Anlage 2 – Technische und organisatorische Maßnahmen

Innerhalb seines Verantwortungsbereichs ergreift Google bei der Erhebung, Verarbeitung und Nutzung personenbezogener Kundendaten die folgenden technischen und organisatorischen Maßnahmen.

1. Zutrittskontrolle

Google ergreift unter anderem die folgenden Maßnahmen, um den Zutritt Unbefugter zu den Datenverarbeitungsanlagen, mit denen Daten verarbeitet oder genutzt werden, zu verhindern:

Durch formale Zutrittsprozeduren wird der Zutritt zu den beteiligten Rechenzentren geregelt.

Alle Personen müssen sich gegenüber dem Sicherheitspersonal ausweisen, um Zutritt zu einem Rechenzentrum oder bestimmten Bereichen des Rechenzentrums zu erlangen. Dies erfordert einen von Google ausgestellten Fotoausweis und ein entsprechendes staatliches Ausweisdokument. Es bestehen dokumentierte Prozesse für das Ausstellen von Ausweisen durch Google. Der Besitz und die Rückgabe dieser Ausweise wird nachvollzogen und überprüft.

Es werden Besucher-Protokolle geführt. Besucher werden mit temporären Ausweisen ausgestattet und müssen von einem Google Mitarbeiter begleitet werden, um Zutritt zu Bereichen hinter dem Empfangsbereich eines Rechenzentrums zu erlangen.

Nur autorisierte Google-Mitarbeiter und Vertragspartner, die dauernd in den Rechenzentren beschäftigt sind, ist es erlaubt, elektronische Zugangskarten für diese Einrichtungen zu erhalten.

Die daneben bestehenden standardmäßigen Sicherheitsmaßnahmen, die in jedem Rechenzentrum durchgeführt werden, setzen sich aus bekannten Technologien zusammen und folgen allgemein anerkannten Best Practices der Branche. Dabei handelt es sich um elektronische Zugangskontrollsysteme per Kartenzugriff, Alarmsysteme, Innen- und Außenkameras und Sicherheitspersonal.

2. Zugangskontrolle

Google ergreift unter anderem die folgenden Maßnahmen um die Nutzung von Datenverarbeitungsanlagen, mit denen Daten verarbeitet werden, durch Unbefugte zu verhindern:

Sichere Zugangsverbindungen und Technologien zur Authentifizierungskontrolle sind implementiert, um den Zugang zu Google Produktivsysteme und interne Support-Tools zu reglementieren. Zugriffsrestriktionen stützen sich auf einen von Google entwickelten und verteilten Authentifizierungs-Service basierend auf Secure Socket Layer (SSL) Zertifikaten. Dieser Service bietet zudem Verschlüsselungsmethoden, um die Datensicherheit bei der Übertragung zu gewährleisten.

Der Zugang zu internen Support-Tools an Autorisierte wird kontrolliert durch Access Control Lists (ACL). Verschlüsselungstechniken werden eingesetzt, um Benutzerauthentifizierungen und Administrator-Sessions über das Internet abzusichern. Der Datenfernzugriff auf Produktionsmaschinen benötigt eine Verbindung zum Firmennetzwerk, die über eine zweifache Authentifizierung geregelt ist.

Google folgt einem formalen Prozess, um den Zugang zu Google-Ressourcen zu erlauben oder zu verweigern. Verschiedene Zugangsschutzmechanismen helfen dabei, sichere und flexible Zugriffe bereitzustellen. Einmalige Benutzerkennungen, starke Passwörter und periodische Überprüfungen der Zugriffslisten sind vorhanden, um die angemessene Verwendung von Benutzerkonten zu gewährleisten. Für kritische Systeme werden zudem Einmal-

Kennwörter bzw. Einmal-Konten verwendet. Alle Gruppen, die Zugang zu Google Services haben, unterlaufen einer regelmäßigen Überprüfung.

Alle genannten Maßnahmen sind in einem formalisierten Berechtigungskonzept beschrieben.

Die Autorisierung bei Google Services wird jederzeit auf allen Ebenen des jeweiligen Systems erzwungen. Die Erteilung oder Bearbeitung von Zugriffsrechten basiert auf den Job-Verantwortlichkeiten des Benutzers oder auf einer Need-to-know-Basis und muss durch den zuständigen Vorgesetzten des Antragstellers autorisiert und bewilligt werden. Die Bewilligungen werden über Workflow-Tools durchgeführt. Der Zugriff auf Produktivsysteme wird nur geschulten und für die jeweilige Aktion berechtigten Benutzern gewährt. Ebenso wird der Zugriff auf Produktivsysteme im Falle einer Kündigung umgehend entzogen.

