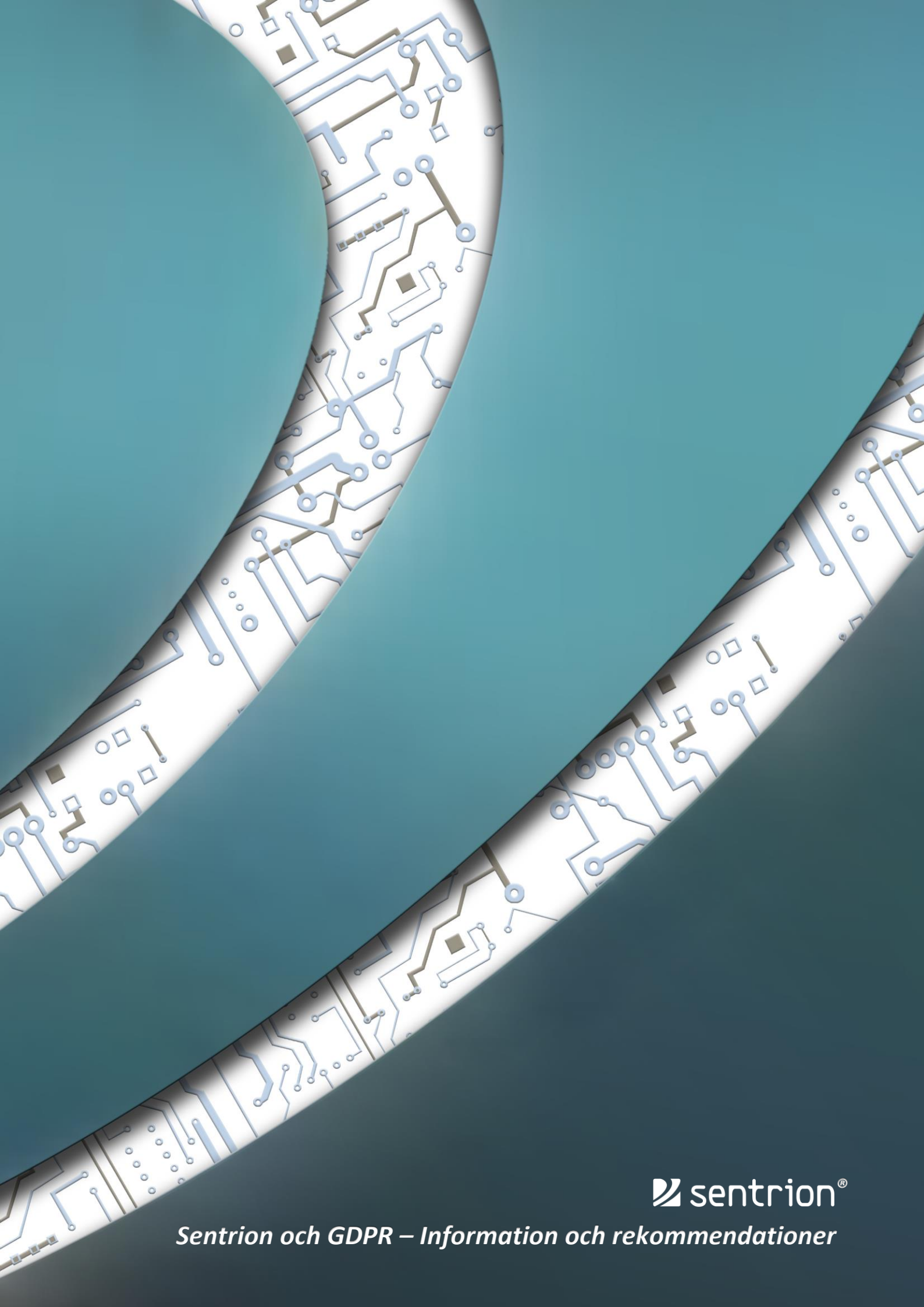

sentrion®

Sentrion och GDPR – Information och rekommendationer

Innehållsförteckning

GDPR

Detta dokument beskriver hur Sentrion kan användas för att uppfylla de krav som GDPR ställer på hantering av personuppgifter.

Dokumentet beskriver främst användning av Sentrion som ett fristående s.k. stand-alone-system. Om Sentrion integrerats med det överliggande systemet Pacom Unison, ansvarar detta system för att GDPR kan efterlevas. Se dokumentation för Pacom Unison för mer information.

