1. Geltungsbereich und Inhalt dieser Regelungen

Die Regelungen dieses Dokuments gelten für alle Externen, also solche, die nicht bei uns angestellt oder über eine Arbeitnehmerüberlassung bei der PAYBACK Group tätig sind.
Soweit Externe Zugriff auf die IT-Systeme der PAYBACK Group (darunter verstehen wir sämtliche unserer Hard-, aber auch Software, wie z.B. PCs, Notebooks, Router, Betriebssysteme, Browser, Kommunikationssoftware, etc., sowie durch uns bereitgestellte Dienste, z.B. Cloud-Services und Cloud-Speicher) haben, hat der Externe die nachfolgenden Regelungen einzuhalten. Diese sind bereits Vertragsbestandteil, bzw. werden es spätestens dann, wenn sie dem Externen ausgehändigt wurden und dieser sodann im Rahmen seiner Auftragsausführung unsere IT nutzt.
Die hiesigen Regelungen ersetzen alle bisherigen Regelungen zur Nutzung unserer IT-Systeme. Soweit für den Umgang und die Nutzung spezieller IT-Systeme und -Dienste eigene Regelungen gelten, sind diese vorrangig.

2. Privatnutzung

Die private Nutzung unserer IT-Systeme ist nicht gestattet.
Ausgenommen hiervon ist die private Nutzung des Gäste WLANs mit einem eigenen Gerät.

3. Datenklassifizierung

Daten und Informationen werden in der PAYBACK Group wie in Anlage 1 „Data Handling Guide" beschrieben klassifiziert. Klassifizieren Sie die von Ihnen erstellten Informationen und Dateien entsprechend und informieren Sie Ihren vertraglich benannten Ansprechpartner. Weitere verbindliche Regelungen und Details zu diesem Thema befinden sich in der **Anlage 1** „Data Handling Guide".

4. Speicherung von Daten

Das Speichern privater und persönlicher Daten auf unseren IT-Systemen ist untersagt. Dienstliche Daten sind ausschließlich in den IT-Systemen der PAYBACK Group zu speichern. Sofern das temporäre Speichern von Daten im Rahmen der Auftragserfüllung auf Clientgeräten erforderlich ist, sind diese Daten regelmäßig, mindestens jedoch einmal pro Woche, auch auf einem zentralen IT-System, aber nicht OneDrive, abzulegen.

5. Cloud-Services und Cloud-Speicher

Es dürfen ausschließlich von der PAYBACK Group bereitgestellte Cloud-Services und Cloud-Speicher genutzt werden.

6. Allgemeine Regelungen

Soweit Sie Zugriff auf unsere IT-Systeme haben, dürfen diese in keinem Fall in einer Weise oder zu Zwecken verwendet werden, durch die die gesetzliche Bestimmungen verletzt werden, die Rechte von uns oder Dritter verletzt werden, die Vertraulichkeit der im Zusammenhang mit uns stehenden Daten oder Informationen in Frage gestellt oder verletzt wird, unser betrieblicher Ablauf gestört wird, die Verfügbarkeit unserer IT-Systeme beeinträchtigt wird, die interne Bestimmungen verletzt werden, einschließlich der Regelungen des hiesigen Dokuments, unser Ruf geschädigt wird oder zusätzliche Kosten für uns entstehen.
Unzulässig ist insbesondere folgende Nutzung unserer IT-Systeme:

- der Besuch von Websites, deren Besuch durch uns aufgrund einer akuten Schädlingsgefahr, wie Viren oder Trojaner, untersagt wurde
- das Ansehen, Verfassen, Herunterladen, Speichern oder Weiterleiten von illegalen oder anstößigen Inhalten, der Aufruf von Websites mit ungesetzlichen, z.B. verleumderischen, obszönen, rassistischen, sexistischen oder gewaltverherrlichenden Inhalten
- das Herunterladen und die Installation von Software aus dem Internet (z.B. MP3, Programme, Spiele, Treiber), siehe dazu auch Ziffer 9.
- Vertrauliche Informationen (LP-Secret und LP-Restricted inklusive Sublabels), sind ausschließlich verschlüsselt (z.B. über das Tool MOVEit) auszutauschen. Entsprechend klassifizierte Dokumente werden automatisiert verschlüsselt.

