COMPLIANCE PRIVACY

Il **GDPR** (General Data Protection Regulation) è un Regolamento dell'Unione Europea che tutela la privacy e la protezione dei dati personali dei cittadini dell'UE. È entrato in vigore il 25 maggio 2018 ed è considerato una delle normative più rigide e complete in materia di protezione dei dati. Stabilisce delle linee guida chiare su come le organizzazioni devono raccogliere, trattare, conservare e proteggere i dati personali.
L'art. 32 del GDPR in particolare, stabilisce gli obblighi per il Titolare del trattamento riguardo alla protezione dei dati personali.

Le misure da adottare devono essere in grado di garantire la **confidenzialità**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento dei dati. Devono anche essere in grado di ripristinare la disponibilità e l'accessibilità dei dati personali in tempi ragionevoli in caso di incidente fisico o tecnico.

Il Titolare del trattamento deve garantire l'attuazione di un elevato standard di misure tecniche ed organizzative adeguate a garantire un livello di sicurezza consono al rischio, tenuto conto della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità del rischio per i diritti e le libertà delle persone fisiche.
Queste misure devono essere in grado di garantire **confidenzialità**, **integrità**, **disponibilità** e **resilienza** dei sistemi e dei servizi di trattamento dei dati. Devono anche essere in grado di ripristinare la disponibilità e l'accessibilità dei dati personali in tempi ragionevoli in caso di incidente fisico o tecnico.
Il tutto deve servire a prevenire:

- Distruzione accidentale o illecita dei dati
- Perdita dei dati
- Alterazione dei dati
- Divulgazione non autorizzata
- Accesso non autorizzato

Ai sensi degli art. 24 e 25 il titolare del trattamento deve attuare una adeguata politica di protezione, rispettando il principio della **"DATA PROTECTION BY DESIGN E BY DEFAULT",** ovvero:

- Prevedere dal principio gli strumenti a tutela dei dati personali
- Pensare alla privacy sin dalla progettazione apparecchiature per ridurre al minimo i rischi connessi al trattamento
- Offrire la massima funzionalità per rispettare le esigenze degli utenti
- Garantire sicurezza durante tutto il ciclo produttivo del prodotto e del servizio
- Pensare alla privacy come impostazione di default

Per guidare al meglio le scelte degli operatori del settore sicurezza, attraverso il processo di installazione, configurazione e utilizzo di dei prodotti DVR ed NVR GAMS in conformità alla normativa, si illustrano di seguito alcune funzioni tecniche che garantiscono il rispetto di quanto suggerito, non solo dal Regolamento Europeo, ma anche dagli enti normativi italiani per il rispetto della legislazione nazionale.

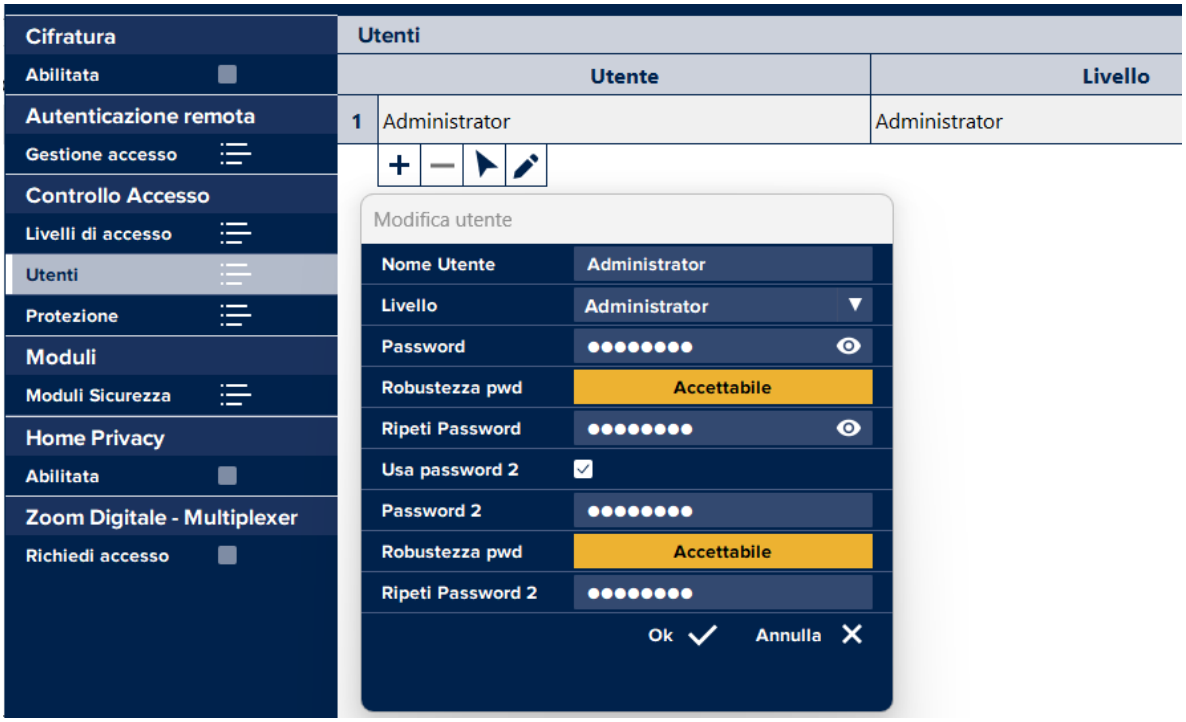
MISURE TECNICHE

- RUE (Remote USB Export)
- Privacy Home
- Privacy Mask
- Impostazione conservazione immagini Weekend-Festività
- Auto Diagnostica
- Memoria eventi (Log)
- Encripted recording
- Protezione dati salvati su HDD
- Supporto LDAP
- Accesso con Password Multilivello
- Permessi di accesso – Gruppi di appartenenza
- Pregresso (Istant replay)
- Preallarme
- Dual Stream
- Ottimizzazione della Banda
- Dual Activity Area
- Recall Preset /Tour scheduled.
- Supporto RTSP
- Supporto NTP protocol
- Rivelazione delle avarie nelle interconnessioni e dei componenti
- Configurazione per la protezione contro attacchi Brute-Force
- Rilascio di aggiornamenti Firmware per aggiornamento di cybersecurity

