Sicherheit, Datenschutz und Technologie

UKG-Lösungen in der Google Public Cloud Anleitung

UKG-Lösungen in der Google Public Cloud

Inhaltsübersicht

Bei UKG stehen die Menschen™ im Mittelpunkt. Wir arbeiten mit unseren Kunden zusammen, um sie dabei zu unterstützen, sich jeden Tag um ihre Mitarbeiter und ihr Geschäft zu kümmern. Dazu gehören der Schutz der Daten ihrer Mitarbeiter und ihrer Belegschaft sowie die Sicherstellung, dass ihre Geschäftsabläufe durch modernste Technologien und Verfahren reibungslos funktionieren.

Da immer mehr Unternehmen ihre Kerngeschäftstechnologien in die Cloud verlagern, ist es wichtig zu wissen, dass die Anbieter die Industriestandards für die Sicherung ihrer Cloud-Lösungen erfüllen oder übertreffen. UKG verwendet modernste Technologien, um die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Personendaten sowie die Sicherheit der Umgebungen zu gewährleisten, in denen unsere Anwendungen gehostet werden. Dieser Leitfaden behandelt die folgenden Punkte:




UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Hochmoderne Rechenzentren

Sicherheit und Datenschutz stehen bei den Planungskriterien im Vordergrund und sind ein integraler Bestandteil aller Google-Aktivitäten. Zu den physischen Sicherheitsmerkmalen aller Google-Rechenzentren gehört ein mehrschichtiges Sicherheitsmodell, das Sicherheitsvorkehrungen wie Alarme, Zugangssperren für Fahrzeuge, Umzäunungen, Metalldetektoren und biometrische Merkmale umfasst.
Die Google-Rechenzentren werden rund um die Uhr von hochauflösenden Innen- und Außenkameras überwacht.

Die Sicherheitsmaßnahmen werden in den Bereichen, die sich näher am Rechenzentrum befinden weiter erhöht. Weniger als 1 % der Google-Mitarbeiter werden jemals einen Fuß in ein Google-Rechenzentrum setzen, und nur autorisierte Google-Mitarbeiter mit bestimmten Rollen dürfen die Etagenbereiche betreten. Der Zugang zur Etage des Rechenzentrums ist nur über einen Sicherheitskorridor möglich, der mit einem Multifaktor-Zugangskontrollsystem ausgestattet ist, das Sicherheitsausweise und biometrische Daten für den Zugang erfordert.

Die Google Cloud läuft auf einer Technologieplattform, die so konzipiert, gestaltet und gebaut wurde, dass die Sicherheit eine zentrale spielt. Google ist ein Innovator in den Bereichen Hardware, Software, Netzwerk- und Systemmanagementtechnologien. Auf der Grundlage dieses Fachwissens hat Google seine Server, sein proprietäres Betriebssystem und seine geografisch verteilten Rechenzentren nach den Grundsätzen der "Defense in Depth" entwickelt, was zu einer IT-Infrastruktur führt, die sicherer und einfacher zu verwalten ist als herkömmliche Technologien.

"Defense in depth" beschreibt die mehreren Verteidigungsschichten, die das Google-Netzwerk vor externen Angriffen schützen. Nur autorisierte Dienste und Protokolle, die die Sicherheitsanforderungen von Google erfüllen, können das durchqueren, alles andere wird automatisch abgelehnt. Branchenübliche Firewalls und Zugriffskontrolllisten werden verwendet, um die Trennung des Netzwerks durchzusetzen. Der gesamte Datenverkehr wird über benutzerdefinierte Google Front End (GFE)-Server geleitet, um böswillige Anfragen und verteilte Denial-of-Service (DDoS)-Angriffe zu erkennen und zu stoppen.

Außerdem dürfen GFE-Server intern nur mit einer kontrollierten Liste von Servern kommunizieren; diese "Standardverweigerungs"-Konfiguration verhindert, dass GFE-Server auf unbeabsichtigte Ressourcen zugreifen. Die Protokolle werden routinemäßig untersucht, um die Ausnutzung von Programmierfehlern aufzudecken. Der Zugang zu vernetzten Geräten ist auf autorisiertes Personal beschränkt.

