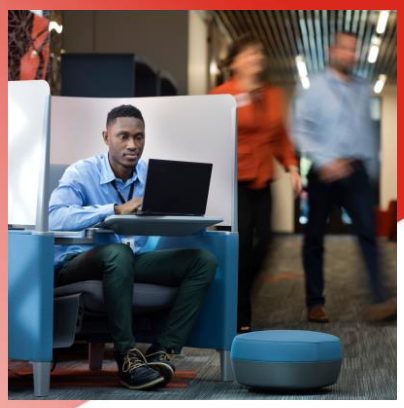
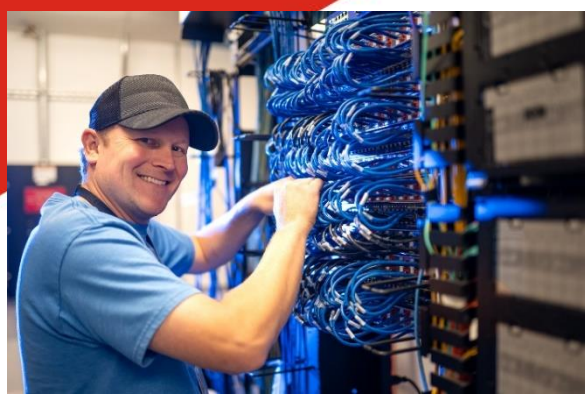
W. L. GORE & ASSOCIATES

ACCEPTABLE USE RICHTLINIE

Für Gore Partner





Einleitung

Dank der Assets von Gore sind wir in der Lage, mit unseren Kunden, Partnern und untereinander Geschäfte zu tätigen. Bei Gore sind wir davon überzeugt, dass unsere Associates und unsere Partner verantwortungsbewusst handeln und die gebotene Sorgfalt walten lassen, um bei der Führung der Geschäfte unsere Assets zu schützen. Diese Acceptable Use Richtlinie und unsere Selbstverpflichtung zur Erfüllung ihrer Anforderungen sind entscheidend für unseren Erfolg als Unternehmen.

Ziel

Ziel dieser Acceptable Use Richtlinie (im Folgenden als „Richtlinie“ bezeichnet) ist es, die Verantwortlichkeiten derjenigen unserer Partner festzulegen, die Zugriff auf Assets von W. L. Gore & Associates (im Folgenden als „Gore“ oder „Unternehmen“ bezeichnet) haben bzw. solche Assets nutzen. Diese Richtlinie dient dazu, die Informationsressourcen von Gore zu schützen und die Gore Partner bei der angemessenen Nutzung dieser Ressourcen anzuleiten.

Diese Richtlinie tritt an die Stelle und ersetzt die frühere „Acceptable Use Policy“ (AUP). Gore Partner müssen diese Richtlinie unterschreiben, um zu bestätigen, dass sie den in diesem Dokument festgelegten Inhalt gelesen und verstanden haben und sich zu dessen Einhaltung verpflichten.

Geltungsbereich

Diese Richtlinie gilt für alle Partner die in einer Geschäftsbeziehung mit Gore stehen („Gore Partner“), die Gore Assets nutzen.

Auch jede Nutzung von Gore Informationsressourcen oder jeder sonstige Zugriff auf Gore Informationen durch Gore Partner, sei es über vom Unternehmen ausgegebene Hardware, ein persönliches verwaltetes Gerät oder ein persönliches, nicht verwaltetes Gerät (vorbehaltlich einer Genehmigung), unterliegt dieser Richtlinie.

Wird etwas in dieser Richtlinie nicht erwähnt, heißt das nicht, dass es erlaubt ist. Vielmehr musst du bei Unklarheiten, Widersprüchen oder nicht eindeutig geregelten Fällen die Entscheidung von Gore herbeiführen.

Definitionen

Nachstehend werden die für diese Richtlinie wesentlichen Definitionen erläutert. Im Enterprise IT Glossary findest du noch weitere Definitionen.

