungen

Jede DS-Vorgabe und Handlungsanweisung muss folgende Anforderungen erfüllen:

- Sie enthält, für wen sie verbindlich ist.
- Sie begründet, warum sie erstellt wurde und legt fest, was mit ihr erreicht werden soll.
- Sie weist auf die Konsequenzen ihrer Nichtbeachtung hin.

DS-Vorgaben und Handlungsanweisungen können auf weitere mitgeltende Unterlagen verweisen.

6.3 Organisatorische Anforderungen an Datenschutz-Vorgaben und Handlungsanweisungen

Für DS-Vorgaben und Handlungsanweisungen gelten folgende Anforderungen:

- Bei der Erstellung und Anpassung müssen gesetzlichen, behördlichen und vertraglichen Anforderungen ermittelt und entsprechend umgesetzt werden.
- DS-Vorgaben und Handlungsanweisungen werden vom DSM unter Mitarbeit des DSB erstellt.
- Das DSM prüft jede DS-Vorgabe und Handlungsanweisung jährlich auf Aktualität und veröffentlicht ggf. eine Aktualisierung.
- DS-Vorgaben und Handlungsanweisungen müssen nach jeder Aktualisierung den Zielgruppen zeitnah bekannt gegeben werden. Dies muss in einer für die Zielgruppe zugänglichen und verständlichen Form geschehen, bspw. im Zuge einer Schulung.
- DS-Vorgabe und Handlungsanweisungen müssen im Unternehmen umgesetzt oder von der Geschäftsführung außer Kraft gesetzt werden.

7. Besonderheiten im Beschäftigtendatenschutz

7.1 Allgemeines

Die Personalabteilung der übergeordneten Loyalty Partner GmbH („Holding") stellt als zentrale Personalabteilung allen Unternehmen der LP-Gruppe ihre Dienstleistungen zur Verfügung.

Beschäftigte im Sinne dieser Regelungen sind neben den in § 26 Abs. 8 BDSG genannten Personen auch Trainees, Praktikanten und Werkstudenten.

Die Regelungen dieser Ziffer sind zwischen den einzelnen Unternehmen und der Holding als Betreiberin der zentralen Personalabteilung, ebenso wie zwischen allen Beschäftigten eines Unternehmens der LP-Gruppe und deren jeweiligen Arbeitgeber rechtsverbindlich. Dies gilt insbesondere für die den Beschäftigten direkt zustehenden Rechte.

7.2 Transparenz des unternehmensübergreifenden Bezuges

Den Beschäftigten ist bei Neueinstellung von dem jeweiligen Arbeitgeber ausreichend zu verdeutlichen, dass ihr Beschäftigungsverhältnis unternehmensübergreifenden Charakter aufweist, insbesondere, dass bei der Holding der LP-Gruppe eine zentrale Personalabteilung vorhanden ist, die die Personalverwaltung übernimmt, sowie ihnen die in der hiesigen Ziffer genannten Rechte direkt zustehen.

Gleiches gilt für Beschäftigte, die zwar mit einem Unternehmen der LP-Gruppe einen Beschäftigungsvertrag abgeschlossen haben, zeitweise aber bei einem anderen Unternehmen der LP-Gruppe eingesetzt werden (insbesondere Praktikanten, Azubis, Trainees oder Werkstudenten).

Die Hinweise können explizit in dem Beschäftigungsvertrag, einem Anhang hierzu oder in anderer Weise erfolgen. Da der unternehmensübergreifende Charakter vom jeweiligen Beschäftigten auch akzeptiert werden muss, soll die Aufnahme in den Beschäftigungsvertrag die Regel sein.

7.3 Besondere Datenschutz-Maßnahmen im Einzelnen

7.3.1 Arbeitgeber als Hauptansprechpartner

Der jeweilige Arbeitgeber bleibt für seine Beschäftigten in jedem Fall in allen Fragen des Datenschutzes für den Beschäftigten Hauptansprechpartner und ist vollumfänglich für die Einhaltung der datenschutzrechtlichen Vorgaben betreffend der personenbezogenen Daten dieses Beschäftigten zuständig und verantwortlich.