Die Google Cloud

Google ist ein Innovator im Bereich der Hardware-, Software-, Netzwerk- und Systemmanagementtechnologien. Die Google Cloud läuft auf einer Technologieplattform, die für einen sicheren Betrieb konzipiert, entwickelt und gebaut wurde.

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Hochmoderne Rechenzentren, Fortsetzung.

Die Rechenzentren von Google verfügen über redundante Stromversorgungssysteme und Umweltkontrollen. Jede kritische Komponente verfügt über eine primäre und eine alternative Stromquelle, jeweils gleich stark sind. Diesel-Backup-Generatoren liefern genug Notstrom, um jedes Rechenzentrum mit voller Kapazität zu betreiben.

Kühlsysteme sorgen für eine konstante Betriebstemperatur von Servern und anderer Hardware und verringern so das Risiko von Serviceausfällen.

Geräte zur Branderkennung und -unterdrückung helfen, Schäden an der Hardware zu verhindern. Wärme-, Feuer- und Rauchmelder lösen akustische und sichtbare Alarme in den betroffenen Bereichen, an den Sicherheitskonsolen und an den Fernüberwachungsstellen aus.

Zertifizierungen und Kontrollen

Das GCP hat die Zertifizierungen ISO 27001, 27017 und 27018 erhalten. GCP wird jährlich von einer unabhängigen Wirtschaftsprüfungsgesellschaft nach den AICPA SSAE 18 SOC 2-Kriterien geprüft und hat eine hohe Betriebsgenehmigung für das Federal Risk and Management Program (FedRAMP) erhalten.

Darüber hinaus werden die Lösungen von UKG jährlich gemäß den AICPA SSAE Trust Principles geprüft, und die SOC 2 Type II- und Google™ Cloud Platform (GCP) SOC 2-Berichte sind auf Anfrage und nach Abschluss einer gegenseitigen Geheimhaltungsvereinbarung erhältlich.

UKG-Lösungen: Sicherheit und Schutzmaßnahmen

Bei den UKG-Lösungen handelt es sich um native, mandantenfähige Software-as-a-Service (SaaS)-Lösungen, die sicher über das GCP gehostet werden und über Sicherheitsvorkehrungen verfügen, die eine Risikominderung ermöglichen und die Verschlüsselung von Daten im Ruhezustand und bei der Übertragung gewährleisten. Die Informationen in diesem Dokument gelten für die Lösungen UKG Pro®, UKG Dimensions™, UKG Ready® und UKG HRSD® , die im GCP bereitgestellt werden.

ISO-ZERTIFIZIERUNG

Die schriftliche Zusicherung einer unabhängigen Stelle (ein Zertifikat), dass das betreffende Produkt, die betreffende Dienstleistung oder das betreffende System bestimmte Anforderungen erfüllt.

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Netzwerksicherheit

Alle Internetverbindungen durchlaufen redundante Firewalls, um Zugangskontrollen durchzusetzen und die Überwachung und Protokollierung des Datenverkehrs zu ermöglichen. UKG konfiguriert die Firewall-Regeln standardmäßig so, dass sie alle Zugriffe verweigern. Erforderliche Ports und Protokolle werden auf der Grundlage eines definierten Geschäftszwecks geöffnet. Netzwerk-Proxys unterbinden jeglichen unnötigen Anwendungsverkehr.

Systeme zur Erkennung von Eindringlingen in Netzwerke (IDS) und Systeme zur Verhinderung von Eindringlingen (IPS) werden eingesetzt, um das Risiko von Eindringlingen und bösartigen Softwareangriffen zu verringern.