KI-Tools – Eine Software-Anwendung, die auf künstlicher Intelligenz beruhende Algorithmen zur Ausführung bestimmter Aufgaben und zur Lösung von Problemen einsetzt. Zu KI-Tools gehören unter anderem:

- *Tools für maschinelles Lernen (ML),* die Daten analysieren, um Muster zu erkennen und Vorhersagen zu treffen. Dies unterstützt Gore bei Aufgaben wie Nachfrageprognosen, Kundensegmentierung und Betrugserkennung.
- *Tools zur Verarbeitung von natürlicher Sprache (Natural Language Processing, NLP),* die menschliche Sprache analysieren und Anwendungen wie Chatbots, Stimmungsanalysen und automatischen Kunden-Support ermöglichen.
- *Tools für maschinelle Bildverarbeitung (Computer Vision),* die es Computern ermöglichen, auf Basis visueller Daten zu interpretieren und Entscheidungen zu treffen; nützlich ist dies in Bereichen wie

Qualitätskontrolle, Gesichtserkennung und bei automatisierten Inspektionen.

- *Tools für robotergestützte Prozessautomatisierung (Robotic Process Automation, RPA),* die repetitive Aufgaben wie Dateneingabe und Rechnungsbearbeitung automatisieren.
- *Tools für prädiktive Analytik,* die mithilfe von statistischen Algorithmen und Techniken des maschinellen Lernens künftige Ergebnisse auf Basis historischer Daten vorhersagen und bei Entscheidungsprozessen helfen.
- *Generative KI wie z. B. große Sprachmodelle (Large Language Models, LLM),* die Inhalte wie Texte, Bilder oder Code auf Basis von Eingabedaten generieren und für die Erstellung von (multimedialen) Inhalten, Marketing und weitere Zwecke genutzt werden können.
- Anwendung mit *Retrieval Augmented Generation (RAG),* die Inhalte auf Basis von Daten generiert, welche nicht aus dem KI-Modell selbst stammen, sondern vom Associate selbst eingegeben oder aus einer externen- Datenquelle abgefragt wurden.
- *Übersetzungsmanagementsystem (Translation-Management-Systeme, TMS),* die mit Automatisierung arbeiten und in die einige KI-Elemente integriert sein können, um Arbeitsabläufe bei Übersetzungen zu verbessern, z. B. die Überprüfung früherer Übersetzungen und die Integration neuer Inhalte in das Layout des Originaldokuments.

Assets - Hardware und/oder Software (von Gore bereitgestellt oder verwaltet), oder andere Komponenten aus der IT-Umgebung von Gore, die den Geschäftsbetrieb unterstützen und im Eigentum von Gore stehen und/oder von Gore lizenziert, genutzt oder betrieben werden.

- *Hardware* umfasst u.a. Computer, Laptops, Tablets, Computerfestplatten, Netzwerk-Komponenten, Flash-Laufwerke/USB-Sticks und sonstige Speichergeräte, Workstations, Telefone, Mobilgeräte, Videokonferenzanlagen (einschließlich Teilen davon), Drucker, Scanner und/oder jede sonstige physische Technologie, die den Geschäftsbetrieb unterstützt.
- *Software* umfasst u.a. Betriebssysteme, Netzwerk-Applikationen, Messaging-Anwendungen wie E-Mail, Voicemail, Tools für Zusammenarbeit, Textverarbeitung, Tabellenkalkulation und weitere Datenanwendungen, Datenbanken, Web-Anwendungen und/oder beliebige weitere Programme, Anwendungen oder Software-Plattformen.

Inhalte - Daten, Informationen oder Unterlagen, die aufgrund von betrieblichen, rechtlichen oder regulatorischen Anforderungen einen geschäftlichen Wert besitzen.

Daten - Inhalte, bei denen es sich um eine symbolische Darstellung von etwas handelt, das im Hinblick auf seine Bedeutung teilweise von seinen Metadaten abhängt. Daten sind eine Sammlung von Fakten, beispielsweise Zahlen, Wörter, Messungen, Beobachtungen oder Beschreibungen von Dingen.

Datenschutzbeauftragter - Die Datenschutz-Grundverordnung (DSGVO) hat das Konzept des Datenschutzbeauftragten (DSB) in Europa eingeführt. Die Arbeit eines DSB hat das Ziel, für die Einhaltung aller einschlägigen Datenschutzgesetze zu sorgen; dazu überwacht er bestimmte Prozesse und arbeitet

mit den jeweiligen Aufsichtsbehörden zusammen.

