GEUTEBRÜCK

Europäische Datenschutz-Grundverordnung (DS-GVO) in der Videoüberwachung

Ausgabe Bundesrepublik Deutschland Stand: 7/2018

VALUE IMAGING VIDEO SECURITY

Inhaltsverzeichnis

1. Allgemeines zur DS-GVO

Seit dem 25. Mai 2018 ist die Europäische Datenschutz-Grundverordnung (DS-GVO) nach einer Übergangszeit von zwei Jahren in Deutschland unmittelbar anwendbar. Die Verordnung enthält neue Regeln zur Verarbeitung personenbezogener Daten von in der EU befindlichen Personen. Gleichzeitig zur DS-GVO ist ein neugefasstes Bundesdatenschutzgesetz (BDSG-neu) in Kraft getreten.

Die DS-GVO stellt zum einen Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5) und für die Rechtmäßigkeit der Verarbeitung (Art. 6) auf. Zum anderen formuliert sie Pflichten für Verantwortliche, Auftragsverarbeiter und Datenschutzbeauftragte, räumt den Betroffenen weitreichende Auskunftsrechte ein, regelt die Befugnisse der Aufsichtsbehörden (einschließlich der Verhängung drastischer Bußgelder) und begründet Haftungsansprüche für Betroffene, denen aufgrund eines Verstoßes gegen den Datenschutz ein materieller oder immaterieller Schaden entstanden ist.

Die Videoüberwachung wird nicht explizit in der DS-GVO geregelt. Das BDSG-neu hingegen enthält in § 4 Regelungen zur Videoüberwachung in öffentlich zugänglichen Räumen, die dem bisherigen § 6b BDSG entsprechen. Auch wenn die Datenschutzbehörden bezweifeln, ob der Gesetzgeber dazu ermächtigt war (es fehlt eine entsprechende Öffnungsklausel in der DS-GVO), sind diese Regelungen geltendes Recht in Deutschland.

Trotzdem ist in Bezug auf die Geltung und Auslegung der neuen Vorschriften noch vieles im Unklaren, insbesondere, was den datenschutzkonformen Betrieb von Videoüberwachungsanlagen angeht. Die Zeit wird zeigen, wie die Anforderungen genau zu deuten sind.
Daher erfolgen die nachfolgenden Informationen ohne Gewähr und können eine rechtliche Beratung im Einzelfall nicht ersetzen.
.

2. Planung der Videoüberwachungsanlage

Der Betreiber einer Videoüberwachungsanlage ist Verantwortlicher im Sinne der DS-GVO und hat einen datenschutzkonformen Betrieb sicherzustellen. Der Errichter schuldet keine rechtliche Beratung, hat den Betreiber jedoch auf die datenschutzrechtliche Relevanz der Bilddatenerhebung hinzuweisen und diesen bei der Umsetzung seiner datenschutzrechtlichen Pflichten zu unterstützen. Dies betrifft auch die Rechenschaftspflichten des Betreibers aus Art. 5 Abs. 2 DS-GVO, die u.a. durch die Erstellung einer Dokumentation der eingesetzten Technik zu erfüllen sind.

Soweit der Errichter im Auftrag des Betreibers selber (Bild-)Daten verarbeitet (z.B. im Rahmen der Wartung oder als Service-Leitstelle), dann obliegen ihm eigene datenschutzrechtliche Pflichten, die weiter unten beschrieben werden.

Im Zuge der Planung sind von Betreiber und Errichter folgende Aspekte zu beachten.

2.1 Rechtmäßigkeit der Videoüberwachung

Jegliche Verarbeitung personenbezogener Daten unterliegt den Grundsätzen des Art. 5 DS-GVO, wonach Daten nur auf rechtmäßige Weise und für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen (Grundsätze der Rechtmäßigkeit und Zweckbindung), wobei die Erhebung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss (Grundsatz der Datenminimierung) und die Verarbeitung für die Betroffenen in transparenter Weise zu erfolgen hat (Grundsatz der Transparenz).

Im Sinne eines Verbotes mit Erlaubnisvorbehalt ist die Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 DS-GVO nur rechtmäßig, wenn mindestens eine der nachfolgenden Bedingungen zutrifft:

(a) Einwilligung der betroffenen Person
(b) Zur Erfüllung eines Vertrags
(c) Zur Erfüllung rechtlicher Pflichten
(d) Zum Schutz lebenswichtiger Interessen
(e) Zur Wahrnehmung eines öffentlichen Interesses
(f) Zur Wahrung der berechtigten Interessen des Verantwortlichen

Videoüberwachung lässt sich i.d.R. nur unter Anwendung des letzten Tatbestandes rechtfertigen. Dabei muss stets eine Abwägung mit den Persönlichkeitsrechten der betroffenen Personen stattfinden. Das gilt auch bei Anwendung von § 4 BDSG-neu, wonach eine Überwachung öffentlich zugänglicher Räume nur zulässig ist, soweit sie zur Wahrung des Hausrechtes oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

2.2 Risikoanalyse – berechtigte Interessen

Bevor ein Videosicherheitssystem entworfen wird, muss der Betreiber eine Bedrohungsabschätzung durchführen. Er muss in der Lage sein, die Überwachung zu begründen und belegen können, dass keine anderen Mittel mit vertretbarem Kostenaufwand zum gleichen Ziel führen können (Stichwort: Erforderlichkeit).

Bei der Risikoanalyse sind Risiken wie Bedrohung, Betrug, Brandstiftung, Diebstahl, Einbruch, Raub, Sabotage, Vandalismus usw. unter Berücksichtigung bekannter Vorfälle, Umfeld, Eintrittswahrscheinlichkeiten und mögliche Auswirkungen ebenso wie abstrakte Risiken (z.B. bei Juwelieren, Tankstellen und Parkhäuser) zu beachten.

Aus den Risiken lassen sich die Zwecke der Überwachung ableiten. Beispiele dazu sind Abschreckung, Aufklärung, Arbeitssicherheit, Objektschutz, Zutrittskontrolle.