Upplägget i dokumentet är som följer:

- Presentation av grundläggande principer för GDPR och vilka rättigheter de registrerade har enligt GDPR vilka vi bedömer är relevanta för Sentrion samt hur Sentrion uppfyller dessa.
- Rekommendationer om best practice för att GDPR-anpassa en Sentrion-installation.

Observera att detta dokument endast är rådgivande. Kunden ansvarar själv för att anläggningen och hantering av personuppgifter sker i enlighet med GDPR.

Principer

GDPR:s grundläggande principer för behandling av personuppgifter är som följer:

- Laglighet, korrekthet och öppenhet – All behandling av personuppgifter måste ha laglig grund och det måste vara tydligt för de registrerade vad som sker med deras personuppgifter.
- Ändamålsbegränsning – Behandling av personuppgifter får enbart vara av överenskommen typ. Personuppgifter får inte användas i andra syften utan överenskommelse med den registrerade.
- Uppgiftsminimering – Enbart nödvändiga personuppgifter skall ingå i behandlingar.
- Korrekthet – De personuppgifter som behandlas skall vara korrekta. Felaktiga personuppgifter skall rättas eller raderas.
- Lagringsminimering – Personuppgifter skall inte sparas längre än vad den lagliga grunden tillåter. Därefter skall personuppgifterna raderas.
- Integritet och konfidentialitet – Personuppgifter skall skyddas så de inte otillbörligen sprids, ändras eller raderas.

Registrerades rättigheter

GDPR definierar ett antal rättigheter som tillfaller de registrerade. De vi anser är relevanta för Sentrion är följande:

- Rätt till information (1) – I samband med insamling av personuppgifter har den registrerade rätt att få information om vilka uppgifter det gäller, hur de kommer att behandlas, vilken laglig grund som finns för behandlingen, mm.
- Rätt till information (2) – En registrerad person har rätt att begära ut registerutdrag om sina egna personuppgifter samt hur de behandlas.
- Rätt till rättelse – En registrerad person har rätt att begära rättning av personuppgifter som uppfattas som felaktiga.
- Rätt till radering – En registrerad person har rätt att få sina personuppgifter raderade under förutsättning att andra tyngre vägande lagliga skäl inte finns för organisationen att behålla dem.

- Rätt till begränsning av behandling – En registrerad person kan begära att deras personuppgifter ”fryses” och inte längre får behandlas. Detta gäller tex om den registrerade personen anser att personuppgifterna utsatts för olaglig behandling och att de måste bevaras som bevis.
- Rätt till dataportabilitet – Den registrerade har under vissa omständigheter rätt att begära ut sina personuppgifter i ett format som tillåter överföring till ett annat system eller tjänst.

Sentrion och GDPR

Sentrion kan normalt vara uppsatt i ett av två distinkta lägen:

Stand-alone: I det här läget sker inmatning, ändring och radering av personuppgifter direkt via Sentrions inbyggda webbgränssnitt. Vilka persondatafält som finns tillgängliga bestäms vid installation av Sentrion.

Kontrollerad av överliggande system: I det här läget sker inmatning, ändring och radering av personuppgifter i ett överliggande system som i sin tur hanterar vilka personer som skickas ut till Sentrion. Enbart presentationstexten för personen (vanligtvis ID + personnamn) skickas till Sentrion från det överliggande systemet. Se det överliggande systemets dokumentation för mer information om GDPR-anpassning.

Laglighet, korrekthet och öppenhet

De behandlingar av personuppgifter som utförs i Sentrion måste täckas av laglig grund. Vanligtvis utgörs detta av avtal (tex anställningsavtal, kontrakt) eller liknande.

Hantering av detta sker utanför produkten Sentrion.

Ändamålsbegränsning

Personuppgifter som finns registrerade i Sentrion får inte användas för andra behandlingar än de som har laglig grund enligt ovan. Vid inmatning av ny person i Sentrion är det därför lämpligt att verifiera att behandlingen täcks av existerande laglig grund och om detta inte är tydligt kan det finnas skäl att se över anställningsavtal mm.

Detta hanteras utanför produkten Sentrion.

Uppgiftsminimering

Sentrion hanterar enbart personuppgifter som överenskommits med kund kompletterat med vissa tekniska data som krävs för att systemet skall fungera. Vilka typer av personuppgifter det rör sig om går att utläsa av inställningarna i Sentrions webbgränssnitt. Finns ytterligare frågor (eller om exempel på faktiskt innehåll önskas) tillhandahåller Sentrions webbgränssnitt även en rapport som hämtar ut alla personuppgifter om en vald person.

