Datenschutzhinweise für Kolleg:innen der Unternehmen der PAYBACK Group

Wir informieren Dich im Folgenden darüber, wie mit Deinen personenbezogenen Daten (im Folgenden „Daten“) im Rahmen Deines Beschäftigungsverhältnisses umgegangen wird und welche Datenschutzrechte Dir zustehen.

I. Datenschutzrechtlich Verantwortliche(r)/ Gemeinsame Verantwortliche

Verantwortlich im Sinne der Datenschutzgesetze für die im Folgenden beschriebenen Verarbeitungen Deiner Daten ist dasjenige Unternehmen der PAYBACK Group, mit dem Du Deinen Arbeitsvertrag hast (im Folgenden dafür auch „Dein Arbeitgeber“ oder „wir“).

Soweit Du bei einer Tochtergesellschaft der Loyalty Partner GmbH angestellt bist, hat Dein Arbeitgeber verschiedene Funktionen (Personal/ Finanzen/ Buchhaltung/ Controlling/ Steuer/ Recht/ Einkauf/ Travel Management/ Office Management/ Empfang/ kaufmännische IT) weitgehend auf die Loyalty Partner GmbH übertragen. Für die im Rahmen dieser übertragenen Funktionen erfolgende Datenverarbeitung ist Dein Arbeitgeber und die Loyalty Partner GmbH jeweils gemeinsam verantwortlich. Sie haben in einer Vereinbarung festgelegt, wer von ihnen welche datenschutzrechtlichen Verpflichtungen erfüllt. Das Wesentliche dieser Vereinbarung, insbesondere eine Darstellung der umfassten Datenverarbeitungen, findest Du in der Toolbox unter HR - Datenschutz.

II. Datenschutzbeauftragter

Für die deutschen Unternehmen ist unser Datenschutzbeauftragter:

Herr Dr. Robert Selk, LL.M., selk@dsb-consulting.com, Telefon: +49 89 489 54 346.

Für das österreichische Unternehmen ist der Datenschutzbeauftragte:

Herr Magister Georg Fellner, LL.M., g.fellner@bkp.at, Telefon + 43 1 532 12 10

Du erreichst den jeweiligen Datenschutzbeauftragten auch über Deinen in Ziffer I genannten Arbeitgeber mit dem Zusatz „zu Händen des Datenschutzbeauftragten“.

III. Datenkategorien

Im Rahmen Deines Arbeitsverhältnisses verarbeiten wir verschiedene Arten von Daten von Dir. Zur besseren Übersichtlichkeit haben wir diese im Folgenden zu Kategorien zusammengefasst. Bei Bedarf geben wir Dir gerne zu den Inhalten der einzelnen Datenkategorien genauere Auskunft:

1. **Personalstammdaten**
   Unter Personalstammdaten verstehen wir diejenigen Daten, die als Grundlage für Dein Arbeitsverhältnis dienen, weitgehend statisch sind und nur selten Veränderungen unterliegen. Hierunter fallen z. B. Name, Anschrift, Geburtsdatum, Bankverbindung, Sozialversicherungsnummer sowie der Notfallkontakt. Teil dieser Daten können auch sog. besondere Kategorien personenbezogener Daten sein („Sensible Daten“), wozu u.a. die Religionszugehörigkeit gehört.

2. **Daten zur Arbeitszeit/Zeitdaten**
   Daten zur Arbeitszeit sind solche, die Art und Umfang Deiner Arbeitszeit definieren, ebenso wie An- und Abwesenheiten.

3. **Betriebs- und Organisationsdaten**
   Betriebs- und Organisationsdaten sind Daten, die Auskunft über Deine Tätigkeit und organisatorische Eingliederung in unserem Unternehmen geben. Darunter fallen z. B. die Abteilung, in der Du arbeitest oder auch Deine Personalnummer.

4. **Daten zur Mitarbeiteradministration**
   Dies sind Daten, die wir ergänzend zur Personalverwaltung benötigen; hierzu gehören z. B. die Verpflichtung auf kartellrechtskonformes Verhalten und die Verpflichtung auf Vertraulichkeit.

5. **Abrechnungsdaten**
   Abrechnungsdaten sind solche, die benötigt werden, um die Gehaltsabrechnung ordnungsgemäß durchführen zu können. Hierzu gehören z. B. die Höhe Deines Gehalts und Dein Eintrittsdatum ins Unternehmen.

6. **Gesundheitsdaten**
   Das sind Daten, aus denen Informationen über Deinen Gesundheitszustand hervorgehen oder diesen betreffen und die wir u.a. für die Durchführung eines betrieblichen Eingliederungsmanagements oder das Erbringungen von Gesundheitsleistungen benötigen. Hierzu gehören z. B. Informationen über Krankheiten und Mutterschutz, aber auch Informationen im Hinblick auf die Beschaffung von bestimmten Gesundheitsmöbeln.

7. **Arbeitsergebnisse und Inhaltsdaten**
   Dies sind Daten, die im Rahmen Deiner Tätigkeit für uns anfallen, wie insbesondere Deine Arbeitsergebnisse inklusive von Dir geschaffener Inhalte (etwa Präsentationen, Programmcode, Schreiben, etc.), aber auch Deine mit den Arbeitsergebnissen unmittelbar zusammenhängenden Daten, wie etwa Dein Name als Autor:in eines Dokuments.

8. **IT-Daten**
   IT-Daten sind solche Daten, die das Arbeiten in der IT-Systemlandschaft ermöglichen oder dort anfallen. Darunter fallen insbesondere
   - Nutzungsinformationen (z.B. Nutzerkonto- und Zugangsdaten, Usernamen und Passwörter, zugewiesene Rollen und Berechtigungen),
   - Informationen über die von Dir eingesetzten Geräte und Software (wie z.B. Gerätename, Hersteller, Betriebssystem, Seriennummern und Geräte-IDs, MAC-Adressen, installierte Softwareanwendungen)
   - Supportinformationen, wie Deine Kontaktinformationen, von Dir gestellte Supportanfragen und die dazugehörige Kommunikation
   - Informationen zu Dateien (Name der Datei, Dateigröße, etc.)

   Ferner gehören die bei der Nutzung der IT-Systeme anfallenden Daten zu den IT-Daten („Nutzungsdaten“), wie z.B. Zeitpunkt der An- und Abmeldung, die Durchführung bestimmter Systemaktivitäten (Logfiles), aber auch sog. Event-Daten. Event-Daten umfassen Informationen über Ereignisse und Aktivitäten in den von Dir benutzten IT Systemen, daneben auch zahlreiche Begleitinformationen dazu, wie etwa die Namen sämtlicher von Dir gespeicherten Dokumente und Dateien, die Zeiten der Erstellung, des Öffnens und des Speicherns von Dateien, den Zeitpunkt und den Namen aller gestarteten Programme, den Zeitpunkt Deines Logins und Logouts, die von Dir oder Deinem PC aufgerufene Webseiten und alle anderen Netzwerkverbindungen.

9. **Daten zur externen und internen Leistungsverrechnung**
   Darunter sind alle Daten zu verstehen, die zur Abrechnung von externen und internen Leistungen nötig sind, wie z. B. Tätigkeitsnachweise. Dieser Fall liegt vor, wenn Deine Tätigkeiten Teil einer Leistung sind, die wir für Dritte erbringen (etwa Partnerunternehmen oder Business-Kunden von uns) und gegenüber diesen abrechnen.