Anhand der Risikobewertung können die Komponenten, Teilsysteme und Funktionen der geplanten Anlage einem angemessenen Sicherungsgrad aus der Normenreihe EN 62676-X-X zugeordnet werden. Hierbei kommt es u.a. darauf an, das erforderliche Niveau der Datensicherheit zu bestimmen.

2.3 Betriebsanforderungen

Zur Planung der Anlage gehört die Erstellung der Betriebsanforderungen. Hier wird u.a. der Zweck der Anlage, die erforderliche Bildqualität, die Aufzeichnung der Bilder, die Bedienung der Systeme und die Weitergabe der Daten festgelegt.

G Tipp:
Der BHE bietet hierzu eine Checkliste an:
Gesprächsleitfaden zur Videoanalyse.

In der Regel werden bei einer Videoüberwachung personenbezogenen Daten verarbeitet. Dies ist der Fall, wenn Personen erkannt werden können oder z.B. Nummernschilder lesbar sind. Das hängt wiederum von Position, Qualität und Auflösung der Kameras sowie dem Zeitpunkt der Nutzung bzw. Speicherung ab.

2.4 Bildqualität

Der Zweck der Anlage bzw. der Aufzeichnung bestimmt die geforderte Bildqualität. Die Bildqualität wiederum sagt aus, ob das Bildmaterial datenschutzrelevant ist oder nicht.

Die Norm EN 62676-4 unterteilt die Bildqualität in diverse Kategorien.

- Eine geringe Bildqualität reicht aus zum Überwachen oder Detektieren. Die Qualität der Bilder reicht i.d.R. nicht aus, um Personen zu erkennen oder Nummernschilder lesen zu können. In diesem Fall werden keine personenbezogenen Daten verarbeitet, es sei denn, eine Erkennbarkeit ist durch die Verknüpfung mit anderen Daten möglich.

- Bei mittlerer Bildqualität ist es möglich, Personen zu beobachten oder zu erkennen. Zwar reicht die Bildqualität in aller Regel nicht aus, um Personen zweifelsfrei zu erkennen, eine Zuordnung der Personen kann sich aber aus dem Kontext ergeben, in dem die Bilder aufgezeichnet werden. Also abhängig von dem Kontext handelt es sich um personenbezogene Daten.

- Die höherwertige Bildqualität lässt das Identifizieren bzw. Überprüfen von Personen zu. Bei dieser Bildqualität ist in jedem Fall die zweifelsfreie Zuordnung zu einer Person möglich und ist die Bildbearbeitung eindeutig datenschutzrelevant.

- Detaillierte Kriterien für die Bildqualität und deren Prüfmethoden finden Sie in der EN 62676-4 – Videoüberwachungsanlagen für Sicherungsanwendungen – Teil 4 Anwendungsregeln. Die Kriterien wurden auch in der VDS 2366 und die Bundeseinheitliche Richtlinie ÜEA (Polizei) übernommen.

2.5 Datenschutzfolgeabschätzung – Art. 35 DS-GVO

Hat eine Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände oder der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche gemäß Art. 35 DS-GVO vorab eine (dokumentierte) Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge durchzuführen.

Eine solche Datenschutz-Folgeabschätzung (DSFA) ist gemäß Art. 35 Abs. 3 insbesondere dann erforderlich, wenn eine „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“ stattfindet, worunter nach den Erwägungsgründen zu dieser Vorschrift die Überwachung mittels „optoelektronischer Vorrichtungen“ verstanden wird.

Bei umfangreicher und systematischer Videoüberwachung öffentlich zugänglicher Bereiche (z.B. Verkaufsräume, Empfang, Außenbereiche einer Liegenschaft) wird danach immer eine DSFA durchzuführen sein. Dies gilt erst recht, wenn dabei Auswertungen anhand biometrischer Merkmale stattfinden. Diese gehören gemäß Art. 9 Abs. 1 DS-GVO zu besonders schützenswerten Kategorien personenbezogener Daten.

Indikatoren für „weiträumige“ Videoüberwachung sind:

- Flächendeckend
- Bewegliche Kameras
- Details erkennbar: Erkennen, Identifizieren, Überprüfen
- Aufzeichnung > 48h
- Mitarbeiter betroffen

Tipp:
Die Gesellschaft für Datenschutz und Datensicherheit e.V. hat dazu die **GDD-Praxishilfe DS-GVO X** herausgegeben, mit Hilfestellungen dazu, ob und wann die DSFA durchzuführen ist. Sehen Sie dazu auch das **Kurzpapier Nr. 5 „Datenschutz-Folgeabschätzung“** von der DSK.
Die Datenschutzbehörden haben kürzlich eine **„Vorläufige Liste von Verarbeitungsvorgängen“** nach Art. 35 Abs. 4 DS-GVO herausgegeben, aus der sich die Voraussetzungen für die Durchführung einer DSFA ablesen lassen.

Wenn aus der Datenschutz-Folgeabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko für die Betroffenen zur Folge hätte, muss der Betreiber die Aufsichtsbehörden konsultieren.
(Art. 36 DS-GVO)

2.6 Nachweispflichten

Betreiber müssen auf Anforderung der Datenschutzbehörden nachweisen können, dass die Bilddatenverarbeitung datenschutzkonform erfolgt (Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO). In Bezug auf die Videoüberwachung sollte eine aussagekräftige Projektdokumentation erstellt werden. Dabei empfiehlt sich folgende Arbeitsteilung:

Betreiber:
- Lageplan – überwachte Bereiche
- Betriebsanforderungen
- Prüfplan
- Datenschutzmanagementsystem

Errichter:
- Anlagenentwurf
- Aufstellung der eingesetzten Kameras (Typen und Auflösung)
- Ausführungsplanung
- Prüfergebnisse, Kamerapläne mit Sichtbereichen
- Anlagenbeschreibung (VdS-Attest) - Siehe BHE für BHE-Mitglieder

G Tipp:
Der BHE bietet hierzu diverse Vorlagen auf der **Homepage** an (nur für BHE-Mitglieder)

2.7 Datenminimierung

Die DS-GVO beschreibt in Art. 5 Abs. 1 die Datenschutzgrundsätze, die auch bei einer Videoüberwachung beachtet werden müssen. Dies betrifft insbesondere die Datenminimierung (Abs. 1 c). Bezogen auf die Videoüberwachung dürfen nur die Bilder verarbeitet werden, die zum Zweck der Anlage erforderlich sind bzw. dazu beitragen.