7. Regelungen zur Nutzung von E-Mail

1. Bei Nutzung unseres E-Mail-Systems

Wenn Sie eine E-Mail-Adresse von uns erhalten, dann gelten für die Nutzung der E-Mail-Adresse folgende Regelungen:

a) Ihre von uns zugeteilte E-Mail-Adresse ist mit dem Zusatz „_ext" (Beispiel: max.mustermann_ext@payback.net) versehen.
b) Sie müssen sicherstellen, dass auch in der Unterschriftszeile/ Signatur klargestellt ist, dass es sich bei Ihnen um einen Externen handelt.
c) Alle über unser E-Mail-System ein- und ausgehende E-Mails werden grundsätzlich in einem Archivsystem archiviert. Dies ist notwendig, um gesetzliche Aufbewahrungsfristen zu erfüllen. Sie haben daher keinen Zugriff darauf.
d) Die Nutzung der E-Mail-Adresse und des E-Mail-Systems darf ausschließlich insofern erfolgen, wie zur Durchführung Ihrer Tätigkeit für uns im Rahmen des Auftrags erforderlich. Deshalb ist beispielsweise eine private Nutzung verboten.
e) Jede auf unserem E-Mail-System ein- und ausgehende E-Mail wird automatisch auf Schadsoftware, Werbung und Betrugsversuche hin überprüft. E-Mails auf die bestimmte, regelmäßig angepasste, Kriterien zutreffen, werden automatisiert abgewiesen und nicht an Sie zugestellt. Über E-Mails, die lediglich als Verdachtsfälle eingestuft werden, werden sie informiert. Diese können unter Verwendung des Selbst-Services freigegeben werden. Generell dürfen nur E-Mails freigegeben werden, wenn es sich hierbei um auftragsbezogene, unbeschädigte und nicht kompromittierende Daten und Informationen handelt.

2. Bei Nutzung eigener E-Mail-Adressen und/ oder IT-Systeme

Soweit Sie für Ihre Tätigkeit für uns Ihre eigene E-Mail-Adresse und/ oder E-Mail-System nutzen bzw. die Ihres Arbeitgebers, dürfen Sie keinerlei Daten und Informationen von uns darüber versenden, wenn Sie nicht ausdrücklich eine schriftliche vorherige Zustimmung von Ihrem im Vertrag genannten Ansprechpartner erhalten haben.

8. Umgang mit unseren IT-Geräten

Soweit Sie ein IT-Gerät von uns zur Erfüllung Ihrer Auftragstätigkeit erhalten, gilt Folgendes:

- Verhindern Sie den Verlust (z.B. Diebstahl) Ihrer IT durch entsprechendes Verhalten. In der **Anlage 3** findest Du weitere Hinweise.
- Jegliche physische Veränderung an unseren IT-Geräten dürfen nur durch die IT der PAYBACK Group erfolgen und dürfen nicht von Ihnen selbst vorgenommen werden.
- Unsere Geräte dürfen nicht getauscht werden, weder mit anderen Externen noch mit internen Mitarbeitern. Jede Änderung der Zuordnung von Personen zu unseren Geräten erfolgt ausschließlich durch unsere IT.
- Es dürfen nur Geräte der PAYBACK Group im Netzwerk eingesetzt werden, welche von unserer IT zur Benutzung freigegeben sind.
- Geräte müssen, sobald sie nicht mehr benötigt werden (Beendigung der Beauftragung, entfallen des dienstlichen Zwecks) bei der IT zurückgegeben werden.

9. Umgang mit Software

Es dürfen aus Sicherheits- und Lizenzgründen auf unserer IT nur Software, Programme und Libraries verwendet werden, die von der PAYBACK Group freigegeben sind. Freigegebene Software und Programme sind über die automatische Softwareverteilung verfügbar. Damit ist es unzulässig, selbst irgendwelche Software herunterzuladen, zu installieren, auszuführen und/ oder zu nutzen, es sei denn die IT erteilt Ihnen hierfür ausdrücklich die Erlaubnis. Dies gilt unabhängig vom Berechtigungslevel, den Sie im Betriebssystem ihres Geräts haben. Dieses Verbot gilt auch für Programme, die nicht extra installiert werden müssen, wie etwa Browser-Plugins. Sie dürfen Software, Programme und Libraries nicht verändern oder löschen, dies ist vielmehr der IT vorbehalten.
Eine Vervielfältigung (z.B. Kopieren oder Installation auf anderen Geräten) der von uns überlassenen Software ist grundsätzlich untersagt. Dies gilt ebenso für die Übertragung und Installation auf firmenfremde Hardware.