10. Daten bzgl. Entwicklung/Fortbildung/Leistung

Diese Daten beinhalten Informationen über Deine Entwicklung und Leistung im Unternehmen sowie über Deine Fort- und Weiterbildungsaktivitäten. Darunter fallen z. B. Deine Zielvereinbarungen, Jahresendbewertungen oder auch Schulungsteilnahmen.

11. Daten aus Beurteilungen (durch Führungskräfte, 270 Grad Feedback, etc.)

Darunter fallen einerseits alle Daten, die bei der Beurteilung von Beschäftigten über diese anfallen oder verarbeitet werden. Dies ist unabhängig, ob die Beurteilung durch die Führungskraft, durch Kolleg:innen (etwa im Rahmen des Feedbacks der 270 Grad Beurteilung) oder durch andere an einer Personalbeurteilung beteiligte Personen erfolgt.

Ebenso fallen anderseits unter diese Kategorie auch die Daten der beurteilenden Personen, also v.a. deren abgegebenes Feedback, Einschätzung oder Beurteilung.

12. Reise- , Spesen- und Auslagenersatzdaten

Dies sind Daten zur Planung, Bearbeitung und Kostenerstattung von dienstlichen Reisen, ebenso wie Daten zur Erstattung von Auslagen für uns als Unternehmen. Beispiele sind die allgemeinen Reisedaten sowie Kreditkartennummern oder Aufenthaltsgenehmigungen.

13. Daten zur Fuhrparkverwaltung und Tiefgaragenplätze

Dazu gehören alle Daten, die zur Beantragung, Verwaltung und Abrechnung von Firmenwagen erforderlich sind, wie beispielsweise die Leasingvertragsnummer oder das Kfz-Kennzeichen; Sofern ein Tiefgaragenstellplatz genutzt wird, auch das KfZ-Kennzeichen von Privatfahrzeugen.

14. Bewerbungsdaten

Dazu gehören alle Daten, die im Zuge Deiner internen Bewerbung innerhalb Deines Unternehmens oder bei einem anderen Unternehmen der Loyalty Partner Gruppe verarbeitet werden, u.a. Name, Kontaktdaten und Bewerbungsdokumente sowie Unterlagen der Bewerbungsgespräche.

15. Tätigkeits- und Buchungsdaten

Soweit nicht schon in den vorstehenden Kategorien beschrieben, handelt es sich um Daten, die im Rahmen Deiner beruflichen Tätigkeiten anfallen, wie z. B. Dein Name und Deine beruflichen Kontaktdaten als Ansprechpartner:in für Dritte oder als Autor:in oder Bearbeiter:in von Dokumenten, oder die im Rahmen eines Workflow anfallenden Daten, wie die Erteilung einer Genehmigung oder der Buchung eines Meeting-Raumes.

16. Zutrittsdaten

Dies sind Daten, die im Rahmen unserer Zutrittskontrolle anfallen und verarbeitet werden, etwa wenn Du bestimmte Bereiche über Lesegeräte mit Deiner Zutrittskarte öffnest.

17. Daten in Umfragen, Auswertungen und Reports

Dabei handelt es sich um Daten von Dir, die Teil einer von uns durchgeführten Umfrage, Auswertung oder von Reportings sind, etwa im Rahmen einer durchgeführten Umfrage unter Beschäftigten oder Arbeitszeitauswertungen.

18. Bildaufnahmen

Mit Bildaufnahmen sind Bilder von Dir in Form einer Fotografie oder eines Videos gemeint.

19. Zusätzliche Profildaten

Dies sind Informationen über Dich, die Du auf freiwilliger Basis für andere Nutzer:innen über verschiedene unserer IT-Systeme sichtbar machen kannst, wie zum Beispiel bestimmte Fähigkeiten von Dir, Informationen zu Deiner Ausbildung, Deine Interessen und Hobbies, etc. Die Angabe solcher Daten ist freiwillig und nicht zur Nutzung dieser IT-Systeme erforderlich. Du kannst diese Angaben jederzeit ändern oder löschen.

20. Sonstiges

Daneben verfügen wir gegebenenfalls noch über weitere Daten, die im Rahmen Deiner Tätigkeit für uns anfallen, aber keiner oben beschriebenen Kategorien zugehören. Über diese informieren wir gegebenenfalls gesondert.

IV. Zwecke und Rechtsgrundlagen

Wir verarbeiten Deine oben beschriebenen Daten zu Zwecken der Begründung, der Durchführung oder der Beendigung des Beschäftigungsverhältnisses, ebenso zur zentralisierten Steuerung und Abwicklung der Personalverwaltung innerhalb der Loyalty Partner Gruppe sowie zur Erreichung der nachfolgend beschriebenen weiteren Zwecke. Im Folgenden erläutern wir die Zwecke genauer und geben Dir dazu eine Reihe von Beispielen. Ebenso nennen wir die Rechtsgrundlage, auf deren Basis wir die Daten verarbeiten. Soweit wir Deine Daten zu anderen Zwecken verarbeiten, informieren wir Dich darüber gesondert.

1. Datenverarbeitung zur Begründung des Beschäftigungsverhältnisses bei Wechsel innerhalb der Unternehmensgruppe

Im internen Bewerbungsverfahren (Bewerbungstool/ Assessment Center) verarbeitet das Unternehmen, bei dem Du Dich intern bewirbst, Deine Daten zum Zweck der möglichen Begründung eines Beschäftigungsverhältnisses mit Dir. Bei der Verarbeitung kommen alle Datenkategorien in Betracht. Insofern

- sehen wir Deine Bewerbungsunterlagen durch,
- leiten wir Deine Bewerbungsunterlagen an die betreffenden Fachabteilungen weiter
- führen wir mit Dir Korrespondenz und kommunizieren mit Dir (z.B. Einladung zum Bewerbungsgespräch oder Assessment Center)
- dokumentieren wir den Bewerbungsvorgang.

Rechtsgrundlage für diese Datenverarbeitung ist Art. 6 Abs. 1 S.1 lit b) iVm Art. 88 Abs. 1, 2 DSGVO iVm § 26 Abs. 1 S. 1 Var. 1 BDSG (Begründung eines Beschäftigungsverhältnisses).

Im Rahmen der „Net(t)work“ – Bewerbung verarbeiten wir Deine Daten als Fürsprecher:in der Person, die sich bewirbt. Rechtsgrundlage für diese Datenverarbeitung ist Art. 6 Abs. 1 S. 1 lit f) DSGVO (Interessensabwägung). Unser Interesse ist, über diesen Weg von qualifizierten Bewerber:innen zu erfahren und Dich als Fürsprecher:in zu kennen sowie Dir gegebenenfalls eine Belohnung zukommen zu lassen.

2. Datenverarbeitung zur Erfüllung der Pflichten aus dem Beschäftigungsverhältnis und zu dessen Durchführung

Aus dem zwischen uns geschlossenen Arbeitsvertrag ergeben sich verschiedene Pflichten, zu deren Erfüllung wir Deine Daten verarbeiten, wie insbesondere zur Personal-, Urlaubsadministration sowie zur Gehaltsabrechnung oder im Rahmen der Bereitstellung eines Firmenwagens oder Reisekostenabrechnungen. Ebenso verarbeiten wir Daten zu Deiner Aus- und Weiterbildung, dem Karriere- und Talentmanagement, im Rahmen von Beurteilungen oder Umfragen.

Bei diesen Verarbeitungen kommen alle Datenkategorien in Betracht. So legen wir beispielsweise eine Personalakte an, veranlassen die Gehaltsabrechnung und richten IT Accounts ein, bei Bewertungen verarbeiten wir die Beurteilungen über Dich bzw. von Dir abgegebene Beurteilungen, ebenso wie wir von Dir geschaffene Arbeitsergebnisse und Inhaltsdaten verwenden, etc.