Gore E-Mail-Konto - Ein Benutzerkonto (einschließlich Software, Speicherplatz und Hardware), das zu einer Gore Domain gehört und es dir ermöglich, E-Mails zu senden und zu empfangen.

Informationen - Inhalte mit kurzfristigem geschäftlichen Wert. Informationen sind in einem Kontext stehende Daten.

Internetzugang - Alle Ressourcen, die elektronische Kommunikation ermöglichen, insbesondere die Abfrage von Daten aus dem Internet, einschließlich zugehöriger Hardware und Software.

Intranet – Alle von Gore bereitgestellten Ressourcen, die elektronische Kommunikation im internen Netzwerk von Gore ermöglichen, einschließlich zugehöriger Hardware und Software.

Unterlagen – Inhalte, die als Nachweis für geschäftliche Handlungen, Entscheidungen oder Transaktionen dienen. Unterlagen sind vollständige und fertiggestellte Informationen in beliebigem Format (auf Papier oder elektronisch), die auf der Grundlage gesetzlicher, behördlicher oder betrieblicher Anforderungen über definierte Zeiträume aufbewahrt werden müssen.

Verwaltete Geräte – Persönliche Mobilgeräte, die für den Zugriff auf Gore Inhalte oder das Gore Netzwerk verwendet werden und auf denen die Gore Geräteverwaltungssoftware installiert und aktiviert ist.

- Siehe die Richtlinien zur Nutzung von Mobilgeräten.

Partner – Auftragnehmer, Dritte usw.

Nutzung von Gore Assets

Geschäftstätigkeiten für Gore müssen mithilfe von genehmigten Anwendungen oder verwalteten Geräten geführt werden. Andernfalls besteht die Gefahr, dass Gore Inhalte nicht ordnungsgemäß verarbeitet werden und weniger sicher sind.

Jeder Gore Partner ist mitverantwortlich dafür, dass Gore Inhalte geschützt sind und der Zugang zu Assets jeglicher Art nur einem dafür autorisierten Associate oder Partner gewährt wird.

Zugang

Gore Partner dürfen nur die Assets nutzen, für die ihnen der Zugang oder Zugriff gewährt wurde.

Wenn Gore Partner auf Gore Assets zugreifen oder den Zugriff darauf gewähren, müssen sie wie folgt vorgehen:

- Gore Partner müssen beim eigenen Zugriff bzw. bei der Gewährung des Zugriffs auf Gore Assets das „Need-to-Know“-Prinzip beachten.
- Gore Partner dürfen den Zugriff auf Gore Assets nur so lange wie nötig gewähren und müssen den Zugriff widerrufen, wenn geschäftliche Anforderungen nicht erfüllt wurden oder es Änderungen beim Commitment gab.
- Sofern erforderlich, müssen Gore Partner einen Zugriff über die geeigneten Kanäle (Verantwortlicher (Owner) für die Anwendung, Abteilung für Informationssicherheit usw.) beantragen.
- Wenn Gore Partner mit einem Partner arbeiten, der Zugriff auf Gore Assets haben wird, müssen sie sich an die „Gore Guide Richtlinien“ halten.
- Ein Fernzugriff auf das Gore Netzwerk ist nur über die von Gore autorisierten Methoden und Geräte gestattet.

Handhabung

Gore Partner müssen Gore Assets sicher und in Übereinstimmung mit den Bestimmungen der Richtlinie zur Sicherheitsklassifizierung (Security Classification Policy) und der Richtlinie zum Management von Unterlagen und Informationen (Records and Information Management Policy) handhaben.