G Tipp:

Geutebrück bietet hierzu die passenden Features an:

- Auswahlmöglichkeit, welche Kameras aufgezeichnet werden
- Privacy Masking: Schwärzen von Bildbereichen in Live-, Speicher- und Exportbilder
- Privacy Masking in Kameras (Live, Speicher und Export)
- Motion Privacy: Verpixelung von Personen bzw. Gesichtern bei Live-, Speicher- und Exportbildern
- Thermalkameras (Live- und Speicherbilder)
- Tourenbetrieb bei Dome-Kameras
- Dome-Kameras automatisch zurück in Home Position

2.8 Speicherbegrenzung

In den meisten Fällen werden die Aufzeichnungen nur für einen begrenzten Zeitraum benötigt, z.B. bis klar ist, ob es ein relevantes Ereignis gegeben hat. Danach müssen die Bilder gemäß Art. 5 Abs. 1 e) DS-GVO sowie § 4 Abs. 5 BDSG-neu gelöscht werden.

G Geutebrück-Systeme werden so betrieben, dass die vorhandenen Daten nach einer festgelegten Frist von einigen Tagen überschrieben werden.

Hinweis: Eine maximale Speicherdauer ist rechtlich nicht eindeutig festgelegt. Dennoch haben sich in der Praxis Speicherfristen von 48 bis 72 Stunden etabliert. Ggf. sind davon abweichende Fristen zur Überbrückung von Wochenenden oder Feiertagen oder aus anderen Gründen zulässig.

Tipp:
Der Düsseldorfer Kreis hat eine **Orientierungshilfe** „Videoüberwachung durch nicht öffentliche Stellen" herausgegeben. Unter Punkt 2.3.1. wird die Speicherdauer behandelt.

Aufzeichnungen, die als Beweismittel benötigt werden, sollten manipulationssicher auf gesonderte Datenträger gespeichert werden, bevor das ursprüngliche Videoband gelöscht wird.

3. Videoüberwachung im Arbeitsumfeld

Da sich die Beschäftigten einer Videoüberwachung im Arbeitsumfeld kaum entziehen können, sind an deren Zulässigkeit besonders hohe Anforderungen zu stellen. Soweit sich die Arbeitnehmer mit derartigen Maßnahmen nicht ausdrücklich einverstanden erklärt haben, oder eine Kollektivvereinbarung vorliegt, muss sich die Zulässigkeit derartiger Maßnahmen an den hierzu in der DS-GVO und dem BDSG-neu aufgestellten Grundsätzen messen lassen.

3.1 Einwilligung

Erfolgt die Videoüberwachung von Beschäftigten auf der Grundlage einer Einwilligung, so sind gemäß §26 Abs. 2 BDSG-neu für die Beurteilung der Freiwilligkeit insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Personen sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Freiwilligkeit kann danach vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen (z. B. bei konkreten Bedrohungslagen). Die Einwilligung bedarf in der Regel der Schriftform, wobei der Arbeitgeber die beschäftigte Person zuvor entsprechend den Vorgaben des Artikel 7 Abs. 3 DS-GVO über die Zwecke der Datenverarbeitung und über ihr Widerrufsrecht aufzuklären hat. Denn eine solche Einwilligung kann jederzeit widerrufen werden, allerdings nur mit Wirkung für die Zukunft (vgl. Art. 7 Abs. 3 DS-GVO).

3.2 Datenschutzrechtliche Erlaubnistatbestände

Fehlt es an einer Einwilligung, so ist die Datenerhebung im Beschäftigungsverhältnis gemäß § 26 Abs. 1 Satz 1 BDSG-neu nur dann zulässig, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder für dessen Beendigung erforderlich ist. Diese Regelung entspricht fast wortgleich dem bisherigen § 32 Abs. 1 BDSG, und lässt Raum für die Anwendung im Einzelfall. Nach bisheriger Auslegung dürften Videoüberwachungslösungen zulässig sein, die der Zutrittskontrolle, der Sicherheit der Beschäftigten und den schützenswerten Interessen des Verantwortlichen dienen, wenn den Arbeitnehmern ausreichende Rückzugsmöglichkeiten eingeräumt werden und die Maßnahme auch sonst verhältnismäßig ist.

> **Hinweis:** Nur ausnahmsweise ist auch die verdeckte Überwachung eines Mitarbeiters erlaubt, wenn die strengen Voraussetzungen des § 26 Abs. 1 Satz BDSG-neu eingehalten werden. Danach müssen zu dokumentierende tatsächliche Anhaltspunkte den konkreten Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat.

Des Weiteren dürfen Art und Ausmaß der Überwachungsmaßnahme im Hinblick auf den Anlass nicht unverhältnismäßig sein und es dürfen die schutzwürdigen Interessen der betroffenen Person nicht überwiegen. Diese Regelung entspricht der ständigen Rechtsprechung des Bundesarbeitsgerichtes, welches dem Arbeitgeber im Falle einer „Notwehrlage“ auch die verdeckte Datenerhebung gestattet.

3.3 Kollektivvereinbarungen

Gemäß § 26 Abs. 6 BDSG-neu bleiben die Beteiligungsrechte der Interessenvertretung der Beschäftigten durch die datenschutzrechtlichen Regelungen unberührt. Damit ist gemeint, dass neben dem Datenschutz auch das kollektive Arbeitsrecht zu beachten ist, wonach die Erfassung personenbezogener Daten von Mitarbeitern der Mitbestimmung unterliegt. Dies erstreckt sich gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz auf die Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

Hinweis: Die Mitbestimmung erfolgt i.d.R. durch den Abschluss von Betriebsvereinbarungen, die von der Unternehmensleitung mit den Vertretern der Beschäftigten ausgehandelt und in denen die Einzelheiten der Videoüberwachung festgelegt werden. Haben die Parteien eine solche Betriebsvereinbarung getroffen, so sind die danach ausgeführten Videoüberwachungsmaßnahmen auch in datenschutzrechtlicher Hinsicht zulässig. Dies ergibt sich aus § 26 Abs. 4 BDSG-neu, wonach die Verarbeitung personenbezogener Daten von Beschäftigten (einschließlich besonderer Kategorien personenbezogener Daten) für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen zulässig sind.