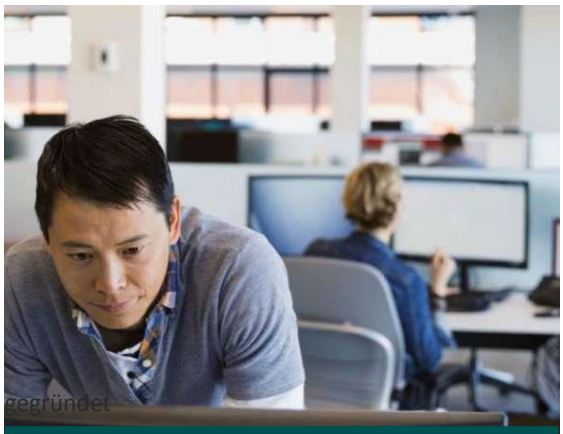
Google Cloud Armor bietet zusätzliche adaptive Schutzfunktionen für UKG-Lösungen, die im GCP bereitgestellt werden.

Schwachstellen-Scans der gehosteten Umgebung und der Anwendung werden durchgeführt, die Ergebnisse überprüft und die Schwachstellen je nach Schweregrad behoben.

Verschlüsselungsprotokolle

Zum Schutz der Kundendaten werden strenge Sicherheitsmaßnahmen getroffen, indem Verschlüsselungsprotokolle verwendet werden.

- Daten im Transit: Webanwendungen, mobile Geräte, Anwendungsprogrammierschnittstellen (APIs) und die Kommunikation mit Endgeräten werden mit TLS (Transport Layer Security) geschützt.
- Daten im Ruhezustand: UKG sichert alle Daten im Ruhezustand (Datenbank- und Dateiserver) für die Produktions- und Nicht-Produktionsumgebungen des Kunden für Daten in GCP mit Advanced Encryption Standard 256-Bit-Verschlüsselung.
- Sichere Dateiübertragung: Die SFTP-Dienste (Secure File Transfer Protocol) nutzen das Secure Shell Transfer Protocol, um einen allgemeinen Endpunkt für Kunden bereitzustellen, die Dateien zu und von UKG-Lösungen senden und empfangen. Darüber hinaus ist eine PGP-Dateiverschlüsselung (Pretty Good Privacy) für Flat-File-Integrationen verfügbar.
- Sichere Post: Die Lösungen von UKG und die Nachrichtensysteme des Unternehmens, die personenbezogene Daten (PII) übertragen, nutzen Secure Mail, um den Schutz sensibler Mitarbeiterdaten zu gewährleisten.



IDS - Intrusion Detection System
IPS - Intrusion Prevention System
GCP - Google Cloud Platform API - Anwendungsprogrammierschnittstelle
TLS - Sicherheit auf der Transportschicht
SFTP - sicheres Dateiübertragungsprotokoll

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Systemüberwachung und Schwachstellenmanagement

UKG hat mehrere Sicherheitsebenen implementiert, beginnend an der Systemgrenze, einschließlich Firewalls der nächsten Generation, Web Application Firewalls, IPS, IDS, Protokollüberwachung sowie Viren- und Malwareschutz. Darüber hinaus nutzt UKG fortschrittliche Endpunktüberwachungsagenten, die maschinelles Lernen und Verhaltensmodellierung für die Analyse und Erkennung potenziell bösartiger Aktivitäten nutzen.

Die SaaS-Umgebungen von UKG werden kontinuierlich rund um die Uhr von unserem globalen Security Operations Center und einem führenden Anbieter von Cybersecurity-Lösungen und -Dienstleistungen überwacht, um eine größere Transparenz zu gewährleisten und Ereignisse in den Cloud-Umgebungen von UKG zu korrelieren.

Sicherheitsinformations- und Ereignisverwaltungssysteme führen Datenquellen (z. B. Anwendungsprotokolle, Firewall-Protokolle, IDS-Protokolle) für granulare Analysen und Warnmeldungen zusammen. Zusätzlich zu den automatischen Warnungen und Benachrichtigungen nutzen die Mitarbeiter des UKG Security Operations Center branchenführende Lösungen und intern entwickelte Tools, um die Analyse von Sicherheitsereignissen zu unterstützen.