Unzulässige Verwendungen

Die folgende Verwendung von Gore Assets ist Gore Partner nicht gestattet:

- Generell jede unrechtmäßige oder böswillige Nutzung, insbesondere in Fällen, in denen eine solche Nutzung den Ruf von Gore schädigen, zu finanziellen Verlusten für das Unternehmen führen oder eine Haftung des Unternehmens auslösen kann.
- Inhalte abrufen, herunterladen, anzeigen oder verbreiten, die als obszön, rassistisch, sexistisch, bedrohlich, beleidigend oder diskriminierend angesehen werden können.
- Bedrohliche, belästigende oder beleidigende Äußerungen tätigen oder diesen entsprechende Inhalte verwenden.
- Das Anzeigen von sonstigen am Arbeitsplatz unangemessenen Inhalten .
- Jeder Versuch, die von der Abteilung für Informationssicherheit oder dem Gore Security Team eingerichteten Sicherheitsmechanismen zu umgehen.
- Verwenden der Login-Daten von anderen Associates oder von Partnern.
- Verbindungsaufbau zum Gore Netzwerk mit einem nicht von Gore verwalteten Privatgerät.
- Verwenden des „Gore Guest“-WLAN für geschäftliche Zwecke.
- Errichten eines nicht genehmigten Drahtlosnetzwerks, das mit dem Gore Netzwerk verbunden ist sowie Zugriff auf ein nicht genehmigtes Drahtlosnetzwerk von einem Gore Standort aus.
- Die Inbetriebnahme oder Änderung vorhandener Assets oder die Beteiligung an Aktivitäten, die vorsätzlich Gore Assets beeinträchtigten oder eine Fehlfunktion oder einen Ausfall solcher Assets verursachen.
- Die Manipulation oder Deaktivierung der bei Gore eingesetzten Virenschutz- oder Verschlüsselungsfunktionen.
- Die Installation einer privaten oder bei Gore nicht standardmäßig verfügbaren Software auf einem Gore Asset (ausgenommen persönliche Apps auf einem Smartphone oder Tablet).
- Das Speichern von Gore-Daten oder -Informationen auf einem persönlichen Gerät (Computer, Telefon, Cloud-Speicher usw.), es sei denn, das Gerät verfügt über Gore-Software zur Verwaltung der auf dem Gerät gespeicherten Informationen (siehe Bring Your Own Device User Agreement) oder in einer Cloud oder einem Netzwerk, das nicht von der Gore Informationssicherheit geprüft wurde.

Überwachung

Soweit gesetzlich zulässig, behält sich Gore das Recht vor, die Nutzung von Gore Assets durch Associates oder Partner, auch ohne vorherige Ankündigung, einzusehen, auszusetzen, abzubrechen, aufzuzeichnen oder auf andere Weise zu kontrollieren („zu überwachen“), um die Einhaltung der

Richtlinien und Standards von Gore zu gewährleisten.

Bei der Überwachung wird Gore alle angemessenen Anstrengungen zur Einhaltung des länderspezifischen Rechts unternehmen, um zu gewährleisten, dass personenbezogene Daten („Personal Information“, „PI“) nur für den vorgesehenen und bestimmten Zweck verwendet werden.

Wann immer zulässig und möglich, wird die Überwachung automatisiert durchgeführt. Bei der Überwachung werden bestimmte Informationen erfasst. Die Arten von Informationen, die unter bestimmten Umständen und für bestimmte Zwecke erfasst werden können, sind im beigefügten Anhang B zu finden.

Soweit dies nach geltendem Recht zulässig ist, kann Gore bestimmte sensible Informationen (z. B. der Exportkontrolle unterliegende Informationen, personenbezogenen Daten oder vertrauliche Gore Technologie, usw.) überwachen, um gesetzliche Bestimmungen einzuhalten und um die Reputation des Unternehmen und der Unternehmensmarken sowie die Wettbewerbsvorteile des Unternehmens zu schützen.

Soweit einschlägig, werden für eine solche Überwachung die länderspezifischen Verfahrensweisen und lokales Recht angewendet. Weitere Informationen darüber, wie die Überwachung für Associates durchgeführt wird, sind im beigefügten Anhang A zu finden.

Wenn Gore Grund zu der Annahme hat, dass ein Gore Partner gegen diese Richtlinie oder andere zugehörige Richtlinien verstößt, wird Gore, soweit nach geltendem Recht zulässig, versuchen, den betroffenen Gore Partner zu identifizieren. Gore kann in Rücksprache mit dem zuständigen Datenschutzbeauftragten ggf. mit einer gezielten Überwachung beginnen.