10. Kontrollen der Einhaltung der hiesigen Regelungen/ Personenbezogene Daten und Datenschutz

Bei der Nutzung unserer IT-Systeme fallen verschiedene personenbezogene Daten von Ihnen an, etwa beim Login, dem Passwort-Wechsel, dem Versand von E-Mails oder Nutzung des Internets. Eine Reihe von Daten werden bei einer Nutzung des Internets protokolliert, wie insbesondere: Die IP-Adressen des Quell- und Zielrechners, die URL des Zielsystems, der Zeitpunkt des Verbindungsaufbaus und -endes, die Verbindungsdauer und der Benutzername. Bei einer E-Mail-Nutzung etwa werden Absender und Empfänger, Zeitpunkt, Länge, etc. erfasst.
Diese Daten werden zum Zwecke verwendet, die jeweiligen technischen Vorgänge abwickeln zu können, also etwa das Login durchzuführen, eine Internetverbindung herzustellen oder eine E-Mail zu versenden. Sie werden ferner zum Zweck der Datenschutzkontrolle, der IT-Sicherheit, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet. Dazu gehört auch die Prüfung, ob unsere Vorgaben zum Umgang mit der IT, insbesondere nach den hiesigen Regelungen, eingehalten werden.
Ein Zugriff auf diese Daten und deren Nutzung erfolgt ausschließlich durch die jeweils zugriffsberechtigten Personen. Bitte beachten Sie, dass Verstöße gegen die hiesigen Regelungen zu vertraglichen Konsequenzen führen können.
Weitere Informationen dazu finden Sie in den Datenschutzhinweisen für Externe. Für bestimmte IT-Systeme gibt es besondere Datenschutzhinweise auf die Sie bei der Nutzung gesondert hingewiesen werden. Dies gilt etwa für Microsoft 365: https://www.payback.group/de/m365-nutzungsbedingungen.

11. Regelungen bei Beendigung Deiner Tätigkeit für uns

Sie haben sämtliche Ihnen überlassene IT, am letzten Tag Ihrer Tätigkeit für uns, bei der IT zurückzugeben oder zurückzusenden. Sie haben sicherzustellen, dass alle betrieblich relevanten Daten auf einem zentralen IT-System gespeichert sind.

12. Ansprechpartner

Technischer Support der IT:
☏ +49 (0) 89 997 41 – 690
✉ IT-Nutzungsbedingungen@loyaltypartner.com

13. Anlagen

Anlage 1: Data Handling Guide

Anlage 2: Anleitung MOVEit

Anlage 3: Umgang mit IT-Geräten

Anlage 1: Data Handling Guide

1. Erstklassifizierung und Informationseigentümer

Führen Sie eine erste Klassifizierung der von Ihnen erstellten Daten und Informationen entsprechend des Data Handling Guides, Punkt 2, durch und informieren Sie Ihren vertraglich benannten Ansprechpartner darüber. Dieser ist auch der Informationseigentümer.

2. Klassifizierung

- Klassen: No-Business, 3rd Party Document, LP-Public, LP-Internal (Standard-Label), LP-Restricted*, LP-Secret*, (*inklusive Sublabel "– Company only" und "- External Collaboration"), LP- NoCloud.
- Re-Klassifizierung, wenn nötig: Anpassung der Kennzeichnung älterer Dokumentation nur, falls eine Re-Klassifizierung erfolgt.
- Jeder ist verantwortlich für den Schutz von Daten.

Beschreibung und Beispiele für die Klassifizierung von Daten:

No-Business	Für die erlaubte private Verwendung der Notebooks (nur interne Mitarbeiter).
3rd Party Document	Wird nur für die Klassifizierung von Dokumenten von Dritten verwendet. Beispiele: Verträge und Angebote von Dritten
LP-Public	Als "LP-Public" klassifizierte Daten und Informationen sind für die öffentliche Verwendung und Verteilung gedacht. Weder Inhalt noch Zusammenhang der als „LP-Public" klassifizierten Daten ist sensibel und bedarf keiner speziellen Absicherung. Beispiele: alle öffentlich über das Internet zugänglichen Dokumente wie veröffentlichte Pressemeldungen und Marketingmaterial oder der Inhalt unserer Webseiten.
LP-Internal	"LP-Internal" sind Daten und Informationen, die im Geschäftsalltag benötigt werden und sind zur Durchführung der täglichen Arbeitsabläufe gedacht. Als „Internal" klassifizierte Daten sind definiert als „nicht sensibel" aber „erfordern angemessene Kontrolle". Beispiele: alle Dokumente die weder als „LP-Restricted" noch „LP-Secret" klassifiziert sind. Dazu zählen beispielsweise Inhalte aus dem Intranet und Policies.
LP-Restricted (inklusive Sublabel)	Als "LP-Restricted" klassifizierte Daten und Informationen gelten alle personenbezogenen Daten und Informationen sowie solche Daten und Informationen, die bei Missbrauch zur Beeinträchtigung des Wettbewerbsvorteils unserer Firma, der Privatsphäre von Partnern, Kunden und Mitarbeitern oder des rechtlichen oder finanziellen Status unserer Firma führen. Beispiele: Kundendaten, Telefonlisten, Punktestände, LP-eigene Software, Berichte und Protokolle zur Produktentwicklung, Netzwerk- und Architekturpläne, Finanz- und Sicherheitsberichte.
LP-Secret (inklusive Sublabel)	Als "LP-Secret" klassifizierte Daten und Informationen können bei Missbrauch zu schwerwiegenden Beeinträchtigungen des Wettbewerbsvorteils unserer Firma oder des rechtlichen oder finanziellen Status unserer Firma führen. Beispiele: Authentifizierungsdaten wie Passwörter und PINs, Geschäftsstrategien, Pläne zur Marktentwicklung.
LP-NoCloud	Alle Dokumente, die nicht in M365 verarbeitet werden dürfen, müssen als LP-NoCloud eingestuft werden. Nur für LPS.