7.3.2 Geltendmachung Betroffenenrechte

Ein Beschäftigter kann sämtliche ihm zustehenden datenschutzrechtlichen Rechte und Ansprüche gegenüber seinem Arbeitgeber, wahlweise auch gegenüber der zentralen Personalabteilung und/ oder dasjenige Unternehmen geltend machen, bei dem er zeitweise eingesetzt wird. In letzteren Falle steht es ihm zu jeder Zeit frei, die weitere Kommunikation nur noch mit seinem Arbeitgeber weiterzuführen; hierüber hat er die zentrale Personalabteilung und seinen Arbeitgeber zu informieren.

7.3.3 Zweckbindung/ Keine Datenweitergabe außerhalb der Personalbearbeitung

Die zentrale Personalabteilung darf Personaldaten von Beschäftigten, die nicht bei der Holding angestellt sind, nur zum Zwecke der Begründung, Durchführung und Abwicklung des jeweiligen Beschäftigungsverhältnisses zwischen dem Beschäftigten und dessen Arbeitgeber erheben, verarbeiten oder nutzen.

Sie darf Personaldaten von „fremden" Beschäftigten nicht weitergeben/ Einsicht gewähren

- an andere Abteilungen oder Personen in der Holding,
- an andere Unternehmen der LP-Gruppe,
- andere Abteilungen/ andere Personen als den Personalverantwortlichen des jeweiligen Arbeitgebers.

Vorstehende Einschränkung gilt nicht, wenn für eine abweichende Datenweitergabe eine gesetzliche Erlaubnis besteht oder eine wirksame Einwilligung des betroffenen Beschäftigten vorliegt.

Vorstehendes gilt auch für die Unternehmen, die Personaldaten eines Beschäftigten erhalten, der nicht bei diesem Unternehmen angestellt ist, sondern dort nur zeitweise eingesetzt wird.

7.3.4 Hinweispflicht bei Weitergabe von Personaldaten an empfangendes Unternehmen

Das Personaldaten übermittelnde Unternehmen

- das empfangende Unternehmen über die Zwecke zu unterrichten, zu denen es selbst die Personaldaten erhoben hat, ebenso wie darüber, dass das empfangende Unternehmen die Personaldaten nicht zu anderen Zwecken verwenden darf.
- darf nur solche Personaldaten übermitteln, die erforderlich sind, dass das empfangende Unternehmen die ihm insofern obliegenden Tätigkeiten erfüllen kann
- darf das empfangende Unternehmen betreffend der übermittelten Personaldaten nicht mit einem „mehr" im Verhältnis zu dem beauftragen, was dem versendenden Unternehmen mit diesen Daten erlaubt ist.

Bezüglich der Personaldaten ist bei einer Übermittlung der Verarbeitungszweck für das Empfängerunternehmen stets auf die Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses begrenzt. Das datenempfangende Unternehmen darf ihm überlassene Personaldaten nicht für andere Zwecke verwenden.

7.3.5 Technisch-organisatorische Maßnahmen

Sowohl die einzelnen Unternehmen wie auch die Holding als Betreiberin der zentralen Personalabteilung haben sicherzustellen, dass betreffend der Personaldaten, insbesondere Personalakten die Anforderungen an technische und organisatorische Anforderungen nach Art. 25 und Art. 32 DS-GVO ausreichend umgesetzt und eingehalten werden.

Dazu gehört insbesondere eine strikte Trennung der Personalakten nach den einzelnen Unternehmen sowie organisatorische Vorkehrungen zur Absicherung vor unberechtigter Datenweitergabe oder Kenntnisnahme

Soweit Personaldaten an die zentrale Personalabteilung oder von einem Unternehmen betreffend eines zeitweise anderen Einsatzes eines Beschäftigten an ein anderes Unternehmen weiter- oder jeweils zurückgegeben werden, hat dies in ausreichend sicherer Form zu erfolgen. Physikalische Dokumente sind in verschlossenen Umschlägen zu transportieren, elektronische Dokumente verschlüsselt zu versenden.

Februar 2019

Loyalty Partner GmbH
PAYBACK GmbH
PAYBACK Austria GmbH
Loyalty Partner Solutions GmbH