Darüber hinaus nutzt UKG das Security Command Center von Google für die laufende Verwaltung, Überwachung und Prüfung der Cloud-Umgebungen.

Härtungseinstellungen und -konfigurationen auf Produktionsservern werden anhand definierter Härtungsstandards überwacht.

Authentifizierung (UKG-Lösungen)

Die Lösungen von UKG unterstützen den Industriestandard Security Assertion Markup Language (SAML) 2.0 für die Authentifizierung bei webbasierten Anwendungen unter Nutzung von Single Sign-On (SSO).

Der Authentifizierungsdienst der UKG-Lösungen bietet einen hochverfügbaren, föderierten SSO-Service für die Benutzeranmeldung bei UKG-Lösungen von den Desktops, Work-from-Home-Geräten und mobilen Geräten der Kundenorganisation aus.

Der Authentifizierungsdienst unterstützt auch die direkte Anmeldung für Kunden, die SSO nicht nutzen oder über Gruppen von nicht legitimierten Mitarbeitern . Benutzernamen und Passwörter werden im UKG-System für Kunden mit Mitarbeitern gespeichert und verschlüsselt, die die direkte Anmeldung nutzen. Kunden können festlegendass einige Mitarbeiter SSO nutzen und andere Mitarbeiter (z. B. Alumni) die direkte Anmeldung verwenden.

Zu den zusätzlichen Authentifizierungs- und Zugangskontrollen, die mit UKG-Lösungen möglich sind, gehören unter anderem eine hohe Passwortkomplexität, Multi-Faktor-Authentifizierung und Zugangsbeschränkungen über das Internetprotokoll (IP).

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Autorisierung der Anwendung

Der Zugriff eines Benutzers auf die UKG-Lösung wird durch konfigurierbare Zugriffsprofile und Sicherheitsrollen gesteuert. Diese Zugriffsprofile und Rollen bestimmen, was ein Benutzer sehen und tun kann, und bestehen aus Komponenten, mit denen Sie den Zugriff auf das System auf der Grundlage der spezifischen Arbeitsanforderungen und der Organisationsstruktur Ihres Unternehmens genau definieren können.

Diese konfigurierbaren Profile und Sicherheitsrollen bestimmen die Funktionen, die ein Benutzer im System ausführen kann, und welche Mitarbeitergruppen er einsehen und bearbeiten kann. Zu den Optionen gehören Lese-/Schreibzugriff und Nur-Ansicht-Zugriff. Diese Kontrollen würden beispielsweise verhindern oder erlauben, dass ein Benutzer einen Mitarbeiterdatensatz ändert, Änderungen genehmigt, einen Stempel zu einem Stundenzettel hinzufügt oder auf Mitarbeiterzeitpläne zugreift.

Die Profile und Rollen bestimmen auch die Anzeigesteuerungen und Inhalte, die den Benutzern zur Verfügung stehen und die sich darauf auswirken, wie ein Benutzer die Komponenten der UKG-Lösung sieht. Sie steuern auch, auf welche Mitarbeiter ein Manager zugreifen kann. Alle Benutzer müssen einem Zugriffsprofil und einer Rolle zugewiesen werden, und dasselbe Profil kann einer Gruppe ähnlicher Benutzer zugewiesen werden, z. B. anderen Managern in derselben Abteilung.

Authentifizierung und Autorisierung (UKG intern)

Der Zugang zu den Anwendungsumgebungen der Kunden erfordert mehrere Stufen der Multi-Faktor-Authentifizierung und ist auf die Mitarbeiter beschränkt, deren Aufgaben einen solchen Zugang erfordern. Internes Personal ist gezwungen, Jump-Point-Technologie zu verwenden, die einen einzigen Ein- und Ausstiegspunkt in Rechenzentrumsumgebungen bietet und gleichzeitig administrative Aktivitäten überwacht und erfasst.

Die UKG-Passwortrichtlinien folgen den branchenüblichen Best Practices bei der Einhaltung und Festlegung komplexer Passwortanforderungen, Rotations- und Verfallsrichtlinien.