Die Router sind entsprechend konfiguriert, um Google's interne Netzwerk Domänen vor unautorisierten externen Verbindungen zu schützen und sicherzustellen, dass Computerverbindungen und Datenflüsse nicht die logische Zugriffsregelung der Google Systeme verletzt. Änderungen an den hardwareseitigen Netzwerkkomponenten oder an deren Konfiguration benötigen die Zustimmung des designierten Verantwortlichen und unterliegen einem Change-Managementprozess.

Google hat ebenso Verschlüsselungsmethodiken, 2-Fach-Authentifizierung, Eingabe- und Session-logging für zentralisierte Serverumgebungen zur Überwachung der Produktivsysteme implementiert.

Google hat eine Firewall-Konfigurationsregelung, welche akzeptable Ports definiert, die auf einer Google Firewall genutzt werden dürfen. Nur benötigte Ports und Dienste sind offen. Der Zugriff zum Ändern der Firewall-Konfiguration ist beschränkt auf das interne Sicherheits-Operations-Team. Das Sicherheits-Operations-Team überprüft regelmäßig kritische Firewall-Regeln.

3. Zugriffskontrolle

Google ergreift unter anderem die folgenden Maßnahmen um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass gespeicherte oder in Verarbeitung befindliche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Webseitenbetreiber können über eine von Google angebotene Administrationskonsole ihre Analyseoptionen (einschließlich der IP-Maskierung) anpassen. Der Zugriff auf die Administratorkonsole ist mittels Benutzername und Passwort auf den Webseitenbetreiber oder durch diesen autorisierte Personen und daneben auf entsprechend berechtigte Mitarbeiter von Google beschränkt.

Der erforderliche Zugriff zur Aktivierung der IP-Maskierungen mittels Einbindung des entsprechenden Javascript-Code-Auszugs verbleibt beim Webseitenbetreiber und etwaige durch ihn autorisierte Personen.

Durch die dargestellten Zugangskontrollen (vgl. Klausel 1) wird der Zugriff auf die im Rahmen des Services erfassten IP-Adressen abgesichert. Der Zugriff ist mittels des Berechtigungskonzepts (vgl. Klausel 1) auf Mitarbeiter von Google mit entsprechenden Verantwortlichkeiten beschränkt.

4. Weitergabekontrolle

Google ergreift unter anderem die folgenden Maßnahmen um zu gewährleisten, dass Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Der Zugriff auf die Systeme zur Anonymisierung unterliegt wirksamen Zugriffskontrollen, die unter Klausel 3 beschrieben sind.

5. Eingabekontrolle

Google ergreift unter anderem die folgenden Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

Die Übertragung der IP-Adresse erfolgt aufgrund der Implementierung von Google Analytics durch den Betreiber der Webseite. Die Kundendaten sind mittels einer eindeutigen Kundennummer gekennzeichnet und so dem Kunden eindeutig zugeordnet.

Der Zugriff bzw. die Veränderung der übermittelten IP-Adresse unterliegt wirksamen Zugriffsschutzmechanismen (vgl. Klausel 3). Eingaben, Veränderungen und Löschungen von Daten werden mittels der in Klausel 3 beschriebenen Session-Loggings protokolliert.

6. Auftragskontrolle

Google ergreift unter anderem die folgenden Maßnahmen um zu gewährleisten, dass die Verarbeitung von Daten im Rahmen der Weisungen erfolgen kann:

Die Interaktion des Benutzers mit der Webseite des Webseitenbetreibers ist Bestandteil der Funktionalität der Webseite.

Wenn der Webseitenbetreiber mittels der Administratorkonsole die Weisung erteilt, dass eine IP-Maskierung erfolgen soll, ist aufgrund der Beschaffenheit des Systems gewährleistet, dass keine vollen IP-Adressen gespeichert werden.

7. Verfügbarkeitskontrolle

Google ergreift unter anderem die folgenden Maßnahmen, um zu gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Google verwendet eine Kombination von redundanten Systemen sowie Backup-Lösungen, um die Kundendaten zu schützen und wiederherstellen zu können.

Bei aktivierter IP-Maskierung wird das letzte Oktett der IP-Adressen vor Speicherung und etwaigen Backups gelöscht.

8. Gewährleistung der Zweckbindung

Google ergreift unter anderem die folgenden Maßnahmen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Die Verarbeitung erfolgt auf Serversystemen, die durch ein System von logischen und physischen Zugriffskontrollen im Netzwerk logisch getrennt sind (vgl. Klauseln 1 bis 3).

Die Verarbeitung der Daten erfolgt nur zum Zweck der Analyse der Benutzung einer Website durch die Besucher der Website.