Rechtsgrundlage für diese Datenverarbeitungen ist Art. 6 Abs. 1 S.1 lit b) iVm Art. 88 Abs. 1, 2 DSGVO iVm § 26 Abs. 1 S. 1 Var. 2 BDSG (Durchführung eines Beschäftigungsverhältnisses). Soweit die Verarbeitung besonderer Kategorien personenbezogene Daten umfasst ist (z.B. Gesundheitsdaten), ist Rechtsgrundlage ergänzend zu vorgenannten Vorschriften Art. 9 Abs. 2 lit b), lit f) DSGVO.

3. Erfüllung gesetzlicher Verpflichtungen

Der Gesetzgeber hat ferner für uns als Arbeitgebende in verschiedenen Gesetzen Verpflichtungen geschaffen, z. B. im Arbeitszeit- und Bundesurlaubsgesetz. Aber auch gesetzliche Aufbewahrungs- und Archivierungspflichten fallen darunter, etwa Dokumente betreffend, die Daten von Dir enthalten. Zur Erfüllung dieser Pflichten kommt die Verarbeitung von allen Datenkategorien in Betracht, ausgenommen sind lediglich Fotografien. Beispiele hierfür sind, dass wir die erforderlichen Meldungen an Behörden vornehmen oder Dich zu erforderlichen Pflichtschulungen (z.B. zum Datenschutz) einladen.

Rechtsgrundlage für diese Datenverarbeitung ist Art. 6 Abs. 1 S.1 lit. c) DSGVO. Diese umfasst auch die Verarbeitung Deiner Gesundheitsdaten (Art. 6 Abs. 1 S. 1 c iVm Art. 9 Abs. 2 lit b) und lit h DSGVO).

5. Zur Kommunikation mit anderen

Wir verarbeiten Deine Daten, soweit dies für die Durchführung der Kommunikation mit Dir oder zwischen Dir und Dritten erforderlich ist, z.B. bei der Nutzung von Email oder anderen Kommunikations- oder Zusammenarbeitstools, wie Videokonferenzen, Teams oder Sharepoint, dies gilt auch, wenn Du als Bevollmächtigte:r oder mit Vertretungsbefugnis auftrittst. Für diese Zwecke verarbeiten wir vor allem Deine Stammdaten, insbesondere Kontaktdaten und gegebenenfalls den Inhalt der Kommunikation, wie etwa eine verfasste E-Mail, aber auch Betriebs-, Organisations- und IT-Daten.

Rechtsgrundlage für diese Datenverarbeitung ist Art. 6 Abs. 1 S.1 lit b) iVm Art. 88 Abs. 1, 2 DSGVO iVm § 26 Abs. 1 S. 1 Var. 2 BDSG (Durchführung eines Beschäftigungsverhältnisses).

Wenn Du in IT-Systemen, etwa in unserer Microsoft 365 Arbeitsumgebung, bestimmte oder alle Profildaten für andere Nutzer:innen freigibst, machen wir diese zum Zweck der Veröffentlichung diese Daten für die anderen Nutzer:innen zugänglich.

Rechtsgrundlage dafür ist Art. 6 Abs. 1 S. lit f) DSGVO (Interessenabwägung, unser Interesse ist, Dir die gewünschte technische Funktionalität zur internen Veröffentlichung Deiner Profildaten bereitzustellen).

6. Sicherstellung eines reibungslosen Betriebsablaufs

Zum reibungslosen Betriebsablauf gehören neben der allgemeinen Organisation auch Zutrittsmöglichkeiten zu Räumen sowie die Buchung und Organisation der Besprechungsräume oder anderer Meeting-Möglichkeiten. Zu diesem Zweck verarbeiten wir Deine Stamm-, Betriebs- und Organisations-, sowie Fortbildungsdaten u.a. bei der Erstellung der Zutrittskarten oder in Protokollen und Organisationsübersichten.

Rechtsgrundlage für diese Datenverarbeitung ist Art. 6 Abs. 1 S.1 lit b) DSGVO iVm Art. 88 Abs. 1, 2 DSGVO iVm §26 Abs. 1 S. 1 Var. 2 BDSG (Durchführung eines Beschäftigungsverhältnisses).

7. Bereitstellung, Nutzung und Verwaltung von IT-Systemen

Soweit nicht schon Teil der Sicherstellung des Betriebsablaufs, verarbeiten wir bei Deiner Nutzung von IT-Systemen, insbesondere der Kommunikation mit anderen (z.B. per E-Mail, Teams, etc.) oder bei der Nutzung des Internets, Daten, um Dir Zugang zu diesen IT-Systemen zu geben und deren Nutzung zu ermöglichen sowie um die IT-Systeme zu administrieren. Zu diesem Zweck verarbeiten wir z.B. beim Login Deine Zugangsdaten, bei der Verwendung des Internets verarbeiten wir die IP-Adressen des Quell- und Zielrechners, die URL des Zielsystems, den Zeitpunkt des Verbindungsaufbaus und -endes, die Verbindungsdauer und den Benutzernamen. Bei der Firmen-E-Mail-Nutzung werden Absender:in und Empfänger:in, Zeitpunkt, Länge, etc. verarbeitet. Vorgenannte Daten verarbeiten wir ebenfalls, um Dir bei Fragen zu helfen (Support).

Betroffen sind Teile Deiner Stamm-, Betriebs- und Organisationsdaten, IT- und Tätigkeitsdaten sowie auch Auswertungsdaten.

Rechtsgrundlage für diese Datenverarbeitung ist Art. 6 Abs. 1 S.1 lit b) iVm Art. 88 Abs. 1, 2 DSGVO iVm § 26 Abs. 1 S. 1 Var. 2 BDSG (Durchführung eines Beschäftigungsverhältnisses).

Vorstehende Absätze gelten unabhängig, ob es sich um ein von uns Dir zur Verfügung gestelltes stationäres IT-Gerät (wie einen Desktop-PC) oder mobiles Endgerät handelt, wie ein Notebook, Tablet oder Mobiltelefon.

Wenn Du dagegen ein eigenes Endgerät einsetzt, um auf unsere IT-Systeme zuzugreifen und Du die dazu nötigen Voraussetzungen alle erfüllst, gelten dafür eigene Datenschutz-Hinweise, die Du gesondert erhältst.

Soweit Du freiwillig optionale Funktionen der von uns bereitgestellten IT-Systeme nutzt, die mit einer zusätzlichen Verarbeitung Deiner Daten verbunden sind, verarbeiten wir diese Daten zum Zwecke der Bereitstellung dieser Funktionen. Hierzu gehört beispielsweise die optionale Synchronisierung von Account-Informationen durch den Browser Microsoft Edge

Rechtsgrundlage dafür ist Art. 6 Abs. 1 S. lit f) DSGVO (Interessenabwägung, unser Interesse ist, Dir die gewünschte technische Funktionalität zur internen Veröffentlichung Deiner Profildaten bereitzustellen).