3. Akzeptable Nutzung / Dos & Don'ts bei der Nutzung von PAYBACK Group IT-Systemen

- Jeder Zugriff auf Daten und Informationen erfolgt nachweislich auf Basis des „Need to Know"-Prinzip
- Keine Veröffentlichung von Daten und Informationen an unautorisierte Personen. Der Versand von sensiblen Daten und Informationen außerhalb der PAYBACK Group muss verschlüsselt erfolgen. Hierfür wurden von der PAYBACK Group Lösungen zur Dateiverschlüsselung sowie zum sicheren und kontrollierten Dateiaustausch eingeführt.
- Alle Passwörter, die bei der PAYBACK Group verwendet werden, müssen folgende Anforderungen erfüllen:
  - Mindestens 8 Stellen
  - Komplexität: Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen
  - Keine Wiederholung der letzten 3 Passwörter
- Alle Daten und Informationen müssen, wenn sie nicht mehr benötigt werden, sicher entsorgt werden, z.B. durch Einwerfen in die Sicherheitsbehälter
- Melden Sie verlorene oder gestohlene IT-Geräte und Unterlagen unverzüglich dem im Vertrag genannten Ansprechpartner und der IT der PAYBACK Group (IT-Nutzungsbedingungen@loyaltypartner.com) (Siehe Anlage 3)

4. Meldung von Vorfällen

- Sicherheitsvorfall: jedes Ereignis das in der Folge zu unautorisierter oder unzweckmäßiger/m:
  a. Verwendung, Zugriff, Veränderung oder Bloßstellung von IT-Systemen oder Anwendungen der PAYBACK Group
  b. und /oder LP-Restricted oder LP-Secret Daten führt.
- Potenzielle oder bestätigte Sicherheitsvorfälle müssen von Ihnen unverzüglich nach der Entdeckung an das „Security Incident Report Program" unter Verwendung des Ticketsystems (helpdesk.loyaltypartner.com unter der Schaltfläche "Security") gemeldet werden. Sollte eine Ticketerstellung nicht möglich sein muss der Sicherheitsvorfall an die E-Mail-Adresse security@payback.net gemeldet werden.
- **Sie dürfen keinesfalls selbständig etwas bezüglich eines Sicherheitsvorfalles unternehmen und müssen den Sicherheitsvorfall mit höchster Vertraulichkeit (Klassifizieren der Daten und Informationen über den Vorfall mit LP-Secret) behandeln! Geben Sie bitte die Kontaktdaten und Ticketnummer des Vorfalls an Ihre IT-Sicherheitsorganisation weiter, um eine firmenübergreifende Abstimmung zu ermöglichen.**

Anlage 2: Anleitung MOVEit

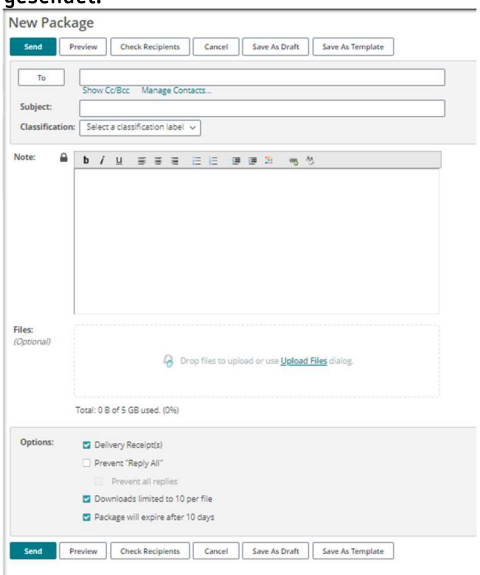
MOVEit® Software zur sicheren Dateiübertragung