Wenn Gore aufgrund der Überwachung vermutet, dass es zu einem Verstoß gegen diese Richtlinie gekommen ist, dann gilt Folgendes:

- Gore behält sich das Recht vor, Gore Partnern den Zugriff auf Gore Assets zu entziehen. Sofern angemessen, wird Gore Unternehmensinformationen, die sich weiterhin auf privaten Geräten befinden, löschen oder den Zugriff auf sie sperren (siehe „Bring Your Own Device User Agreement“).
- Gore ist berechtigt, Kopien von Inhalten, die im Rahmen von Überwachungsmaßnahmen erfasst wurden und die eine unangemessene Nutzung von Gore Assets durch einen Gore Partner zeigen, im Rahmen der geltenden Gesetze aufzubewahren. Gore ist auch berechtigt, Kopien solcher Inhalte oder eines Geräts, das solche Inhalte enthält, offenzulegen, falls dies im Rahmen eines Rechtsstreits oder einer Ermittlung erforderlich ist.

Private Geräte

Gore kann es Gore-Partnern gestatten, persönliche Geräte wie Smartphones oder Tablets zu verwenden, um auf Gore Assets oder Gore Informationsressourcen zuzugreifen. In diesen Fällen:

- Gore Partner müssen über das ITAC-Antragsverfahren eine Nutzungsvereinbarung unterzeichnen und Gore IT die Installation der Mobile Device Management Software erlauben. Die Mobile Device Management Software ermöglicht es der Gore IT-Abteilung, Gore-Inhalte und -

Anwendungen auf dem Gerät zu kontrollieren, oder
- In begrenztem Umfang kann der Zugang gemäß dem unten beschriebenen Ausnahmeverfahren gewährt werden.

Elektronische Kommunikation

Das E-Mail-System und andere Messaging-Services von Gore, wie beispielsweise Microsoft Teams oder andere von Gore verwaltete Instant-Messaging-Tools („IM“), sowie alle zugehörigen Informationen innerhalb dieser Tools, sind als Eigentum von Gore zu behandeln, sofern nicht anderweitig durch lokales Recht oder Gesetz geregelt. E-Mail- und IM-Konten von Gore sind für die geschäftliche Nutzung vorgesehen. In der gesamten elektronischen Kommunikation muss die Vertraulichkeit sensibler und personenbezogener Daten (im Allgemeinen durch den Einsatz von Verschlüsselung) im Einklang mit unserem Standard zur Sicherheitsklassifizierung (Security Classification Standard) gewährleistet sein.

Messaging-Apps

Gore sieht die Notwendigkeit, intern und extern über Instant Messaging- oder Kommuniktions-Apps zu kommuniziern. Wann immer möglich, empfehlen wir dringend, sowohl ein von Gore genehmigtes Gerät als auch eine von Gore bereitgestellte und gewartete Anwendung, Plattform oder ein Tools zu verwenden.

Wenn du über eine externe Messaging-App wie beispielsweise WhatsApp kommunizieren musst, übertrage niemals vertrauliche oder sensible Informationen; hierzu gehören auch personenbezogene Daten oder geistiges Eigentum.

Messaging sollte in erster Linie für logistische Zwecke verwendet werden. Speichere niemals Gore Geschäftsunterlagen in einer Instant Message oder einer Messaging-App. Alle Geschäftsunterlagen, beispielsweise Genehmigungen und Transaktionsbelege, müssen gemäß den festgelegten Geschäftsprozessen aufbewahrt werden.

Aufzeichnung

Gore Partner können Tools (wie z. B. Microsoft Teams oder andere Software) zum Aufzeichnen und Transkribieren von Meetings und Interaktionen verwenden. Gore Partner müssen Teilnehmer vor dem Beginn des Meetings, vorzugsweise in der Einladung zu dem Meeting, über die Aufzeichnung oder Transkription informieren und Teilnehmern die Möglichkeit geben, sich dagegen zu entscheiden. Wenn ein Aufzeichnungs-Tool nicht während des gesamten Meetings einen deutlich sichtbaren Hinweis anzeigt, muss der Host später hinzukommende Teilnehmer über die Aufzeichnung des Meetings informieren.