8. Gewährleistung von Informationssicherheit

Um einen reibungslosen Betriebsablauf und die IT-Sicherheit zu gewährleisten, das IT-Equipment bestmöglich vor Bedrohungen wie Schadsoftware, wie Viren, Trojaner, Würmer, insbesondere Ransomware zu schützen, ist es notwendig, dass bestimmte IT-Daten einzelner IT-Systeme systemisch protokolliert und analysiert werden. Dazu gehören z.B. die Datensicherung, die Prüfung, ob unsere Vorgaben zum Umgang mit der IT eingehalten werden und die Kontrolle von Zutritts-, Zugangs- und Zugriffsmöglichkeiten auf IT-Systeme und Server-Räumen, aber auch die Überwachung von Systemaktivitäten und Systemevents, wer wann wie welche Events oder Aktivitäten ausgelöst hat, etc.

Weitere Informationen zu dem von uns eingesetzten Security-Überwachungstool findest Du in der Anlage „Zusatzinformationen zur Informationssicherheit“.

Rechtsgrundlage für diese Datenverarbeitung ist einerseits Art. 6 Abs. 1 S.1 lit b) iVm Art. 88 Abs. 1, 2 DSGVO iVm § 26 Abs. 1 S. 1 BDSG (Durchführung eines Beschäftigungsverhältnisses), andererseits aber auch Art. 6 Abs. 1 S. 1 f) DSGVO (Interessenabwägung, basierend auf unseren Interessen, dass Schadsoftware erkannt und beseitigt wird, um die auf unseren IT-Systemen befindlichen Daten zu schützen. Im Fall der Verarbeitung von Logfiles basiert die Interessenabwägung auf unseren Interessen, unberechtigte Datenverarbeitung zu verhindern sowie zu erkennen und gegebenenfalls zu ahnden).

9. Leistungserbringung gegenüber Dritten

Wenn Deine Tätigkeiten Teil einer Leistung ist, die wir für Dritte erbringen (etwa Partnerunternehmen oder Geschäftskunden von uns), kann es sein, dass wir zum Zwecke Deiner dortigen Zuordnung zu uns und zu einem bestimmten Projekt sowie zu Zwecken der Authentifizierung und Autorisierung bestimmte Stamm-, Betriebs- und Organisationsdaten an Dritte melden müssen (etwa Deinen Namen und berufliche Kontaktdaten, unter Umständen zu Identifizierungszwecken aber auch Dein Geburtsdatum oder andere Identifikationsdaten). Soweit eine Abrechnung der Tätigkeiten gegenüber Dritten erfolgt, verarbeiten wir zum Zwecke dieser Abrechnung und dem Nachweis Deiner Leistungen Deine Daten zur Leistungsverrechnung.

10. Förderung des sozialen Miteinanders/ Betriebsklimas

Zu diesen Zwecken verarbeiten wir Stamm-, Abrechnungs-, Betriebs- und Organisationsdaten, z.B. um Dir die Mitgliedschaft in der Turnhalle anbieten zu können oder um Dir zu Jubiläen oder zum Geburtstag zu gratulieren.

Rechtsgrundlage für diese Datenverarbeitung ist Art. 6 Abs. 1 S. 1 lit. f) DSGVO (Interessenabwägung). Unser Interesse ist, unseren Betrieb optimal zu organisieren und ein gutes soziales Miteinander und Betriebsklima zu fördern.

11. Bildaufnahmen für Zutrittskarte

Fotografien von Dir verwenden wir für Deine Zutrittskarte zu Deiner Authentifizierung, zum Teil auch in IT-Systemen, falls Du Dich dort mit Deinem Foto zeigen möchtest. Rechtsgrundlage dafür ist zur Nutzung in der Zutrittskarte Art. 6 Abs. 1 S.1 lit b) iVm Art. 88 Abs. 1, 2 DSGVO iVm § 26 Abs. 1 S. 1 Var. 2 BDSG (Durchführung eines Beschäftigungsverhältnisses, ansonsten Art. 6 Abs. 1 S. 1 lit f) DSGVO (Interessenabwägung: unser Interesse ist, Deinen Kolleg:innen und Dir darüber die Möglichkeit zum besseren Kennenlernen zu geben). Dazu verwenden wir die Fotografie von Dir und gegebenenfalls Teile Deiner Stammdaten.

Soweit wir Bildaufnahmen von Dir fertigen, die über vorstehend genannte Zwecke hinausgehen, erfolgt dies – soweit sich keine andere gesetzliche Erlaubnis ergibt - nur bei Vorliegen Deiner Einwilligung. Die Zwecke der Verwendung richten sich dann nach dem Inhalt der Einwilligung. Rechtsgrundlage ist insofern die von Dir erteilte Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DSGVO iVm Art. 88 Abs. 1, 2 DSGVO iVm § 26 Abs. 2 BDSG-neu.

12. Aufzeichnung von Meetings

In Einzelfällen und nur mit Einwilligung aller Teilnehmenden können echte oder virtuelle Meetings, etwa in Microsoft Teams, zu Dokumentations- oder Schulungszwecken aufgezeichnet werden. Wir verarbeiten zu diesem Zweck den Ton- und gegebenenfalls auch Bilddaten sowie verschiedene IT-Daten. Zweck ist, die Aufzeichnung anschließend anderen Personen zugänglich zu machen, etwa anderen Beschäftigten von PAYBACK oder von Partnern.

Eine Aufzeichnung erfolgt nur mit Einwilligung der jeweils am Meeting Teilnehmenden.

Rechtsgrundlage ist daher Art. 6 Abs. 1 S. 1 lit. a) DSGVO iVm Art. 88 Abs. 1, 2 DSGVO iVm § 26 Abs. 2 BDSG (Einwilligung). Die Einwilligung wird in solchen Fällen eingeholt, wenn Teilnehmende das jeweilige Meeting betreten bzw. wenn die Aufzeichnung gestartet wird.

13. Weitere Zwecke

Über etwaige darüber hinausgehende Zwecke und die Rechtsgrundlage zur Verarbeitung informieren wir Dich gesondert im jeweiligen Zusammenhang.

V. Pflicht zur Bereitstellung von Daten/ Freiwillige Angaben

Deine Personalstammdaten (siehe oben Ziffer III.1.) müssen von Dir verpflichtend bereitgestellt werden, einerseits aus gesetzlichen Gründen, andererseits, da ohne diese Daten die Durchführung des Beschäftigungsverhältnisses nicht möglich ist.

Soweit Du Dich intern bewirbst, werden Deine Bewerbungsdaten benötigt, ohne die Deine Bewerbung nicht bearbeitet werden kann.

Fotografien sind nur verpflichtend bereitzustellen, wenn dies aus Sicherheitsgründen nötig ist, wie z.B. für Zutrittskarten. Zur Nutzung in Newslettern, der Bubble App, in der Toolbox oder im Internet sowie in Sozialen Netzwerken erfolgt die Bereitstellung freiwillig.

Zu den vertraglichen Pflichten von Führungskräften gehört die Beurteilung ihrer Mitarbeiter:innen. Bei einer angefragten Beurteilung von Kolleg:innen dagegen besteht keine vertragliche oder gesetzliche Pflicht zur Teilnahme und damit Abgabe von Beurteilungen.

VI. Herkunft der Daten

Wir erhalten Deine Daten in erster Linie von Dir selber, z. B. aus Deinen Bewerbungsunterlagen, Deinem ausgefüllten Personalfragebogen oder aus Deiner Tätigkeit für uns. Daten aus Beurteilungen über Dich erhalten wir von den Personen, die Dich beurteilen, in der Regel Deine Führungskraft, bei Teilnahme am 270 Grad-Feedback aber auch von Kolleg:innen.

Einige personenbezogene Daten werden auch durch individuelle Vergabe, z. B. Vergabe einer Personalnummer, oder automatisch aus unseren IT-Systemen generiert, z. B. beim Anlegen Deiner Benutzer-ID.