SICUREZZA IN ACCESSO

Utilizzare videoregistratori (configurazione, accesso locale, accesso remoto) attraverso credenziali, definendo username e password differenziati.
Ad ogni utente è possibile assegnare un diverso livello di sicurezza che ne determina i privilegi d'accesso. Per agevolare la fase di programmazione possono essere creati "Gruppi di Appartenenza".
E' opportuno definire un utente amministratore abilitato a tutte le funzioni dell'apparato, un utente con l'accesso solo al live remoto di determinate telecamere, un altro con anche l'accesso alle registrazioni o al comando delle telecamere dome, e così via.
Tutte le operazioni saranno registrate nel log eventi (accesso al menu di configurazione, accesso alle registrazioni, movimentazione delle telecamere PTZ, ecc.).

Accesso al sistema con «Doppia Password»



Metodi di Accesso (Locale / Centralizzato)

È possibile abilitare la gestione delle credenziali di accesso ai sistemi periferici (DVR/NVR), anziché localmente (sull'apparato), attraverso un server (ad esempio un server Active Directory raggiungibile tramite connessione di rete e protocollo LDAP ha il compito di gestire le credenziali di autenticazione (username/password) per l'accesso all'apparato (in locale e da remoto).

Memoria eventi (controllo accessi ed altro)

Estrarre un file "Log_Eventi" dettagliato impostato sino ad almeno 180 giorni di memoria; viene riportato "COSA" è stato effettuato, da "CHI" e "QUANDO". Il menu "Log Eventi" consente di visionare tutte le operazioni eseguite sull'apparato (da un utente in locale e/o da remoto, dal sistema in modo automatico, da altri fattori esterni come l'attivazione di un ingresso digitale, la perdita di un segnale video, un movimento individuato dall'Activity Detector, etc.), elencate in ordine cronologico.

Limitazione del numero di giorni in archivio e cancellazione automatica

Una volta terminato il tempo attivo di archiviazione preimpostato, le registrazioni saranno automaticamente cancellate e non potranno essere più riprodotte.

Cyber security

Gli apparati GAMS utilizzano i più efficienti protocolli di sicurezza a livello informatico per elevare al massimo la possibilità di opporsi a tentativi di attacco. È utilizzato il sistema operativo Linux (embedded per macchine con HW dedicato), kernel con i soli pacchetti FW richiesti per il funzionamento dell'apparato per ridurre rischi di vulnerabilità specifici, configurabilità dei servizi di rete, nessun servizio telnet (accesso solo tramite protocollo ssh con chiave asimmetrica).
Sistematicamente i prodotti vengono sottoposti a metodici «Penetration Test» per stabilirne e certificarne il grado di robustezza e resistenza ad attacchi «Cyber».
Per la protezione dell'apparato da attacchi Brute-Force è possibile configurare la seguente schermata:

Crittografia delle trasmissioni

Tra le prescrizioni definite dalle diverse normative, si ha la cifratura dei flussi video trasmessi via LAN, definiti in tutte le diverse tipologie di connessione:

- Live
- Play
- Esportazione da remoto

Questa funzione deve essere attivata dall'Amministratore del sistema.
In questo modo i dati **trasmessi, esportati** e **scritti** su Hard_Disk vengono cifrati (chiave simmetrica 128bit). L'accesso in SSH è protetto da una autenticazione a chiave asimmetrica.

Esportazione protetta

In fase di esportazione di uno o più filmati deve essere possibile proteggere i dati con una password di lettura; chi non sarà in possesso di questo dato non potrà riprodurre il filmato stesso. I file esportati saranno cifrati e visibili solo con il **Player dedicato.**
È possibile esportare i filmati sia da locale all'apparato su un supporto di memoria USB, sia da remoto attraverso un SW di centralizzazione.

Protezione dei dati salvati su HDD

Tutti i file registrati sono cifrati.
A tutti i file registrati viene assegnato un codice dipendente dal videoregistratore (codice apparato) in modo da:

1. Impedirne la visualizzazione su un altro videoregistratore (copia del file sull'HDD di un altro DVR\NVR o spostamento dell'HDD)
2. Impedirne la visualizzazione a seguito di copia su PC

Home Privacy

La funzione Privacy Home consente di disabilitare su evento o fascia oraria uno o più ingressi video. Interfacciando un ingresso di allarme del DVR/NVR opportunamente programmato, con un comando esterno è possibile disinibire l'utilizzo delle telecamere programmate come *Home Privacy*. Tale funzione trova applicazione in tutti quei casi dove occorra manualmente o in particolari fasce orarie disattivare la ripresa degli ambienti "vietati" senza dover intervenire direttamente sulle telecamere da inibire.

Sistema di monitoraggio diagnostico

Attraverso una funzione di diagnostica è possibile ricevere eventi in tempo reale su smartphone e tablet tramite notifiche Push. Ricezione di eventi di carattere tecnico manutentivo in tempo reale da tutti i periferici. Servizio basato su notifica push.