Hinweis: Verfügt das Unternehmen über keinen Betriebsrat (z.B. weil es nicht die dafür erforderliche Betriebsgröße aufweist), so sollte der Arbeitgeber frühzeitig – d. h. zu Planungsbeginn – die betroffenen Mitarbeiter über die Einführung und Anwendung der Videoüberwachungsanlage aufklären und dabei deutlich machen, dass die Überwachung nicht der Verhaltens- und/oder Leistungskontrolle dient. Einwilligungserklärungen der Mitarbeiter sind nur in Ausnahmefällen einzuholen, weil der Arbeitgeber beim Widerruf einer Einwilligung in Rechtfertigungsnot kommen könnte. Vielmehr sollte der Arbeitgeber den Mitarbeitern die Gründe für die Überwachung, die vorgenommene Interessenabwägung und die Maßnahmen zum Schutze der erhobenen Daten transparent darlegen und all dies unter Berufung auf die einschlägigen Erlaubnistatbestände in seinem Verfahrensverzeichnis (und einer i.d.R. durchzuführenden Datenschutz-Folgeabschätzung) beweiskräftig protokollieren.

G Tipp:
Weiteres hierzu ist dem **DSK Kurzpapier Nr. 14 „Beschäftigten-schutz“** zu entnehmen.

4. Technische und organisatorische Maßnahmen

Der Betreiber der Videoanlage muss gemäß Art. 5 Abs. 1 f sowie Art. 25 und 32 DS-GVO alle erforderlichen technischen und organisatorischen Maßnahmen (sog. TOM's) ergreifen, um den Zugriff auf die Daten durch Unbefugte zu verhindern. Auch Videodaten können für Täter interessant sein, etwa zur Ausforschung der abgebildeten Personen oder zur Vorbereitung von Straftaten. Aus diesem Grund erhält das Thema Cyber-Security in der Videoüberwachung einen zunehmend hohen Stellenwert.
Natürlich trägt die richtige Auswahl der eingesetzten Überwachungssysteme und Kameras zur Datensicherheit bei.

4.1 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung gemäß Art. 25 DS-GVO (Privacy by Design, Privacy by Default)

Videoüberwachungslösungen von Geutebrück unterstützen mit einer Vielzahl von Features den datenschutzkonformen Betrieb. Dabei orientiert sich die nachfolgende Darstellung an den in § 64 BDSG-neu formulierten Anforderungen an die Sicherheit der Datenverarbeitung.

Zugriffskontrolle:

- Zentrales Zugriffsrechtemanagement
- Berechtigungen arbeitsplatzabhängig, für Live- und Speicherbilder getrennt
- Berechtigungen auf Kameraebene
- Berechtigungen mit Zeithorizont
- Vier Augen-Prinzip
- Steuerung beweglicher Kameras mit Prioritäten entsprechend Alarm und Nutzerlevel
- Einbindung in Domain mit Single-Sign-On

- Passwortgeschützter Zugang
- Passwörter verschlüsselt mit SHA-256
- Verschlüsselte Datenspeicherung (proprietäres Format GBF mit AES-256)
- Verschlüsselung zwischen allen Systemkomponenten
- Bitlocker Integration in Windows zur Verschlüsselung von Laufwerken (auch virtuell)

G Tipp:
Sehen Sie dazu das **Statement zur Geutebrück Systemsicherheit**.

Weitergabekontrolle:
- Passwortgeschützte und verschlüsselte Exportfiles mit generischem Videoformat MP4/H264EAW mit Geutebrück-RSH-1024-Signature
- Exportfiles mit Wasserzeichen mit M4A-Signature
- Einstellbare Speichermöglichkeiten für den Export
- Zertifizierte Schnittstellen (SDK) für die Anbindung an G-Core

G Tipp:
Weitere Hinweise finden Sie beim BHE: **Cyber Security bei Videoanlagen**.

Eingabekontrolle:
- Verbindliche Zeitangabe beim Gesamtsystem
- Audit-Trail: Manipulationssichere Protokollierung von benutzerbezogenen Aktivitäten, z.B.
  - Anmeldung am Arbeitsplatz
  - Versuche zu Aktionen ohne Berechtigung
  - Auswahl und Dauer der betrachteten Kameras
  - Ansehen von Speicherbildern
  - Suchen von Bildern (Motion Search)
  - Export von Bildern und wohin
  - Änderungen von Einstellungen, Bearbeitung von Alarmen

Verfügbarkeitskontrolle:
Zur Gewährleistung der Verfügbarkeit der Daten bietet Geutebrück

- Redundanzsysteme Multispare
- Failover
- Edge Recording.

Wo immer möglich, sind die Features werksseitig so ausgelegt, dass zunächst der höchstmögliche Datenschutz gewährleistet wird (Privacy by Design).

- Einschränkung der Berechtigungen auf Administratoren
- Verständliche Installations- und Bedienungsanleitungen sowie Onlinehilfen

G Tipp:
Schulungen und Webinare zur optimalen Einstellung und den Umgang mit Geutebrück-Lösungen. Bitte erkundigen Sie sich hierzu bei der **Geutebrück-Akademie**.

