GDPR Compliance på AXIOM V

GDPR er en anderledes størrelse i Adgangskontrol (AXIOM V) sammenhæng, da de to er modstridende i deres ophav.

Adgangskontrol (AXIOM V) er skabt til at logge al aktivitet for at beskytte virksomheden mod Tyveri, adgang for uvedkommende i udvalgte områder, Terror sikring og den slags, ved at gemme aktivitet pr. bruger/person.

GDPR er skabt til at beskytte private data, og sikre at disse er ejet af personen selv.

Altså vil et Adgangskontrol anlæg pr. teknisk definition ikke give mulighed for at udnytte "retten til at blive glemt" som ellers er en del af GDPR.

Det er pr. design ikke muligt at slette en eller flere enkeltstående hændelse(r) i systemet.

Vi anbefaler at der benyttes et minimum af personfølsomme eller personhenførbare data i systemet. Vores anbefaling er maksimalt at benytte, Fornavn, Efternavn og initialer.

Anbefalinger og egenskaber

For at imødekomme kravene vedr. GDPR har vi følgende informationer og anbefalinger til brug for implementering af GDPR Compliance i sammenhæng med AXIOM V:

1. AXIOM V gemme ingen personhenførbar- eller personfølsom data på UNC, NURC, RC2 og øvrige Controllere. Disse Hardware enheder indeholder udelukkende kortnumre, samt information om dørene.

2. AXIOM V gemmer alle informationer i en SQL-Database. Det er muligt at opsætte en tidsbegrænsning for opbevaring af historisk data, således at personhenførbare data kun opbevares i den tid som er angivet i virksomhedens GDPR-politik. Tiden for opbevaring angives i antal dage, og understøtter fra 1 – 9999 dage.

3. Persondata der indgår i brugerlogs, er afhængig af hvordan man stykker sine brugernavne sammen i AXIOM V. Normalt vil det være <Fornavn Efternavn> og et kortnummer der indgår, altså ingen telefonnumre, personnumre eller andre følsomme data.

Et eksempel kan også være at der benyttes AD som integration. I så fald vil et brugernavn blive stykket sammen af ”Fornavn Efternavn (Initialer)”

Eksempel på hvordan en logentry ser ud:

	RecordID	EventID	PCDate	NC100D...	ID1	ID2	PanelID	NetworkID	ID1Name	ID2name	ID3	ID3Na...	ID4
49	2571	65536	2018-11-13 14:36:31.800	595434990	1	292215	257	256	UNCRC2 1-1-1\Reader 1	AWID BRIK	0		0
50	2576	65536	2018-11-13 14:36:42.710	595435001	1	292215	257	256	UNCRC2 1-1-1\Reader 1	AWID BRIK	0		0
51	2579	65536	2018-11-13 14:36:46.203	595435004	1	292215	257	256	UNCRC2 1-1-1\Reader 1	AWID BRIK	0		0
52	2581	65536	2018-11-13 14:36:47.077	595435005	1	292215	257	256	UNCRC2 1-1-1\Reader 1	AWID BRIK	0		0
53	2583	65536	2018-11-13 14:36:48.383	595435007	1	292215	257	256	UNCRC2 1-1-1\Reader 1	AWID BRIK	0		0
54	2587	65536	2018-11-13 14:36:53.183	595435012	1	292215	257	256	UNCRC2 1-1-1\Reader 1	AWID BRIK	0		0

ID2name er feltet som indeholder ”Fornavn Efternavn”

4. Alle operatørlogins gemmes i en log på lige fod med adgang til døre. Operatør logning indeholder, Hvem loggede ind, og ændringer foretaget på systemet (Døråbning, skemaændringer, o. lign.) samt evt. ændringer af brugere.

5. AXIOM V gemmer alle informationer i en SQL-Database, det er ikke muligt at anonymisere enkelt loghændelser gennem AXIOM V egen software, men i yderste nødstilfælde vil det være muligt at konstruere en SQL-forespørgsel som kan udsøge en specifik person, anonymisere denne, og således kunne opfylde et evt. ønske om at blive "glemt".

Det skal understreges at det IKKE er designmæssigt muligt at ændre denne egenskab i software, og det svarer til at kompromittere databasen at udføre ikke tilsigtede ændringer af data direkte i databasen, en evt. anonymisering af data vil derfor foregå på kundens eget ansvar. Det vil være muligt at få hjælp fra ARAS Security A/S til at konstruere en anonymiserings SQL-forespørgsel, samt få hjælp til at udføre en evt. anonymisering af personer i AXIOM V.

Generelt om GDPR ved brug af AXIOM V

Anbefalingen for at leve op til GDPR vil være at man oplyser de dele af ovenstående som er relevante for jer i et tillæg til ansættelseskontrakten, og henviser til at det er hensynet til beskyttelse af virksomhedens aktiver, beskyttelse mod sabotage, industrispionage og beskyttelse af virksomhedens personale der danner grundlag og vægtes for denne datahåndterings metode. Graden af alvorlighed og vægtning af loghistorik, må bero på en sikkerhedsvurdering fra virksomheden selv.

GDPR er en levende proces, og vi ser på forskellige muligheder for at hjælpe installatørerne og kunderne til at opnå en enklere håndtering af deres Adgangskontrolsystemer når det kommer til persondataforordningen. Det skal dog altid sammenholdes med at AXIOM V er et Sikkerhedssystem i sin oprindelse, og det vil altid være sikkerheden i systemet der kommer i første række.

Det vil være muligt at indgå en databehandler aftale med ARAS Security A/S direkte hvis det bliver nødvendigt, men under normale omstændigheder vil det være Kunde og Installatør, som indgår denne aftale.

ARAS Security A/S tilbyder at indgå en databehandler aftale med alle installatører der forhandler vores produkter, og vi indgår eventuelle databehandler aftaler med producenter af hardware og software i det omfang det er påkrævet.

ARAS Security A/S overfører ikke personhenførbar- eller personfølsomme data til 3. lande (Lande udenfor EU/EØS), dog undtaget registrerede sikre 3. lande, uden forudgående skriftlig tilladelse fra kunden.

Spørgsmål vedr. GDPR til ARAS Security A/S foretages på gdpr@aras.dk eller telefon +45 70 27 40 90.