Der Zugang zu den Systemen wird durch ein formelles Antragsverfahren und ein spezielles Zugangsverwaltungsteam sorgfältig kontrolliert und verwaltet. Die Verwaltung des privilegierten Zugriffs wird weiter genutzt, um die Benutzerkonten mit erhöhten Zugriffsrechten zu schützen und zu sichern.

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Leistung

Die Lösungen von UKG werden während des Softwareentwicklungszyklus strengen Leistungstests unterzogen. Dabei werden branchenführende Schwellenwerte für interaktiven Datenverkehr, Integrations- (API-) Datenverkehr sowie Hintergrundberechnungen und -analysen festgelegt. Die Lösungen von UKG sind auf hohe Leistung ausgelegt, um die Geschäftsanforderungen unserer Kunden in allen Branchen und bei einer Vielzahl von Arbeitslasten zu erfüllen. Dieser Leistungstestprozess ist in den Lebenszyklus der Softwareentwicklung eingebettet und gilt gleichermaßen für neue und bestehende Funktionen.

In kundenorientierten Umgebungen werden die Antwortzeiten regelmäßig mit einer Kombination aus synthetischer Transaktionsüberwachung von mehreren geografischen Standorten aus (die den Kundenstamm repräsentiert) und interner Überwachung (die den UKG-Teil der Erfahrung repräsentiert) überwacht.

Interne Tools zur Überwachung der Anwendungsleistung sorgen für Transparenz vom Rand des UKG-Cloud-Netzwerks bis zur Datenebene, so dass die UKG-Ingenieure etwaige Leistungsprobleme genau lokalisieren können.

Die gesammelten Daten aus beiden Quellen werden regelmäßig von speziellen Technik- und Betriebsteams überprüft, um sicherzustellen, dass die Lösungen von UKG die Erwartungen unserer Kunden und die hohen Leistungsstandards von erfüllen oder übertreffen.

Verfügbarkeit

Die Lösungen von UKG sind hohe Verfügbarkeit und Ausfallsicherheit ausgelegt. UKG-Lösungen sind so konzipiert, dass sie bei Spitzen in der Benutzeraktivität und der Systemverarbeitung widerstandsfähig sind. Alle Servicekomponenten auf der Web-, Anwendungs- und Datenebene sind redundant ausgelegt, um eine äußerst zuverlässige und hochverfügbare Lösung zu gewährleisten. Lastausgleichstechnologien und Software-Clustering werden ebenfalls zur Erhöhung der Verfügbarkeit eingesetzt.

Performance evaluation process

Die Lösungen von UKG werden während der Entwicklung einem strengen Leistungsbewertungsprozess unterzogen. Die Lösung ist auf hohe Leistung ausgelegt, um die Geschäftsanforderungen unserer Kunden in allen Branchen und bei einer Vielzahl von Arbeitslasten zu erfüllen.

Service & availability

UKG Application Services sind so konzipiert, dass sie mehrere Cloud-Rechenzentren (Zonen) innerhalb eines geografischen Gebiets (Region) nutzen, um die Ziele der Notfallwiederherstellung (DR) zu erreichen.

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Skalierbarkeit

UKG-Lösungen verfügen über eine moderne, verteilte Service-Architektur in einer mehrschichtigen Plattform. UKG nutzt verschiedene Cloud-Management-Funktionen zur Bereitstellung und Konfiguration der zugrunde liegenden Infrastruktur und Computerressourcen. Dies ermöglicht die horizontale und/oder vertikale Skalierung von Diensten unabhängig voneinander, basierend auf der tatsächlichen und prognostizierten Auslastung.

Die UKG sammelt eine große Anzahl von Infrastruktur- und Anwendungsmetriken, um die Gesamtnachfrage nach Diensten sowie den Zustand und die Leistung Umgebung zu bewerten. Diese Metriken werden sowohl passiv als auch aktiv für eine Vielzahl von Betriebszwecken genutzt.