4.2 Maßnahmen zum Datenschutz und zur Datensicherheit durch den Betreiber und Installateur

Abgesehen von den in den Videolösungen integrierten Sicherungsmaßnahmen, muss der Betreiber und Installateur ebenfalls geeignete Maßnahmen zur Datensicherheit ergreifen, um den Zugriff auf Daten durch Unbefugte zu unterbinden (Privacy by Default).

a) Physikalische Sicherheit (Zutritts- und Zugangskontrolle)

- Zugang zu Gebäuden
- Zugang zu Servern
- Zugang zu Terminals

b) Organisatorische Maßnahmen

- Schulungen der Mitarbeiter/Wachdienst
- Verträge mit Dienstleistungsunternehmen im Sinne der Datenauftragsverarbeitung gemäß Art. 28 DS-GVO (z.B. für externe Wachdienstunternehmen)
- Festlegung von Verfahren für den Umgang mit den Daten
- Anfragen von Betroffenen, Vorgehensweise bei Datenpannen, Passwortmanagement

c) Technische Maßnahmen bei der Inbetriebnahme

- Hardening von Systemen

G Tipp:
Sehen Sie auch den Geutebrück **Hardening Guide**.
Geutebrück bietet diverse Dienstleistungen zur Unterstützung an, z.B. Patchmanagement. Bitte wenden Sie sich dazu an unseren Central Support.

d) Instandhaltung

Es wird empfohlen, die Systeme ständig auf dem neuesten Stand zu halten. Das betrifft sowohl die Netzwerk-Systeme und -Komponenten wie die Lösungen von Geutebrück.

G Tipp:
Geutebrück stellt regelmäßig Informationen bereit und empfiehlt eine zeitnahe Aktualisierung der betreffenden Systeme. Die jeweiligen Updates werden grundsätzlich vor Freigabe bezgl. der Auswirkung auf Funktionalität und Performance getestet. Aktuelle Versionen finden Sie als registriertes Mitglied im **WebClub** auf der Geutebrück-Homepage unter Software-Downloads.

- Neueste Releases von G-Core, G-SIM und weitere Produkte mit neuen Features und Verbesserungen in der Sicherheit
- Neue Firmware Versionen für Hardwarekomponenten und Kameras
- Neueste Bios-Updates der Mainboard-Hersteller
- Neueste Windows-Updates mit Sicherheitspatches

G Tipp:
Geutebrück bietet hierzu auch geeignete **Wartungs-Dienstleistungen** an. Bitte wenden Sie sich dazu an unseren **Central Support.**

Hinweis: Bitte beachten Sie, dass, wenn Sie im Supportfall (Reparaturen, Wartung) ggf. Dienstleister oder Hersteller wie Geutebrück beauftragen, diese Unternehmen gemäß Art. 28 DS-GVO als Auftragsverarbeiter gelten und vertraglich in die Pflicht genommen werden müssen.

G Tipp:
Geutebrück bietet hierzu ein Standardvertragsentwurf an. Bitte wenden Sie dazu sich an Ihren Ansprechpartner im **Vertrieb**.

5. Transparenz- und Hinweispflichten

Gemäß § 4 Abs. 2 BDSG-neu sind der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Dies hat in der Regel durch Schilder zu erfolgen, deren Inhalt von den Betroffenen wahrgenommen wird, bevor sie in den Erfassungsbereich der Kameras geraten.

5.1 Informationspflichten

Nach den Vorgaben von Art. 13 DS-GVO müssen die Schilder jedoch noch weitere Informationen enthalten, die den Betroffenen „zum Zeitpunkt der Erhebung der Daten“ mitzuteilen sind. Zur Erfüllung dieser Informationspflichten wird von den Datenschutzbehörden eine gestufte Informationserteilung empfohlen.

Dies bedeutet, dass vor dem Betreten des zu überwachenden Bereiches

- ein Hinweisschild mit den wesentlichen Informationen (sog. „vorgelagertes Hinweisschild“) vorzuhalten ist. Dieses Schild enthält u.a. ein Piktogramm des Kamerasymbols, den Namen und die Kontaktdaten des Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, den Zweck und die Rechtsgrundlage der Verarbeitung, ggf. die berechtigten Interessen sowie die Speicherdauer. Zudem gibt es einen Verweis auf weitere Informationen.

- ein ausführliches Informationsblatt an anderer, gut zugänglicher Stelle anzubringen bzw. vorzuhalten ist. Dies kann auch im Internet sein. Hier sind zusätzlich zu den o.g. Informationen die Rechte der Betroffenen auf Auskunft, Widerspruch, Löschung und Beschwerde bei der Aufsichtsbehörde dokumentiert.

Gemäß Art. 12 Abs. 7 DS-GVO müssen die Informationen in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung vermitteln.

G Tipp:
Die Landesbeauftragte für den Datenschutz Niedersachen hat **Beispiele für ein vorgelagertes Hinweisschild sowie ein vollständiges Informationsblatt** herausgegeben.
Auch der BHE bietet für BHE-Mitglieder Informationen zur **DS-GVO-konformen Hinweisbeschilderung** an.

5.2 Rechte der Betroffenen

Hinsichtlich der Rechte der Betroffenen gibt es bei der Videoüberwachung einige Besonderheiten zu beachten. Dazu die nachfolgenden Hinweise:

Recht auf Auskunft (Art. 15 DS-GVO)

> **Hinweis:** Wenn die Anfrage auf Auskunft zu vage formuliert ist, und dadurch der Aufwand zu groß wird oder die betroffene Person unmöglich identifiziert werden kann, ist der Betreiber nicht verpflichtet, Auskunft zu erteilen.
> Anderenfalls sind gemäß Art. 12 Abs. 3 DS-GVO die zu erteilenden Informationen zügig, in jedem Fall innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Da die Bilder aber i.d.R. bereits nach wenigen Tagen überschrieben werden, erledigt sich die Anfrage häufig von selbst. Sind auf den Bildern auch andere Personen zu sehen, dürfen davon keine Kopien weitergegeben werden, wenn dies die Persönlichkeits- und Freiheitsrechte dieser Personen beeinträchtigen könnte (vgl. Art. 15 Abs. 4 DS-GVO). Eine entsprechende Rückmeldung mit Erklärung des Sachverhalts ist dennoch erforderlich.

Recht auf Berichtigung (Art. 16 DS-GVO)

> **Hinweis:** Das Recht auf Berichtigung ist dahingehend eingeschränkt, dass die Videoaufzeichnungen i.d.R. technisch nicht verändert werden können oder zur Wahrung der Authentizität der Daten nicht verändert werden dürfen.