Korrekthet

De personuppgifter som behandlas i Sentrion skall vara korrekta. Operatörer med tillräcklig behörighet kan redigera existerande personuppgifter i Sentrions webbgränssnitt.

Lagringsminimering

Personuppgifter får inte lagras längre än vad medges enligt den lagliga grunden. Operatörer med tillräcklig behörighet kan radera personuppgifter i Sentrions webbgränssnitt.

En annan viktig komponent i lagringsminimering är hanteringen av loggar. Loggdata betraktas som ”livedata” i Sentrion och är åtkomlig för operatörer. Hur länge loggposter sparas är konfigurerbart och ett tidsintervall som passar kunden måste anges i systemet.

Säkerhetskopiering av Sentrions databas sker via Sentrion Manager eller direkt i Sentrions webbgränssnitt av operatörer med tillräcklig behörighet. Säkerhetskopiorna bör alltid krypteras med lösenord.

Rekommendationen är att organisationen har strikta processer för hantering av säkerhetskopior av Sentrions databas. Säkerhetskopior bör tas regelbundet och måste sparas säkert. Säkerhetskopior får dock inte sparas längre än vad organisationen har rätt till enligt den lagliga grund som gäller för behandlingen av personuppgifterna. Det kan vara relevant för organisationen att utreda om berättigat intresse behöver användas för att motivera lagringstider utöver tex avtalslängd, väga dessa intressen mot de registrerades integritetskrav och dokumentera detta.

Integritet och konfidentialitet

I Sentrion sker alltid åtkomstkontroll innan en användare kan få tillgång till personuppgifter. Rekommenderat är att operatörskonton som sätts upp i Sentrion följer organisationens policy för lösenordshantering. Vilka personuppgifter en operatör kan se beror på operatörens behörigheter i Sentrion.

Sentrion bör vara installerat på ett skyddat nätverk så kommunikation med enheten skyddas.

Sentrions webbgränssnitt tillåter enbart https-anslutningar från webbläsare.

Säkerhetskopior av Sentrions databas kan sparas ner i lösenordskyddad krypterad form.

Rätt till information (1)

Den information som skall meddelas registrerade i samband med registrering hanteras normalt sett av HR eller motsvarande. Se *Laglighet, korrekthet och öppenhet* ovan för mer information.

Rätt till information (2)

Då en registrerad person begär ut information om sina personuppgifter från personuppgiftsansvarige kan den registerutdragsfunktion som finns inbyggd i Sentrion användas för att ta ut ett registerutdrag. Detta utdrag innehåller persondata (användarfält i Sentrion), en förteckning över tilldelade behörigheter samt ett utdrag ur loggen innehållande poster som berör användaren. Registerutdraget sparas i läsbart format.

Rätt till rättelse

Om en registrerad person begär och beviljas rättelse kan rättelsen ske genom att operatör med tillräcklig behörighet redigerar berörda personuppgifter i Sentrions webbgränssnitt. Kontrolleras Sentrion av ett överliggande system sker rättelsen där.

Rätt till radering (rätten att bli glömd)

Om en registrerad person begär och beviljas radering kan raderingen ske genom att operatör med tillräcklig behörighet raderar personen i Sentrions webbgränssnitt. Kontrolleras Sentrion av ett överliggande system sker raderingen där.

Rätt till begränsning av behandling

Om en registrerad person begär och beviljas begränsning av behandling och detta påverkar de personuppgifter som behandlas av Sentrion bör detta hanteras på följande sätt. Ett registerutdrag för personen tas ut med hjälp av den registerutdragsfunktion som finns inbyggd i Sentrion (se *Rätt till information (2)* ovan). En säkerhetskopia av Sentrions databas skapas av behörig operatör för att säkerställa att en exakt bild av nuläget bevaras och därefter raderas personen i Sentrion. Raderingen sker för att säkerställa att berörda personuppgifter inte behandlas ytterligare i Sentrion. Notera att om Sentrion kontrolleras av ett överliggande system måste det systemet säkerställa att personen inte skickas ut till Sentrion igen.