MOVEit® ist eine interne Lösung zur Übermittlung von Daten an externe Partner. Bitte beachten Sie, dass es nicht als dauerhafte Speicherlösung für Dateien verwendet werden darf. Nach der Dateiübertragung, aber spätestens nach zwei Wochen, müssen die Dateien von MOVEit® gelöscht werden.
MOVEit® kann über die folgende URL aufgerufen werden: https://moveit.loyaltypartner.com
Interne Benutzer können sich mit ihrem Windows-Konto anmelden, nachdem sie Zugang erhalten haben. Die externe Partei erhält einen separaten Account. Es gibt zwei verschiedene Methoden für den Datentransfer, die MoveIT anbietet.

1. Ordner:
Dies ist die bevorzugte Methode für den regelmäßigen Datentransfer mit denselben externen Partnern.
Die Ordnerstruktur funktioniert so, wie Sie es von den Fileservern gewohnt sind. Die Struktur, Berechtigung und neue Benutzer müssen von Office & Datacenter Services eingerichtet werden.

Der Ordner kann von mehreren Personen genutzt werden, so dass dieser auch für Teams genutzt werden kann.
Da dies nicht als Ablage gedacht ist, versuchen Sie bitte die Ordnerstruktur so einfach wie möglich zu halten und beantragen Sie Unterordner nur dann, wenn diese zum Setzen von speziellen Berechtigungen benötigt werden.
Die Dateien müssen nach spätestens zwei Wochen gelöscht werden.
Um einen MOVEit®-Ordner anzufordern, öffnen Sie bitte ein Ticket: MOVEit Folder Access (https://pb-itsm.intra.loyaltypartner.com/servicedesk/customer/portal/2/create/385)

2. Pakete:
Dies ist die bevorzugte Methode für spontane Dateiübertragungen mit wechselnden Partnern.
Sie funktioniert wie das Versenden einer E-Mail mit dem Vorteil, dass die Dateien auf der MOVEit®-Plattform gespeichert werden. Diese Lösung kann NICHT von Teams verwendet werden - Sie können nur Ihre eigenen übertragenen Dateien sehen. Mit dieser Lösung können Sie neue Übertragungspartner hinzufügen, indem Sie sie einfach in das Feld "TO" eintragen. Es wird automatisch ein temporäres Konto erstellt und an den Empfänger gesendet.



Anlage 3: Umgang mit IT-Geräten

Der Verlust von IT-Geräten ist unverzüglich in schriftlicher Form:

- dem Helpdesk (IT-Nutzungsbedingungen@loyaltypartner.com)
- sowie Deinem im Vertrag genannten Ansprechpartner anzuzeigen!

Für den Umgang mit all unseren IT-Geräten gilt generell folgendes.

Um Verlust (z.B. Diebstahl) vorzubeugen müssen folgende Punkte für sämtliche Hardware beachtet werden:

- Innerhalb unserer abgeschlossenen Büroumgebung (z.B. durch Zutrittskarten, Schleusen gesichert) gilt das Gerät während Deiner Arbeitszeit als verschlossen aufbewahrt. Geräte, die außerhalb der Arbeitszeit innerhalb unserer abgeschlossenen Büroumgebung bleiben sind über Nacht zusätzlich verschlossen aufzubewahren (z.B. abschließbarer Schrank oder Kensington-Schloss).
- Außerhalb unserer abgeschlossenen Büroumgebung sind die Geräte ebenfalls verschlossen aufzubewahren (z.B. verschlossene Wohnung oder zutrittsgesichertes Firmengelände anderer Firmen). Es ist sicherzustellen, dass kein unbefugter Zugriff durch Dritte erfolgen kann.
- Bei einem Transport muss die Hardware entweder in einem verschlossenen Behälter (z.B. nicht einsehbarer, verschlossener Kofferraum) oder direkt am Körper unter Deiner Aufsicht transportiert werden.

Bei Beschädigung infolge unsachgemäßen oder nicht bestimmungsgemäßen Umgangs oder bei Verlust des Firmeneigentums behalten wir uns vor, einen etwaigen Schaden Dir gegenüber geltend zu machen, was im Einzelfall geprüft wird.