Recht auf Löschung („Recht auf Vergessenwerden“) (Art. 17 DS-GVO)

Hinweis: Das Recht auf Vergessenwerden wird i.d.R. durch das automatische Überschreiben gewährleistet, sofern keine zweckgebundene Speicherung erfolgt, zum Beispiel, wenn im Alarmfall die Bilder in einen anderen Ringspeicher gespeichert werden und somit für Auswerte- und Beweiszwecke länger zur Verfügung stehen.

Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)

Hinweis: Dieses Recht wird aufgrund der automatisierten Datenlöschung durch Überschreiben und der Zweckbindung bei einer Speicherung berücksichtigt.

Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)

Hinweis: Hier gilt zu bedenken, dass die Übertragung technisch nur eingeschränkt möglich ist. Außerdem kann eine Übertragung möglicherweise die Rechte Dritter beeinträchtigen.

Recht auf Widerspruch (Art. 21 DS-GVO)

Hinweis: Dieses Recht wird aufgrund der automatisierten Datenlöschung durch Überschreiben und der Zweckbindung der Speicherung berücksichtigt.

Recht auf Beschwerde (Art. 77 DS-GVO)

Hinweis: Beschwerden können jederzeit an den betrieblichen Datenschutzbeauftragten adressiert werden.
Zudem besteht die Möglichkeit einer Beschwerde bei der Aufsichtsbehörde für den Datenschutz.

Der Betreiber muss eine Regelung etablieren, womit gewährleistet wird, dass die Anliegen der betroffenen Personen zeitnah in verständlicher Form beantwortet werden, ungeachtet, ob es technisch oder rechtlich möglich ist, die Forderungen umzusetzen.

6. Weitere Pflichten, Sanktionen, Auftragsverarbeitung

Auf weitere datenschutzrechtliche Verantwortlichkeiten soll noch in gebotener Kürze hingewiesen werden:

6.1 Weitere datenschutzrechtliche Pflichten

Gemäß Art. 30 DS-GVO müssen alle Verarbeitungstätigkeiten von personenbezogenen Daten in einem Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden. Dies gilt in aller Regel auch für die Videoüberwachung. Zur Dokumentation gehören u.a. der Zweck der Verarbeitung, die Rechtsgrundlage, die Kategorien der betroffenen Personen, die Datenkategorien, die Empfänger, die Löschfristen und die technischen und organisatorischen Maßnahmen.

G Tipp:
Sehen Sie dazu auch das **Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO.**

Der Betreiber einer Videoüberwachungsanlage wird des Weiteren eine/n Datenschutzbeauftragte/n bestellen und diesen bei den zuständigen Landesdatenschutzbehörden anmelden müssen (Art. 37 DS-GVO). Gemäß § 38 Abs. 1 BDSG-neu ist ein solcher unabhängig von der Anzahl der Mitarbeiter zu bestellen, wenn Verarbeitungen im Unternehmen stattfinden, die einer Datenschutzfolgeabschätzung unterliegen, was bei umfangreicher und systematischer Videoüberwachung in öffentlich zugänglichen Bereichen regelmäßig der Fall ist.

Es gehört auch zur Verantwortung des Betreibers, Verantwortlichkeiten und Prozesse zur Gewährleistung eines datenschutzkonformen Betriebes zu definieren und zu dokumentieren. So muss z.B. sichergestellt sein, dass die Aufsichtsbehörden innerhalb von 72 Stunden im Falle eines Datenverlustes informiert werden, wenn die Verletzung des Schutzes dieser Daten zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

6.2 Sanktionen und Haftung

Die Verletzung der genannten datenschutzrechtlichen Pflichten kann von den zuständigen Aufsichtsbehörden (das sind die Landesdatenschutzbeauftragten) künftig mit hohen Bußgeldern belegt werden. So kann z. B. bei der Nichtdurchführung einer Datenschutz-Folgeabschätzung oder bei einem fehlenden Verfahrensverzeichnis eine Geldbuße von bis zu 10 Millionen Euro oder im Falle eines Unternehmens von bis zu 2 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden. Verstöße gegen die Grundsätze der Datenverarbeitung oder die Zulässigkeitsvoraussetzungen aus Artikel 5 und Artikel 6 DS-GVO können sogar Geldbußen von bis zu 20 Millionen Euro und im Falle eines Unternehmens von bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes auslösen.

Darüber hinaus können die Betroffenen künftig Schadensersatzansprüche gegen den Verantwortlichen geltend machen, wenn sie aufgrund eines Verstoßes gegen die DS-GVO einen materiellen oder immateriellen Schaden erlitten haben (vgl. Artikel 32 DS-GVO). Auch Verbandsklagen sind künftig möglich (vgl. Artikel 80 DS-GVO), sodass derartige Ansprüche auch gebündelt durch Interessenverbände geltend gemacht werden können.

6.3 Auftragsverarbeitung

Solche Sanktionen und Haftungsgefahren können nicht nur den Betreiber einer Videoüberwachungsmaßnahme als originär Verantwortlichen treffen, sondern auch alle Dienstleister, die den Betreiber dabei unterstützen und in diesem Zusammenhang an der Verarbeitung der durch die Überwachung erhobenen Bilddaten mitwirken (sog. Auftragsverarbeiter i.S.v. Art. 28 DS-GVO), sofern sie die in diesem Zusammenhang entstehenden datenschutzrechtlichen Pflichten verletzen. Das betrifft in erster Linie Leitstellen, auf die Überwachungsbilder aufgeschaltet werden.

Aber auch die regelmäßige Wartung und Parametrierung einer Videoanlage ist nach Auffassung der Datenschutzbehörden Auftragsverarbeitung, wenn der Dienstleister dabei die Notwendigkeit oder die bloße Möglichkeit des Zugriffs auf personenbezogene Bilddaten hat.

G Tipp:
Weitere Voraussetzungen der Auftragsverarbeitung lassen sich dem **Kurzpapier Nr. 13 der DSK entnehmen.**

In solchen Fällen hat der Verantwortliche den Auftragsverarbeiter vertraglich zu verpflichten, bei der Verarbeitung der personenbezogenen Daten die gleiche datenschutzrechtliche Sorgfalt anzuwenden, die dem Verantwortlichen selbst obliegt. Einzelheiten hierzu sind in Art. 28 DS-GVO geregelt, der den Parteien eines solchen Vertragsverhältnisses umfangreiche Auflagen macht. Bei laufenden Wartungsverträgen werden die Parteien künftig wohl auch einen gesonderten Vertrag über Auftragsverarbeitung schließen müssen. Ob dies auch für den Fall der einmaligen Planung, Errichtung und Inbetriebnahme einer Überwachungsanlage gilt, die vom Errichter nicht weiter betreut wird, ist im jeweiligen Einzelfall zu prüfen.