Zum Teil erhalten wir Daten über Dich auch von Dritten, etwa im Rahmen der Umsetzung der unter Ziffer IV. beschriebenen Zwecke, wie z. B.
- Bestätigung von externen Schulungsveranstaltern, dass Du an einer Schulung teilgenommen hast
- Rückmeldungen von Behörden wie dem Finanzamt oder der Aufsichtsbehörde für Mutterschutz im Rahmen der gesetzlich erforderlichen Meldungen
- Rückmeldung von Krankenkassen, Sozialversicherungsträgern oder Banken.

VII. Empfänger oder Kategorien von Empfängern

1. Empfängerkategorien innerhalb unseres Unternehmens und der Unternehmensgruppe

Je nach Zweck und Notwendigkeit können folgende interne Empfängerkategorien sowie Abteilungen Zugriff auf Deine Daten haben oder interne Empfänger sein:
- Personal/ Personalkommittee

- Geschäftsführung/ Führungskraft/ Vorgesetzte/ Hiring Manager:in
- Kolleg:innen (interne Emails, Besprechungen, etc.)
- Administrator:innen der IT Systeme (Urlaubstool, etc.)
- Finanzen/ Buchhaltung/ Controlling/ Steuer/ Recht/ Einkauf
- Travel Management/ Office Management/ Empfang
- Turnhalle

Soweit Du nicht bei der Loyalty Partner GmbH angestellt bist, hat Dein Arbeitgeber verschiedene Funktionen (Personal/ Finanzen/ Buchhaltung/ Controlling/ Steuer/ Recht/ Einkauf/ Travel Management/ Office Management/ Empfang/ kaufmännische IT) weitgehend auf die Loyalty Partner GmbH übertragen. Insofern sind die entsprechenden Abteilungen bei der Loyalty Partner GmbH ebenfalls Empfänger der Daten.

2. Externe Empfängerkategorien ansässig in der EU/EWR

Teilweise übermitteln wir Deine Daten auch externen Empfängern oder gewähren diesen Zugriff darauf. Bei diesen unterscheiden wir zwischen Dienstleistern, die uns bei der Durchführung des Beschäftigungsverhältnisses unterstützen, und solchen Dritten, denen wir aus gesetzlichen Gründen oder zur Erfüllung des Arbeitsvertrages Daten zukommen lassen, ebenso weiteren Dritten, die Daten von Dir anlassbezogen erhalten, etwa im Rahmen Deiner Kommunikation mit diesen oder bei der Veröffentlichung von Fotos im Internet die entsprechenden Webseitenbetreiber.

Beispiele für unterstützende Dienstleister sind:
- Gehaltsdienstleister, Personaldienstleister, Trainingsanbieter, Seminareinrichtungen,
- IT-Firmen, die Software für uns betreiben oder unsere internen Systeme warten,
- die PAYBACK GmbH, die für die anderen Gesellschaften der LP Gruppe im Rahmen einer Auftragsverarbeitung deren Office IT betreibt, sowie die von der PAYBACK GmbH hierfür eingesetzten IT-Dienstleister (z.B. Microsoft),
- Akten- und Datenträgervernichtungs-Firmen.

Beispiele für Dritte, die Deine Daten aus gesetzlichen Gründen oder zur Erfüllung Deines Arbeitsvertrags erhalten, sind:
- Finanzamt, Sozialversicherungsträger und Krankenkassen, Betriebsprüfung
- Betriebsärzt:innen, Pensionskassen
- Banken

Beispiele für weitere Dritte:
- Partnerunternehmen von uns
- unsere Geschäfts-Kunden
- Webseitenbetreiber, insbesondere auch Social Media Plattformen

3. Externe Empfängerkategorien ansässig außerhalb der EU/ EWR

Folgende Kategorien von Empfängern haben ihren Sitz außerhalb der EU/ EWR. Du findest im Folgenden jeweils auch die rechtlichen Grundlagen für die Übermittlung dorthin angegeben:

a. Teil der AMEX Firmengruppe

Die Unternehmen der Loyalty Partner Gruppe gehören zur Firmengruppe der American Express Inc mit Sitz in den Vereinigten Staaten von Amerika. Zum Zwecke der Durchführung des Beschäftigungsverhältnisses kann es erforderlich sein, dass Daten von Dir an American Express weitergegeben werden. Beispiele dafür sind Daten aus Schulungsmaßnahmen, aus Leistungs- und Potentialbewertungen oder Daten im Zusammenhang mit der Vorbereitung und Durchführung von Entsendungen.

Rechtsgrundlage ist einerseits Dein Arbeitsvertrag (Art. 6 Abs. 1 S. 1 lit b) DSGVO, Art. 88 Abs. 1,2 DSGVO iVm § 26 Abs. 1 S. 1 BDSG), andererseits die zwischen uns und der American Express Inc. abgeschlossenen EU-Standarddatenschutzklauseln controller-to-controller aus dem Jahre 2004 (Art. 46 Abs. 2 lit c) DSGVO).

b. Technische Dienstleister/ IT-Unternehmen

Uns unterstützende technische Dienstleister oder deren Unterauftragnehmer, die jeweils Empfänger der Daten sein können, gibt es auch in solchen Ländern außerhalb der EU/ EWR, die kein der EU gleichwertiges Datenschutzniveau bieten (sog. „Drittländer“). Daraus können sich zusätzliche Risiken ergeben, beispielsweise kann die Durchsetzung der Betroffenenrechte erschwert sein.

Zu diesen Dienstleistern gehört zum Beispiel die Crowdstrike, Inc. mit Sitz in den USA als Herstellerin und Betreiberin unseres Security-Überwachungstools (siehe dazu auch die Anlage zu diesen Datenschutzhinweisen mit weiteren Informationen).

Auch Microsoft in den USA kann darunterfallen. Soweit wir Microsoft Produkte einsetzen, haben wir darauf geachtet, dass unsere Daten in Microsoft Rechenzentren und Servern innerhalb der EU gespeichert werden. In bestimmten Fällen, etwa für Support- oder Diagnosezwecken, kann es aber dennoch sein, dass Microsoft aus Drittstaaten zugreift oder eine Zugriffsmöglichkeit besteht, etwa den USA.

Es gibt aktuell keinen Beschluss der EU-Kommission, dass diese Drittländer, insbesondere die USA, allgemein ein angemessenes Schutzniveau bieten. Um den Risiken aus den Drittland-Übermittlungen zu begegnen und eine Rechtsgrundlage dafür zu schaffen, haben wir mit unseren dortigen Dienstleistern jeweils von der EU-Kommission für solche Fälle vorgegebenen EU-Standard-Datenschutzverträge abgeschlossen. Darin ist auch die Umsetzung von für den konkreten Fall angemessenen Schutzmaßnahmen festgelegt, die abhängig von der Schutzbedürftigkeit der Daten beispielsweise auch deren Verschlüsselung umfassen können.

Rechtsgrundlage für diese Drittlandübermittlungen ist Art. 46 Abs. 2 lit. c) DSGVO in Verbindung mit den genannten EU-Standarddatenschutzverträgen und zwar in Form des Durchführungsbeschlusses der EU-Kommission (EU) 2021/914 vom 04.06.2021.

c. Ansprechpartner bei der Visa-Beantragung

Für die Erteilung der Visa nach den jeweiligen Einreisebestimmungen des Landes kann es erforderlich sein, Daten an das jeweilige Außenministerium sowie an Ansprechpartner (Kontakt, der besucht werden soll) im Reiseland, die ein Einladungsschreiben für Dich erstellen müssen, zu übermitteln.