Die UKG nutzt die Cloud-Management-Funktionen regelmäßig und stützt sich dabei auf quantitative und qualitative Daten aus internen Überwachungslösungen. Die Lösungen und Dienste der UKG werden entsprechend der tatsächlichen und erwarteten Belastung und Beanspruchung des Systems skaliert.

Wiederherstellung im Katastrophenfall

Das UKG-Cloud-Disaster-Recovery-Programm wurde entwickelt und wird gepflegt, um eine kontinuierliche Anpassung an das UKG Business Resiliency Program zu gewährleisten, in dem die Anforderungen an die Notfallpläne und Krisenmanagementstrategien der UKG definiert sind. Die Datenintegrität und -verfügbarkeit der Kunden wird durch planmäßige Datensicherungen mit führender Unternehmenssicherungssoftware gewährleistet.

UKG Application Services sind so konzipiert, dass sie mehrere Cloud-Rechenzentren (Zonen) innerhalb eines geografischen Gebiets (Region) nutzen. Das UKG Cloud Disaster Recovery Program basiert auf einer Alles-oder-Nichts-Failover-Strategie. Für den Fall, dass die UKG-Anwendungsdienste des Kunden nicht verfügbar sind und nicht innerhalb akzeptablen Zeitrahmens wiederhergestellt werden können, wird der gesamte Stack in einer Katastrophensituation auf die DR-Region umgeschaltet.

Rechenzentren (Zonen) in der DR-Region werden verwendet, um eine warme/passive DR-Umgebung zu schaffen für Wiederherstellung der UKG-Dienste im Falle einer längeren Dienstunterbrechung.

DR-Umgebungen werden mithilfe von Techniken wie der kontinuierlichen oder Streaming-Datenreplikation mit ihren Pendants in der Produktion synchronisiert.

UKG setzt verschiedene Technologien ein, um die Sicherung und Wiederherstellung von Kundendaten an einem alternativen Standort im Falle eines längeren Ausfalls zu gewährleisten. Diese Technologien können Folgendes umfassen:

- Vollständige Backups
- Inkrementelle Sicherungen
- Air-Gapping, Cold-Storage und Offline-Backup-Repositories (falls zutreffend)

Die Disaster-Recovery-Lösungen von UKG, die in der Google Cloud Platform eingesetzt werden, stellen sicher, dass in den DR-Regionen Ressourcen verfügbar sind, die ein ähnliches Kapazitätsprofil wie in der Produktion aufweisen.

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Mediensanierung und Vernichtung von Daten

Google verfolgt den Standort und den Status aller Speichermedien in seinen Rechenzentren während des Erwerbs, der Installation, der Stilllegung und der Zerstörung über Asset-Tags, die in der Asset-Datenbank von Google verfolgt werden. Physische Speichermedien können aus einer Reihe von Gründen außer Betrieb genommen werden. Wenn eine Komponente zu irgendeinem Zeitpunkt ihres Lebenszyklus einen Leistungstest nicht besteht, wird sie aus dem Bestand entfernt und ausgemustert. Google rüstet auch veraltete Hardware auf, um die Verarbeitungsgeschwindigkeit und Energieeffizienz zu verbessern oder die Speicherkapazität zu erhöhen.

Unabhängig davon, ob die Hardware aufgrund eines Ausfalls, eines Upgrades oder aus einem anderen Grund außer Betrieb genommen wird, werden die Speichermedien unter Verwendung geeigneter Sicherheitsvorkehrungen außer Betrieb genommen. Google-Festplatten verwenden Technologien wie die vollständige Festplattenverschlüsselung, um die Daten während der Außerbetriebnahme zu schützen. Wenn eine Festplatte außer Betrieb genommen wird, überprüfen autorisierte Personen entweder 1), ob die Festplatte gelöscht ist, indem sie die Festplatte mit Nullen überschreiben und einen Überprüfungsprozess durchführen, um sicherzustellen, dass die Festplatte keine Daten enthält, oder 2) ein Werkzeug verwenden, um die Festplatte zu zerkleinern und zu verformen oder die Festplatte in kleine Stücke zu schreddern.