7. Dokumente und Quellen

Geutebrück

- **Statement zur Geutebrück Systemsicherheit**
- **Geutebrück Hardening Guide**
- Checkliste 1: Allgemeine Anforderungen der DS-GVO bei Videoüberwachungsanlagen
- Checkliste 2: Anforderungen zur Einhaltung der Datenschutzgrundsätze nach DS-GVO
- Checkliste 3: Anforderungen hinsichtlich der Datensicherheit nach DS-GVO
- Checkliste 4: Anforderungen hinsichtlich der Cyber Security nach DS-GVO

Die Gesellschaft für Datenschutz und Datensicherheit e.V.

- **Praxishilfe DS-GVO**

Landesbeauftragte für Datenschutz

- **Beispiele für ein vorgelagertes Hinweisschild sowie ein vollständiges Informationsblatt**
- **Vorläufige Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO**

Düsseldorfer Kreis

- **Orientierungshilfe** „Videoüberwachung durch nicht öffentliche Stellen“.

Datenschutzkonferenz

- **Übersicht DS-GVO-Kurzpapiere**
- **Kurzpapier Nr. 15 – Videoüberwachung nach der Datenschutz-Grundverordnung**
- **Kurzpapier Nr. 14 - Beschäftigtendatenschutz**
- **Kurzpapier Nr. 13 – Auftragsverarbeitung**
- **Kurzpapier Nr. 5 - Datenschutz-Folgeabschätzung**
- **Kurzpapier Nr. 1 - Verfahrensverzeichnis von Verarbeitungs-tätigkeiten**

BHE

- Checkliste - **Gesprächsleitfaden zur Videoanalyse**
- **Wichtige Hinweise für Errichter – Cyber Security bei Videoanlagen**
- **DS-GVO-konforme Hinweisbeschilderung (nur für BHE-Mitglieder)**

Für den Inhalt dieses Whitepaper gibt es keine Gewähr.
Das Dokument ersetzt keine juristische Beratung.

Die Verantwortung für den Inhalt von verlinkten Dokumenten trägt der jeweilige Verfasser. Lesen Sie dazu auch den Haftungsauschluß auf der Geutebrück Webseite.

Für eine juristische Beratung empfehlen wir die Anwaltskanzlei Dieckert.	DIECKERT Recht und Steuern Gertraudenstraße 20 10178 Berlin
Bitte beachten Sie, dass diese Beratung kostenpflichtig ist.	Telefon: 030 27 87 07 Telefax: 030 27 87 06 Mail: ulrich.dieckert@dieckert.de Web: www.dieckert.de

Impressum	Geschäftsführer:
GEUTEBRÜCK GmbH	Katharina Geutebrück
Im Nassen 7-9	Christoph Hoffmann
D - 53578 Windhagen	Handelsregister: HRB 14475 Montabaur
Tel: +49 (0) 26 45 /137 - 0	UST-Ident-Nr.: DE813443473
Fax:+49 (0) 26 45 /137 - 999	info@geutebrueck.com

VIDEO SECURITY VALUE IMAGING

www.geutebrueck.com

Follow us on

GEUTEBRÜCK

Allgemeine Anforderungen der DS-GVO an Videoüberwachungsanlagen

Diese Checkliste dient zur Unterstützung des Betreibers der Videoanlage bei der Wahrnehmung der Pflichten hinsichtlich des Datenschutzes.

DS-GVO-Bezug	Thema	Erläuterung	Erfüllt
Art. 30	Verzeichnis- Beschreibung der Verarbeitungs-tätigkeiten		
Art. 37	Benennung eines Datenschutzbeauftragten		
	Meldung des Datenschutzbeauftragten an die Landesdatenschutzbehörden	Siehe auch: **bfdi**	
Art. 6	Prüfung der Rechtmäßigkeit der Videoüberwachung		
	Einbindung Betriebsrat		
Art. 5 (2)	Rechenschaftspflicht - Dokumentation		
	■ Risikoanalyse		
	■ Betriebsanforderungen		
	■ Prüfplan		
	■ Anlagenentwurf		
	■ Aufstellung der eingesetzten Kameras (Typen und Auflösung)	Siehe hierzu EN 62676-4	
	■ Ausführungsplanung		
	■ Prüfergebnisse, Kamerapläne mit Sichtbereichen		
	■ Anlagenbeschreibung (VdS-Attest)		
Art. 35	Datenschutz-Folgeabschätzung (DSFA)		
Art. 36	Einbindung Datenschutzbehörden nach DSFA		
Art. 13	Transparenz- und Hinweispflichten		
	■ Hinweisschild im Zugangsbereich		
Art. 15	■ Weitere Informationen + Rechte der Betroffenen		
Art. 33	Prozessdefinition Datenverlust	Information der Datenschutz-behörden - Information der Betroffenen	
Art. 15	Prozessdefinition Auskunftsbegehren von Betroffenen	Recht auf Auskunft, Berichtigung, Löschung	
Art. 28	Verträge zur Auftragsverarbeitung	Wachdienstleistungen	

Anforderungen zur Einhaltung der Datenschutzgrundsätze nach DS-GVO

Es handelt sich hier um eine Auswahl von Systemen, Produkten oder Funktionen, die zur Einhaltung datenschutzrechtlicher Anforderungen beitragen.
Abhängig von der Situation können unterschiedliche Elemente erforderlich sein.