Bei Hybrid- oder automatisch aufgezeichneten Meetings muss der Host alle Teilnehmer in der Einladung zu dem Meeting oder dem Meeting-Chat über die Aufzeichnung informieren. In Pausen oder bei nicht geschäftsbezogenen Diskussionen muss die Aufzeichnung angehalten werden.

Soweit auf Meetings sensible personenbezogene Daten oder andere sensible Themen besprochen werden, sollte dies nicht aufgezeichnet werden. Beispiele sind u. a. Gespräche über Patientendaten, Beiträge (Contribution) und Vergütung (Compensation).

Gore KI-Tools

Gore Partner werden dazu ermutigt, **von Gore bereitgestellte** KI-Tools zur Steigerung der Produktivität, Optimierung von Arbeitsabläufen und zur Unterstützung von Entscheidungsprozessen einzusetzen. Wenn Gore Partner unternehmens- oder personenbezogene Daten in solche Gore KI-Tools eingeben, müssen sie sicherstellen, dass diese Daten korrekt und relevant sind und die

Datenschutz- und Sicherheitsprotokolle einhalten. Gore Partner dürfen keine vertraulichen, sensiblen, firmeneigenen oder gesetzlich geschützten Daten in nicht von Gore bereitgestellte KI-Tools hochladen oder eingeben, es sei denn, dies wurde ausdrücklich vom Leader genehmigt und von der Abteilung für Informationssicherheit überprüft. Gore Partner müssen sich außerdem bewusst machen, dass KI-generierte Ergebnisse manchmal irreführend oder nicht richtig sein können. Deshalb ist es sehr wichtig, die Richtigkeit und Zuverlässigkeit des KI-Outputs zu überprüfen, bevor auf seiner Grundlage Entscheidungen getroffen oder Maßnahmen ergriffen werden. Gore Partner sind für die mithilfe von KI-Tools generierten Ergebnisse verantwortlich und müssen bereit sein, diese Ergebnisse zu erklären und zu begründen. Der Missbrauch von KI-Tools, beispielsweise Generieren irreführender Informationen, Verstoß gegen Rechte an geistigem Eigentum oder Automatisieren von Aufgaben ohne angemessene Aufsicht, ist streng untersagt und kann Disziplinarmaßnahmen bis hin zur Kündigung des Beschäftigungsverhältnisses zur Folge haben.

Compliance und Meldungen

- Gore Partner müssen alle zu dieser Richtlinie bereitgestellten Schulungen absolvieren; hierzu gehört auch die verpflichtende Schulung zu Datenschutz und Informationssicherheit.
- Gore Partner, die einen tatsächlichen oder vermuteten sicherheitsrelevanten Vorfall oder eine unbefugte Nutzung oder einen unbefugten Zugriff auf Gore Assets bemerken, müssen umgehend ITAC benachrichtigen.
- Ein Verstoß gegen diese Richtlinie kann, vorbehaltlich der geltenden Gesetze, Disziplinarmaßnahmen bis hin zur Kündigung des Beschäftigungsverhältnisses sowie sonstige rechtliche Schritte zur Folge haben.

Anhang A - Regionale Abweichungen

Abschnitt 1	Informationen zur Überwachung für Italien	Legt zusätzliche Bestimmungen fest, die für Associates in Italien relevant sind.

Abschnitt 1 – Informationen zur Überwachung für Italien

Die in der Richtlinie beschriebenen Überwachungsmaßnahmen werden von Gore nur innerhalb der Grenzen und unter Einhaltung der Modalitäten durchgeführt, die im italienischen Arbeits- und Datenschutzrecht festgelegt sind.

Nach Artikel 4, Abs. 1 des Gesetzes vom 20. Mai 1970, Nr. 300, führt Gore insbesondere keine dieser Maßnahmen zu dem Zweck durch, die Tätigkeit von Associates am Arbeitsplatz zu überwachen, sofern dies nicht zur Einhaltung der italienischen Datenschutzgesetze erforderlich ist.