Speichergeräte und Hardware

Google verfolgt den Standort und den Status aller Speichergeräte in seinen Rechenzentren. Google rüstet auch veraltete Hardware auf, um die Verarbeitungsgeschwindigkeit und Energieeffizienz zu verbessern oder um die Speicherkapazität.

Teil Nummer

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Datenschutz

Als führendes Unternehmen für Life-Work-Technologielösungen ist sich UKG des regulatorischen Drucks bewusst, dem unsere Kunden in dem sich ständig weiterentwickelnden Bereich des individuellen Datenschutzes ausgesetzt sind. UKG hat sich verpflichtet, Systeme und Prozesse für die Personalverwaltung, die Lohnabrechnung und das Personalmanagement so zu entwickeln und einzusetzen, dass der Schutz personenbezogener Daten in allen Phasen des Datenlebenszyklus in Übereinstimmung mit den Anweisungen unserer Kunden, unserer veröffentlichten Datenschutzrichtlinie und den geltenden Gesetzen gewährleistet ist.

Priorisierung des Datenschutzes

Das Engagement, die Prioritätensetzung und die Unterstützung durch die Geschäftsleitung haben dazu geführt, dass die Mitarbeiter besser sensibilisiert sind und die Prozesse zur Unterstützung des Datenschutzes und des Schutzes personenbezogener Daten kontinuierlich verbessert werden.

Datenschutz durch Design

Das Konzept des Datenschutzes ist in die UKG-Lösungen eingebettet und wird in allen Phasen der Produktentwicklung angewendet.

Aufzeichnungen über die Verarbeitung

Das Dateninventarisierungsverfahren der UKG ist so konzipiert, dass eine äußerst genaue Berichterstattung über die im Auftrag unserer Kunden durchgeführten Verarbeitungstätigkeiten möglich ist.

Datenverarbeitung

UKG unterhält technische und organisatorische Maßnahmen zur Unterstützung der Sicherheits- und Compliance-Verpflichtungen unserer Kunden im Rahmen der EU-Datenschutzgrundverordnung (GDPR).

Datenschutz-Folgenabschätzungen

Im Zuge der Weiterentwicklung von Produkten und Prozessen wird UKG weiterhin den Datenschutz bewerten und Risikobereiche anhand des UKG-Dateninventars und -Klassifizierungssystems identifizieren.

Risikomanagement für Anbieter

Das Risikomanagement der UKG-Verkäufer umfasst die Überwachung und vertragliche Verpflichtungen, um sicherzustellen, dass Daten im Einklang mit den Grundsätzen der EU-Grundverordnung verarbeiten.

Management von Zwischenfällen

Der UKG Cybersecurity Incident Response Plan behandelt Vorfälle, bei denen personenbezogene Daten betroffen sind, mit höchsten Schweregrad der Reaktion.

Die Datenschutzbestimmungen von UKG sind unter dem folgenden Link abrufbar: Datenschutzhinweis | UKG

UKG-Lösungen in der Google Public Cloud

Sicherheit, Datenschutz und Technologie

Zusätzliche UKG-Leitlinien

UKG-Transparenzseite

Engagement für den verantwortungsvollen und ethischen Einsatz von künstlicher Intelligenz

Zusätzliche Google-Anleitung

Sicherheit in der Google Cloud

Generative KI, Datenschutz und Google Cloud

Our purpose is people

Bei UKG stehen die Menschen im Mittelpunkt. Wir glauben fest an die Kultur und den Aufbau lebenslanger Kundenpartnerschaften und setzen uns für großartige Arbeitsplätze ein, damit Unternehmen erkennen, was möglich ist, wenn sie in Menschen investieren. Unser Life-Work-Technology-Ansatz für HR-, Gehaltsabrechnungs- und Workforce-Management-Lösungen hilft Unternehmen, sich auf Mitarbeiter einzustellen, die nicht nur arbeiten. Besuchen Sie ukg.com.