Die Rechtsgrundlage für die Übermittlung Deiner Daten in Drittländer, für die die Kommission keinen Angemessenheitsbeschluss erlassen hat, ist Art. 49 Abs. 1 Nr. b DSGVO (Datenübermittlung zur Erfüllung des Arbeitsvertrags mit Dir).

d. Weitere Nicht-EU-/ EWR-Empfänger

Es kann weitere Empfänger auch außerhalb der EU/ EWR geben, die Daten von Dir anlassbezogen erhalten, etwa im Rahmen Deiner Kommunikation mit diesen oder bei der Veröffentlichung von Fotos im Internet die entsprechenden Webseitenbetreiber. Wir haben mit diesen ebenfalls die vorgenannten EU-Standarddatenschutzverträge abgeschlossen.

e. Zu allen Nicht-EU/ EWR Empfängern

Auf Anfrage stellen wir Dir betreffend der Nicht-EU/ EWR Empfänger eine Kopie der Beschlüsse der EU sowie geschlossener EU-Standarddatenschutzverträge zur Verfügung. Bitte wende Dich dazu an den Datenschutzbeauftragten.

VIII. Dauer der Aufbewahrung und Speicherung Deiner Daten

Wir speichern/ bewahren Deine personenbezogenen Daten so lange, wie wir gesetzlich dazu verpflichtet sind oder es für die Erfüllung der Zwecke, für die sie verarbeitet werden, erforderlich ist.

Personalstammdaten: In Deiner Personalakte werden alle wichtigen Unterlagen von Dir abgespeichert. Diese benötigen wir, um das laufende Arbeitsverhältnis zu betreuen. Die Unterlagen haben unterschiedliche Aufbewahrungsfristen. Damit verwaltungstechnisch eine einheitliche Handhabung erfolgen kann, vernichten wir die Unterlagen in der Personalakte 10 Jahre nach Ablauf des Jahres, in dem Du aus dem Unternehmen ausgeschieden bist.

Abrechnungsdaten: Als GmbH sind wir nach Handels- und Steuerrecht dazu verpflichtet, diejenigen Unterlagen aufzubewahren, die für einen Nachweis der ordentlichen Buchführung und Bilanzerstellung erforderlich sind. So müssen z. B. gem. § 147 Abs. 1 Nr. 4 AO Buchungsbelege 10 Jahre aufgehoben werden. Andere Lohnunterlagen, die unter den Lohnsteuerabzug fallen (siehe § 147 Abs. 3 S. 1 AO), müssen 6 Jahre aufbewahrt werden. Darunter fallen z. B.: Spesenabrechnungen, Reisebuchungen und-rechnungen sowie Unterlagen zum Lohn- und Gehaltskonto.

Nutzungsdaten und Logfiles: Diese speichern wir in der Regel für einen Zeitraum von bis zu 90 Tagen, in begründeten Ausnahmefällen bis zu 12 Monaten. Danach erfolgt entweder eine Löschung oder Anonymisierung der Daten. Soweit solche Daten in der Security-Software „Falcon Plattform“ anfallen, findest Du Angaben zur Speicherdauer in der Anlage zu diesen Datenschutzhinweisen.

Weitere Daten: Deine übrigen Daten speichern wir jeweils nur so lange, wie sie für die jeweiligen Zwecke (siehe oben), zu denen wir sie erhoben oder gespeichert haben, noch notwendig sind oder so lange gesetzliche Aufbewahrungspflichten gelten und entsprechende Aufbewahrungsfristen laufen. Im Anschluss löschen wir auch diese Daten.

IX. Automatisierte Entscheidungsfindung

Bei der Verarbeitung Deiner Daten wird keine automatisierte Entscheidungsfindung iSv. Art. 13 Abs. 2 Nr. f DSGVO eingesetzt.

X. Deine Rechte

Dir stehen jeweils bei Vorliegen der gesetzlichen Voraussetzungen verschiedene Rechte zu, über die wir Dich im Folgenden informieren:

Auskunft: Auf Anforderung teilen wir Dir gerne mit, ob und welche Daten über Dich gespeichert sind.

Berichtigung, Einschränkung der Verarbeitung oder Löschung: Soweit die gesetzlichen Voraussetzungen vorliegen, hast Du ein Recht auf Berichtigung, Einschränkung der Verarbeitung oder Löschung dieser Daten.

Datenherausgabe: Du hast weiter das Recht, die Dich betreffenden Daten, die Du uns bereitgestellt hast, in einem strukturierten, gängigen und maschinenlesbaren Format von uns zu erhalten; Du kannst diese Daten an andere Stellen übermitteln oder übermitteln lassen. Voraussetzung ist zudem, dass wir diese Daten auf Basis einer Einwilligung oder zur Vertragsdurchführung verarbeiten und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Widerruf: Wenn Du eine Einwilligung zu einer Datenverarbeitung abgegeben hast (etwa der Nutzung von Fotos), so kannst Du diese jederzeit widerrufen. Die bis dahin auf der Einwilligung erfolgte Datenverarbeitung bleibt rechtmäßig.

Beschwerde: Du hast außerdem ein Beschwerderecht bei einer Aufsichtsbehörde für den Datenschutz. Du kannst Dich dabei auch direkt an die für uns zuständige Behörde wenden: Bayerisches Landesamt für Datenschutzaufsicht, Promenade 27, 91522 Ansbach, poststelle@lda.bayern.de.

XI. Zukünftige Änderungen und Fragen

Soweit sich in Zukunft Änderungen ergeben, werden wir Dich proaktiv darüber vorab informieren. Bei Fragen wende Dich bitte an unseren Datenschutzbeauftragten, dessen Kontaktdaten findest Du oben in Ziffer 2.

Gesonderter Hinweis zum Widerspruchsrecht

Soweit wir Daten auf Basis einer Interessenabwägung verarbeiten (siehe dazu die Vermerke in den obigen Datenschutzhinweisen), kannst Du dagegen Widerspruch erheben. Wir verarbeiten Deine Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Deine Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Stand April 2022

ANLAGE: „Zusatzinformationen zur Informationssicherheit“

Im Folgenden möchten wir Dir betreffend der Verarbeitung Deiner Daten zum Zwecke der „Gewährleistung von Informationssicherheit“ und der dazu von uns eingesetzten Software „Falcon Plattform“ und „Illusive Networks Platform“ zusätzliche Informationen geben:

1. Falcon Plattform

a) Was ist die „Falcon Plattform“? Wozu dient sie?

Wir setzen dazu auf allen unseren PCs (dazu gehören auch Notebooks und andere Geräte, wie Server, im Folgenden sprechen wir nur von „PC“ oder „PCs“) die Security-Software namens „Falcon Plattform“ ein. Diese besteht aus zwei Teilen:

- Dem Falcon-Sensor: Dies ist eine Software, die wir auf Deinem PC installieren. Dieser überwacht fortlaufend und ständig Deinen PC und die dortigen Aktivitäten, unabhängig, ob diese von Dir ausgelöst oder rein technisch vom System durchgeführt werden.
- Der Falcon-Cloud, die von unserem Dienstleister Crowdstrike Inc. mit Sitz in den USA betrieben wird: In diese Cloud sendet der Falcon-Sensor laufend Daten, die dort analysiert und auf verdächtige Muster überprüft werden. Gibt es Auffälligkeiten oder sogar einen Alarm, meldet die Cloud-Software dies an unsere IT-Security-Abteilung, damit diese der Meldung nachgehen kann.