DS-GVO-Bezug	Thema	Erläuterung	Erfüllt
Art. 5c)	**Datenminimierung**		
	Einsatz und Montage der Kameras		
	Ausrichtung auf nicht sensible Bereiche		
	Sichtschutzbleche	Vermeidung von Überwachungsdruck	
	Bewegliche Kameras	Vermeidung von Überwachungsdruck	
	Thermalkameras	Identifikation erschwert	
	Tourenbetrieb bei Dome Kameras		
	■ Einstellbare Touren	Vorher festgelegte nicht sensible Bildbereiche	
	■ Automatische Rückführung in Home Position		
	Schwärzen von Bildanteilen	**Privacy Masking**	
	Livemodus	Siehe hierzu EN 62676-4	
	Speicherbilder	Die Schwärzung kann ggf. rausgenommen werden	
	Exportbilder		
	In Kameraeinstellungen		
	Verpixelung von Personen oder KFZ-Kennzeichen	**Motion Privacy**	
	Livemodus		
	Speicherbilder		
	Exportbilder		
Art. 5 e)	**Speicherbegrenzung**		
	Überscheiben der Daten	Bedingt durch die Speichergröße	
	■ Normale Videobilder	Typischerweise nach 3 bis 5 Tagen	
	■ Alarme und Events (in separaten Ringspeichern)	Abhängig von Zweck der Speicherung (z.B. bei Bankautomaten)	

Anforderungen hinsichtlich der Datensicherheit nach DS-GVO

Es handelt sich hierbei um eine Auswahl von Maßnahmen, gegliedert nach §64 BDSG, die zur Datensicherheit beitragen. Je nach Situation trägt die richtige Auswahl von Datensicherheits-Maßnahmen zum gewünschten bzw. erforderlichen Sicherheits-niveau bei.

§64 BDSG	Thema	Erläuterung	Erfüllt
	Zugangskontrolle	**Physikalische Sicherheit**	
	Zugang zu Gebäuden		
	Zugang zu Servern		
	Zugang zu Terminals		
	Datenträgerkontrolle	**Exportfiles und Backupfiles**	
	Auswahl geeignet Exportmedien (Passwortgeschützt)		
	Verschlüsselung		
	Passwortgeschützt		
	Wasserzeichen in Exportfiles		
	Speicherkontrolle	**Passwortschutz**	
	Passwort nach BSI-Vorgaben		
	4-Augen-Prinzip		
	Einbindung in Domain mit Single Sign On		
	Passwortgeschützter Remotezugang		
	Passwort verschlüsselt		
	Verschlüsselter Datenaustausch zwischen den Systemkomponenten		
	Laufwerke (Bitlocker)		
	Benutzerkontrolle	**Exportfiles mit Wasserzeichen**	
	Zugriffskontrolle	**Rechte- und Rollenkonzepte**	
	Berechtigungsgruppen		
	Administratoren		

§64 BDSG	Thema	Erläuterung	Erfüllt
	Zugriffskontrolle	**Gruppenberechtigungen für..**	
	■ Maps		■
	■ Betrachtung Live-/Speicher-/Exportbilder		■
	■ Berechtigungen auf Kameraebene		■
	■ Zeitlich befristeter Zugang		■
	■ Privacy Masking		■
	■ Motion Privacy		■
	■ Videoanalysen		■
	■ Alarmmanagement		■
	Übertragungsontrolle	**Audit-Trail**	■
	Eingangskontrolle	**Protokollierung benutzerbezogener Aktivitäten**	
	■ Verbindliche Zeitangabe		■
	Transportkontrolle	**Verschlüsselte Exportfiles**	■
	Wiederherstellbarkeit	**Notfallplan**	■
	Zuverlässigkeit	**Monitoring und Fehlerbeseitigung**	
	■ Diagnosetools		■
	Datenintegrität	**Datensicherungskonzept**	■
	Auftragskontrolle	**Datenverarbeitung nach Weisung**	
	■ Vertrag zur Auftragsdatenverarbeitung		■
	■ Schulung Wachdienst		■
	Verfügbarkeitskontrolle	**Schutz vor zufälliger Zerstörung und vor Verlust**	
	■ Redundanzsysteme Multispare		■
	■ Failover		■
	■ Edge Recording		■
	■ Datensicherung		■
	■ Virenschutz		■
	Trennbarkeit	**Trennungsgebot zur Zweckbindung**	
	■ Berechtigungskonzepte		■

Anforderungen hinsichtlich der Cyber Security nach DS-GVO

Dem Schutz vor Zugriff von Unbefugten stellen sich in aktuellen Zeiten besondere Herausforderungen. Abhängig von dem erforderlichen Schutzniveau müssen ausreichend Sicherheitsvorkehrungen gegen Cyber Attacken entsprechend dem Stand der Technik getroffen werden.

DS-GVO-Bezug	Thema	Erfüllt
Art. 25	**Netzwerksicherheit**	
	Trennung von CCTV-Netzwerk und sonstige Netzwerke	
	Verwendung von VLAN	
	Sichere Verbindungen nach Außen über Gateways	
	Einschränkung auf MAC-Adressen	
	Vermeidung WLAN	
	Verwendung von Firewall	
	Remote Access über VPN	
	Antivirus Software	
	Sichere Verbindung zw. allen Systemkomponenten	
	Verschlüsselter Übertragung zw. allen Komponenten	
	Feste IP-Adressen	
	Deaktivierung SSH Access	
	Deaktivierung Multicast	
	Deaktivierung QoS	
	Änderung Default Ports	

DS-GVO-Bezug	Thema	Erfüllt
Art. 25	**Passwörter- und Anwenderverwaltung**	
	■ Änderung Default Passwort Geutebrück System-Admin	
	■ Änderung Default Passwort Windows Betriebssystem	
	■ Änderung Default Passwort alle G-Core Clients and Services	
	■ Änderung Default Passwort G-Health	
	■ Änderung Default Passwort G-SIM	
	■ Änderung Default Passwort G-Link	
	■ Änderung Default Passwort GeViSoft	
	■ Änderung Default Passwort GeViScope	
	(Passwort Verwendung gemäß BSI-Vorgaben)	
	Windows Betriebsysteme	
	■ NTP Zeit Synchronisierung	
	■ Deaktivierung von nicht genutzten Services	
	■ SQL Server Zugang ohne administrative Möglichkeiten	
	■ Wartungsverträge für die turnusmäßige Aktualisierung der Systeme	