Gore hat dennoch Sicherheits-Tools installiert, die die indirekte Möglichkeit auslösen können, die Tätigkeit von Associates aus der Ferne zu überwachen.
Diese Installation ist notwendig, um die Organisation und die Assets von Gore angemessen zu schützen. Wie weiter oben ausgeführt, dient dies der Sicherheit, dem Schutz vor Datenlecks bei sensiblen Daten, der Betrugserkennung sowie der Einhaltung des geltenden Rechts und dem Schutz vor Missbrauch, aus dem Gefahren für die Organisation und Assets von Gore entstehen.

Wann immer möglich, wird die Überwachung automatisiert und/oder nach dem Zufallsprinzip durchgeführt. Wenn Gore jedoch Grund zu der Annahme hat, dass der Gore Partner Fehlverhalten an den Tag gelegt hat und dieses Fehlverhalten möglicherweise die Organisation, die Sicherheit oder die Assets von Gore gefährdet, kann Gore gleichwohl versuchen, einen Gore Partner zu identifizieren.

Anhang B – Arten von Informationen, Umstände und Zweck bei der Überwachung der Aktivität von Gore Partnern in Gore Assets.

Informationen, die ggf. bei der Überwachung erfasst und protokolliert werden

Netzwerkaktivität, einschließlich:

- Datum/Uhrzeit
- Benutzer-ID, Geräte-ID, Arbeitsstations-ID, IP-Adresse und andere eindeutige Kennungen
- Physischer und logischer Pfad des Datenflusses, einschließlich Ursprung und Ziel
- Datenvolumen
- Aktionen
- Schlüsselwörter (z. B. „vertraulich“, „nur für den internen Gebrauch“, usw.).

Internetaktivität, einschließlich:

- Datum/Uhrzeit
- Benutzer-ID
- Ursprungs-IP-Adresse

- Zieladresse (sofern zulässig)
- Übertragenes Datenvolumen

Eingehende und ausgehende E-Mails:

- Datum/Uhrzeit
- Absender- und Empfängeradresse
- Nachrichten-ID
- Nachrichtengröße
- Betreff
- Schlüsselwörter für sensible Daten (z. B. „vertraulich“, „nur zur internen Verwendung“, usw.)
- Nur bei E-Mails, bei denen „Markierte Inhalte“ festgestellt wurden: E-Mail-Text und Anhänge.

Tools zur Verhinderung von Datenverlusten suchen nach Schlüsselwörtern (wie z. B. „Patienten-ID“) und Mustern in den Daten, um potenzielle Datenlecks sensibler Daten (wie z. B. Kunden, Patienten im Gesundheitswesen oder sensible Daten von Gore) zu erkennen. Diese Tools überwachen ausgehende E-Mails und ausgehenden Datenverkehr von Laptops, Desktops und der Cloud-Nutzung (Datenverkehr im Internet, in der Cloud, auf USB/CD/DVD, Druckern und Netzlaufwerken) und kennzeichnen bestimmte Elemente.

Verarbeitete Daten (die auf den jeweiligen Benutzer, das Gerät und/oder den Standort verweisen) werden nur für die folgenden Zwecke verwendet:

- Analyse und Korrektur technischer Fehler.
- Gewährleistung der Systemsicherheit, einschließlich der Pflege der Listen blockierter Internetseiten (sog. „Schwarze Liste“).
- Optimierung und Zugangskontrolle des Netzwerks.
- Kontrolle des Datenschutzes.

Abschnitt 2: Spezifische Beispiele für die Überwachung und deren Zweck:

- Schutz von Gore Assets vor unbefugter Offenlegung, Löschung oder Änderung.
- Einhaltung und Durchsetzung rechtlicher Anforderungen und der Richtlinien von Gore sowie Durchführung diesbezüglicher Untersuchungen.
- Schutz von Systemen und Netzwerken des Unternehmens vor Viren, Trojanern und anderer Malware.
- Schutz von Systemen und Netzwerken des Unternehmens vor unberechtigtem Zugriff und/oder unberechtigter Manipulation.
- Wahrung gesetzlicher Rechte von Gore und anderen sowie zu deren Schutz und zur dahingehenden Prävention; und
- Sofern dies aufgrund von Gesetzen, Vorschriften, Gerichtsbeschlüssen oder auf Anfrage oder Forderung der zuständigen Behörden oder Strafverfolgungsbehörden erforderlich ist.