Zweck der in der Falcon Plattform erfolgenden Datenverarbeitung ist ausschließlich die Gewährleistung der Informationssicherheit und damit insbesondere der Schutz unserer PCs vor Schadsoftware. Eine Auswertung der Daten zu anderen Zwecken erfolgt über die Falcon Plattform nicht. Wir haben die Verarbeitung der Daten zu anderen Zwecken, wie zum Beispiel der Kontrolle Deines Arbeitsverhaltens, vielmehr intern strikt verboten und werden Verstöße gegen dieses Verbot streng ahnden. Um dies zu erreichen, haben nur bestimmte Mitarbeiter:innen der IT-Security Zugriff, zudem wird zu Kontrollzwecken jeder Zugriff dieser Mitarbeiter:innen auf die Falcon Plattform systemisch protokolliert.

b) Welche genauen Datenkategorien werden von der Falcon Plattform im Detail verarbeitet?

Im Folgenden beschreiben wir Dir – als Detaillierung zu den obigen Datenschutzhinweisen – die in der Falcon Plattform verarbeiteten Event-Daten, die im Rahmen der Falcon-Plattform verarbeitet werden, genauer und führen zur Verdeutlichung jeweils Beispiele auf und konkretisieren die verfolgten Zwecke noch weiter:

Datenkategorie	Beispiel für Einzeldaten	Konkretisierung der Zwecke
General Events sind die grundlegenden Ereignisse, die zur Überwachung des Zustands des Falcon-Sensors und zur Identifizierung von Geräten erforderlich sind.	Falcon-Sensor Online, Benutzeridentität, Absturzbenachrichtigung	Die Daten dieser Kategorie werden benötigt, um den Falcon-Sensor zu managen. Benötigt werden diese Events insofern zum Beispiel zur Feststellung: - der Version (Patchmanagement) - Betriebssystem des PCs - zur Fehlerbehandlung des Falcon-Sensors - um Prozesse zu überwachen und zu melden
User Session Events ist die Überwachung von Benutzersitzungsereignissen.	Statusmeldungen des PCs: verbunden, angemeldet, getrennt	Diese Daten dienen der Überwachung von Benutzerereignissen, wie z.B. die Anmeldung, der Anmeldenamen, die Berechtigungen (Admin oder Nutzer), ob ein Programm vom Nutzer, System oder einem anderen Dienst gestartet wird (Erkennung von Malware).
Process Events Standard-Prozessdaten, die zur Identifizierung und Analyse von PC-Prozessen benötigt werden	Prozess-erstellung, Prozess-informationen, Zeicheninfo, Prozess-beendigung	Diese Daten dienen der Überwachung, wann auf dem PC ein Programm gestartet wurde, die Prozess-ID (PID), wo die zugehörige Datei gespeichert ist und zu welchem Dienst/ welcher Anwendung der Prozess gehört. Diese Erfassung ist notwendig, da alle Dateien bzw. Programme (Anwendungssoftware wie auch Schadprogramme), die ausgeführt werden, aus einem oder mehreren Prozessen bestehen.
File Events sind Dateien, die durch einen Prozess innerhalb einer verdächtigen Ausführungskette generiert werden.	Dateierstellung, Dateizugriff	Unter diesen Daten versteht man z.B. Informationen zu Dateien, etwa deren Namen, Informationen zur Erstellung von Dateien, den Schreib- und Lesezugriff auf Dateien und die Möglichkeit, Dateien in den Speicher (RAM) zu laden (z.B. CreateFileMapping). Durch diese Überwachung kann der Angriff durch Ransomware (Verschlüsselung) wirksam verhindert werden.
Network Events sind Daten zur Identifizierung von Netzwerkaktivitäten	Ausgehende/ eingehende Verbindung herstellen, Netzwerk schließen, Verbindung, Zusammen-fassung	Diese Daten betreffen Aktivitäten, die sich mit den Netzwerkaktivitäten des PCs beschäftigen. Dazu gehören unter anderem alle ausgehenden und alle eingehenden Verbindungen. Dadurch können verdächtige Verbindungen herausgefiltert und blockiert werden. Denkbar ist hierbei z.B. der Verbindungsaufbau des PCs zu einem „feindlichen“ Server, oder das im Hintergrund ausgeführte Herunterladen von Schadsoftware beim Surfen auf einer kompromittierten Webseite.
Library Events Identifizierung von Softwarebibliotheken im Zusammenhang mit geladenen Prozessen	Laden der Bibliothek	Unter Software- oder Programm-Bibliotheken versteht man in der IT sogenannte Hilfsprogramme, die nicht eigenständig lauffähig sind, sondern von anderen Programmen (Prozessen) angefordert und ausgeführt werden können. Im Rahmen eines Angriffs werden durch die Schadsoftware oftmals Windows-Programmbibliotheken manipuliert. Diese werden dadurch mit Systemrechten ausgeführt und ermöglichen die weitere Kompromittierung des betroffenen PCs.
Thread Events Daten zu verdächtigen Ausführungsketten	Thread-Erstellung, Thread-Injektion	Daten zu "Thread Events" sind notwendig, da jeder Prozess aus einem oder mehreren sog. Threads besteht. Es handelt sich hierbei um eine Basiseinheit, die vom Betriebssystem Rechenleistung zugewiesen bekommt. Ein Thread beinhaltet den Programmteil, der gerade von Windows ausgeführt wird. Threads

		werden von Malware genutzt, um schadhafte Programmbibliotheken bzw. Programme in einen Prozess anderen zu laden und auszuführen.
Registry Events Daten zu Lastpunkten, mit denen Angreifer die Persistenz feststellen können	ASEP-Schlüssel-aktualisierung, ASEP-Wertaktualisierung	"Registry Events" dienen der Überwachung von Aktivitäten, die die Windows Registry betreffen. In dieser Registry sind und werden alle Betriebssystem- und Programmkonfigurations-einstellungen langfristig gespeichert (z.B. welche Programme/Dienste automatisch gestartet werden sollen). Schadsoftware schreibt oftmals Einträge in die Registry, um darüber ein Laden der Malware beim Systemneustart zu erzwingen.
DNS Events ermitteln fehlerhafte DNS-Suchvorgänge - mit Schwerpunkt auf unerwarteten Abfragen unter Windows	DNS-Anfrage	Über eine DNS-Abfrage wird die im Browser eingegebene URL in eine IP-Adresse übersetzt, anhand der die Verbindung zu der aufgerufenen Webseite hergestellt wird. Die Überwachung der "DNS Events" ist notwendig, da DNS-Anfragen an bekannte bösartige Domains oftmals ein wichtiger Indikator und Anhaltspunkt sind, mit dem festgestellt werden kann, ob bestimmte Systeme von Malware befallen sind. Auch der Hintergrund-Download von Schadsoftware über verseuchte Webseiten kann dadurch verhindert werden.
Miscellaneous Events überwachen verdächtige Prozessketten.	Erstellung von benannten Objekten (z. B. Mutexe, Semaphoren)	Darunter fallen alle weiteren verdächtigen Events, die vom Falcon-Sensor überwacht werden. So ist es z.B. notwendig, die Erstellung von sog. “Objekten“ zu überwachen, da Schadprogramme solche verwenden. Ziel ist sicherzustellen, dass ein System nicht mehrfach von der gleichen Malware infiziert wird.