Rätt till dataportabilitet

Om en registrerad person begär och beviljas dataportabilitet hanteras det enligt följande. Ett registerutdrag för personen tas ut med hjälp av den registerutdragsfunktion som finns inbyggd i Sentrion (se *Rätt till information (2)* ovan). Registerutdraget sparas i maskinläsbart format och kan lämnas ut till den registrerade. Om personens begäran om dataportabilitet även innebär en flytt från Sentrion till ett annat system bör personen även raderas (se *Rätt till radering* ovan)

Best practice för säkerhet i Sentrion

I denna sektion presenteras en rad olika åtgärder och rekommendationer som kan användas som en checklista för att utvärdera och säkerställa att organisationens Sentrion-installation uppfyller GDPR från ett åtkomst- och säkerhetsperspektiv. Notera att GDPR inte pekar på några specifika säkerhetslösningar, lagstiftningen är avsedd att vara helt teknikneutral, utan hänvisar till branschstandarder, best practice och liknande. Att säkra ett system är därför att betrakta som ett löpande arbete och nya säkerhetslösningar bör utredas och värderas när de blir tillgängliga.

Kommunikation

Sentrion bör vara installerat på ett skyddat nätverk för att säkra all kommunikation med enheten. Sentrion har även inbyggt stöd för krypterad kommunikation med överliggande system och mellan centraler (vid global funktion, tex global MAP). Krypteringen använder TLSv1, TLSv1.1 eller TLSv1.2 (TLSv1 är på väg ut och kommer så småningom tas bort). Används Pacom Unison som överliggande system, paras Sentrion ihop med Unison första gången man anger *Krypterad med autentisering* som protokoll. Unika certifikat (X509) skapas på båda sidor och de publika delarna överförs mellan systemen. Det är viktigt att denna parning sker under kontrollerade former på ett säkert nät (en motståndare med möjlighet att påverka kommunikationen mellan systemen kan i teorin kapa de nyskapade certifikaten och ersätta dem med sina egna). Efter parningen är kommunikationen säkrad med kryptering (TLS) och båda sidornas identitet kontrolleras alltid mot certifikaten.

Från och med Sentrion Manager version 3.3.0 i kombination med Sentrion firmware version 4.5.0 eller nyare, har Sentrion Manager stöd för att ange lösenord för anslutningen till Sentrion. Sedan tidigare har det varit möjligt att använda en nyckelfil men nu stöds även lösenord för att underlätta

säkrandet av kommunikationen mellan produkterna. Sentrion Manager 3.3.0 eller nyare uppmanar dessutom användaren att sätta ett lösenord om inget redan är angivet.

Loggningsinställningar

Kräver Sentrion FW version 4.5.0 eller högre samt Pacom Unison version 5.9.0 eller högre.

Nedanstående två inställningar behöver anges med för organisationen relevanta värden. Inställningen kan göras antingen i Sentrions webbgränssnitt eller i Pacom Unison om det används som överordnat system.

- *Behåll passerlogg (mån) / Keep access log (months)*: Antal månader att hålla kvar loggposter
- *Passerloggposter före radering / Access log entries before deletion*: Minsta antal loggposter att hålla kvar oavsett ovanstående inställning

Anges till exempel *Behåll passerlogg (mån)* till 3 och *Passerloggposter före radering* till 0 så raderas automatiskt alla loggposter direkt när de blir äldre än 3 månader.

Säkerhetskopior

Från och med Sentrion FW v4.5.0 och Sentrion Manager v3.3.0 kan säkerhetskopior krypteras med lösenord. Möjligheten att lagra säkerhetskopior lokalt i Sentrion har även tagits bort för att minimera risken att bryta mot krav på lagringsminimering.

Registerutdrag

Kräver minst Sentrion FW version 4.5.0

I Sentrions webbgränssnitt är det nu möjligt att plocka ut en rapport som sammanställer vald användares data i systemet. Rapporten inkluderar även relevanta loggposter m.m. Rapporten kan sparas ner antingen som XML eller som ett Excel-dokument.

Säkerhetschecklista

- ☐ Använd krypterad anslutning med certifikat om överordnat system eller globala funktioner används
- ☐ Stäng av möjlighet till extern anslutning om överordnat system eller globala funktioner inte används
- ☐ Byt alltid ut standardlösenordet för administratörskontot (admin) i webbgränssnittet om detta används
- ☐ Verifiera att såväl administratörskonto som operatörskonton följer organisationens lösenordspolicy
- ☐ Åtkomst till webbgränssnittet från internet bör inte tillåtas annat än via VPN eller motsvarande.
- ☐ Stäng av webbgränssnittet om detta inte används
- ☐ Sätt alltid ett lösenord för inloggning med Sentrion Manager
- ☐ Använd alltid lösenord för att kryptera backuper