Neben den vorgenannten Event-Datenkategorien gibt es zwei weitere Datenkategorien:

Datenkategorie	Beispiel für Einzeldaten	Konkretisierung der Zwecke
Alarm-Meldung Daten, die im Falle eines Verdachts auf eine Schadsoftware bzw. deren Fest-stellung in eine Alarm- Meldung geschrieben werden	Erkannte Malware	In einer Alarm-Meldung wird die erkannte Malware und der PC dokumentiert, auf dem sich diese findet, ebenso wie weitere Informationen zu dem Vorgang, wie die Information, wann welche Malware worauf zugegriffen hat, welche Prozesse betroffen waren und welcher Nutzer angemeldet war.
Audit-Protokoll Die Zugriffe der Administratoren auf die Falcon-Plattform werden aus Sicherheitsgründen protokolliert.	Anmeldung n der Falcon-Plattform, Administratoraktivitäten	In den Auditlogs werden alle Informationen über die einzelnen Aktivitäten protokolliert. Hier findet man die Anmeldezeiten der einzelnen Nutzer sowie die durchgeführten Arbeiten. Zweck ist die Kontrolle der Tätigkeiten der Administratoren.

<u>Zu allen Kategorien:</u>
Da die Event-Daten automatisch erhoben werden, ist keine gesonderte Bereitstellung durch Dich erforderlich. Gleiches gilt für die Alarm-Meldungen und Audit-Protokolle, die automatisiert von der Plattform erstellt werden.

c) Welche Regelungen gelten zur Speicherdauer bei der Falcon Plattform?

In der Falcon-Plattform speichern wir die anfallenden personenbezogenen Daten (siehe dazu oben in den Datenschutzhinweisen Ziffer II. und III.) für 7 Tage zur Auswertung und Analyse, im Anschluss werden diese gelöscht oder gemäß den datenschutzrechtlichen Vorgaben so anonymisiert, dass keinerlei Möglichkeit des Rückschlusses auf eine Person mehr möglich ist.

Von der Falcon Plattform generierte Alarm-Meldungen werden zur Überprüfung und Bearbeitung, aber auch zur Nachverfolgbarkeit und aus Beweisgründen bis zu 90 Tage lang gespeichert und dann gelöscht oder gemäß den datenschutzrechtlichen Vorgaben so anonymisiert, dass keinerlei Möglichkeit des Rückschlusses auf eine Person mehr möglich ist.

Informationen über Zugriffe auf Daten in der Falcon Plattform speichern wir zu Sicherheits- und Überwachungsgründen bis zu 365 Tage und löschen diese im Anschluss. Zu diesen Zwecken hat der Datenschutzbeauftragte Zugriff auf diese Informationen.

2. Illusive Plattform

a. Was ist die „Illusive Networks Plattform“? Wozu dient sie?

Bei der Illusive Networks Plattform („Illusive“) handelt es sich um eine Software, die der Sicherheitsüberwachung interner (Büro-)Systeme (Server + Laptops) zur Erkennung von Sicherheitsrisiken und bösartigen Aktivitäten auf Computern dient. Deren Zweck ist ausschließlich die rechtzeitige Erkennung, Verhinderung und Abwehr von internen und externen Cyberangriffen.

b. Welche Datenkategorien werden von Illusive im Detail verarbeitet?

Im Folgenden beschreiben wir Dir – als Detaillierung zu den obigen Datenschutzhinweisen – die in Illusive verarbeiteten Datenkategorien noch genauer und führen zur Verdeutlichung jeweils Beispiele auf und konkretisieren die verfolgten Zwecke noch weiter:

Sog. „Collection“-Daten:
Die nachfolgenden gelisteten Datenkategorien werden im Rahmen der routinemäßigen Einsatzzyklen verarbeitet, um Angriffspfade, Regelverletzungen und Regelvorschläge sowie Gegenmaßnahmen zu berechnen:

Datenkategorie	Beispiel für Einzeldaten	Konkretisierung der Zwecke
Systemdaten	Betriebssystem, Version, IP-Adresse, MAC-Adresse, Computername	Die Daten werden benötigt, um den Computer eindeutig zuordnen zu können
Benutzerdaten	Anmeldename, Benutzer:innen, die auf dem Gerät angemeldet waren	Diese Daten dienen der Überwachung von Benutzerereignissen, wie z.B. die Anmeldung, der Anmeldenamen
Verbindungsdaten	Protokolle, Ports, Hosts	Diese Daten betreffen Aktivitäten, die sich mit den Netzwerkaktivitäten des PCs beschäftigen. Dazu gehören unter anderem alle ausgehenden und alle eingehenden Verbindungen. Dadurch können verdächtige Verbindungen

		herausgefiltert und blockiert werden. Denkbar ist hierbei z.B. der Verbindungsaufbau des PCs zu einem „feindlichen“ Server, oder dass im Hintergrund ausgeführte Herunterladen von Schadsoftware beim Surfen auf einer kompromittierten Webseite.

Sog. „Forensic“-Daten:
Die nachfolgendend genannte Datenkategorien werden zum Zweck der Echtzeit- und nachgelagerten Analyse eines Vorfalls verarbeitet:

Datenkategorie	Beispiel für Einzeldaten	Konkretisierung der Zwecke
Systemdaten	Betriebssystem, Version, IP-Adresse, MAC-Adresse, Computername, Events, DNS Cache, Anmeldesitzungen	Die Daten werden benötigt, um den Computer eindeutig zuordnen zu können
Benutzerdaten	Anmeldename, Benutzer:innen, die auf dem Gerät angemeldet waren	Diese Daten dienen der Überwachung von Nutzungsereignissen, wie z.B. die Anmeldung, der Anmeldename
Verbindungsdaten	Protokolle, Ports, Hosts, alle aktive Verbindungen des Computers	Diese Daten betreffen Aktivitäten, die sich mit den Netzwerkaktivitäten des PCs beschäftigen. Dazu gehören unter anderem alle ausgehenden und alle eingehenden Verbindungen. Dadurch können verdächtige Verbindungen herausgefiltert und blockiert werden. Denkbar ist hierbei z.B. der Verbindungsaufbau des PCs zu einem „feindlichen“ Server, oder dass im Hintergrund ausgeführte Herunterladen von Schadsoftware beim Surfen auf einer kompromittierten Webseite.
Prozessdaten	Name, ProzessID, Startzeit, Hashwert des Prozesses, Session, Status	Diese Daten dienen der Überwachung, wann auf dem PC ein Programm gestartet wurde, die Prozess-ID (PID), wo die zugehörige Datei gespeichert ist und zu welchem Dienst/ welcher Anwendung der Prozess gehört. Diese Erfassung ist notwendig, da alle Dateien bzw. Programme (Anwendungssoftware wie auch Schadprogramme), die ausgeführt werden, aus einem oder mehreren Prozessen bestehen.
Speicherdaten	Daten im Zwischenspeicher,	Diese Daten werden benötigt, um ausgeführte Angriffe rekonstruieren zu können.

c. Welche Regelungen gelten zu Speicherfristen bei Illusive?

„Collection-Daten“ werden im Normalfall nach der Erhebung für maximal 20 Stunden zum Zwecke der Berechnung von Angriffspfaden, Regelverletzungen und Regelvorschlägen sowie Gegenmaßnahmen gespeichert, unmittelbar im Anschluss gelöscht.

Tritt ein Sicherheitsvorfall ein, dann werden „Forensic-Daten“ erfasst und zum Zwecke der Echtzeit- und nachgelagerten Analyse eines Vorfalls für die Dauer von bis zu einem Jahr gespeichert.

Die Zugriffsprotokolle speichern wir zu den genannten Sicherheits- und Überwachungsgründen für 365 Tage und löschen diese im Anschluss.