POINTSHARP

Personuppgiftsansvariges instruktion för behandling av personuppgifter

Pointsharp Secure Cloud Net iD SweID

Classification:	Public
Publication No.:	PSC-Lg22-13
Document version:	1.0
Document status:	Final
Date:	07 Jun 2022

Table of Contents

Personuppgiftsansvarigs instruktion till Personuppgiftsbiträdet (Pointsharp) för behandling av personuppgifter inom Pointsharp Secure Cloud Net iD SweID.

Personuppgiftsansvarig
Personuppgiftsansvarig enligt definitionen i Personuppgiftsbiträdesavtalet.

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående instruktion:

1 Ändamål, föremålet och arten

Enligt avtal med den personuppgiftsansvarige tillhandahåller Pointsharp tjänsten Pointsharp Secure Cloud Net iD SweID (Tjänsten). I det uppdraget agerar Pointsharp som personuppgiftsbiträde och behandlar personuppgifter för:

- Utsedd personal hos Personuppgiftsansvarig med roller i förvaltningen av RA-domänen.
- Användarna hos Personuppgiftsansvarig, det vill säga innehavarna av e-identiteterna, som hanteras i system relaterade till Tjänsten.

Ansvaret som Personuppgiftsbiträde gäller alla personuppgifter som Pointsharp kan ha tillgång till under drift, backup och andra underhållsaktiviteter, oavsett om personuppgifterna finns tillgängliga i okrypterad eller krypterad form.

Personuppgifter som rör Personuppgiftsansvarigs personal och användare kommer i huvudsak att lagras i krypterad form i databaser och i säkerhetskopior av dessa (i vila) samt i krypterade kanaler under transport, men kan finnas tillgängliga i okrypterad form i samband med felsökning eller annat underhåll initierat av Personuppgiftsansvarig.

2 Behandlingen omfattar följande typer av Personuppgifter

Användare och personal inom Personuppgiftsansvarigs RA-domän som hanteras som en del av Tjänsten.

Informationen är normalt krypterad och kan innehålla följande personuppgifter:

- namn,
- unik identifierare, till exempel personnummer,
- e-postadress,
- UPN,
- telefonnummer,
- serienummer på nyckelbäraren,
- organisationstillhörighet,
- organistionsnummer,
- momsregistreringsnummer eller EUID,
- Microsoft SID (Microsoft security identifier),
- RA-roll,
- foto,
- signatur,

- elektronisk signatur,
- kontorsadress,
- titel,
- certifikat med innehåll,
- offentlig nyckel,
- MIFARE-nummer,
- IMEI-nummer, och
- andra personuppgifter som lagts till av den personuppgiftsansvarige.

3 Behandlingen omfattar kategorier av Registrerade

Behandlingen av personuppgifter inkluderar följande kategorier av registrerade:

- Användare hos Personuppgiftsansvarig: anställda, konsulter eller andra personer associerade med Personuppgiftsansvarig som använder Tjänsten.
- Personal med RA-roller hos Personuppgiftsansvarig: anställda, konsulter eller annan personal som har Personuppgiftsansvarigs uppdrag att hantera sina åtaganden inom Tjänsten.

4 Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

Tjänsten ska förse applikationer med tillhörande systemkomponenter och databaser där personuppgifter behandlas och lagras. Personuppgifter i vila kommer att bestå av personuppgifter och loggar som måste krypteras. Systemadministratörer på Pointsharp och dess underleverantörer ska endast ha tillgång till personuppgifter i krypterad form.

Administratörer på Pointsharp kommer att ha tillgång till att hantera personuppgifter i Tjänsten. Sådan behandling av personuppgifter ska endast utföras på begäran av en behörig representant för den personuppgiftsansvarige. Personuppgiftsansvarig ska kunna granska loggar över all utförd behandling.

I händelse av att spårningsloggning är aktiverat för felsökning, kommer personuppgifter tillfälligt att hittas i loggfiler som används under felsökning. Loggfiler måste raderas omedelbart efter att felsökningen har utförts.

En bakgrundskontroll ska göras för all personal innan de tillsätts en roll som ger tillgång till personuppgifter om Personuppgiftsansvarig. Utsedd personal ska ha visat sig vara lämplig att inneha rollen och ska ha genomgått utbildning i hantering av personuppgifter i enlighet med GDPR och denna DPA.

Skydd av personuppgifter under överföring bör inte bara förlita sig på TLS, utan bör använda en extra krypteringsmetod.

4.1 Säkerhetskopior

Säkerhetskopior som innehåller personuppgifter ska skyddas till minst samma nivå som systemet eller applikationen där personuppgifterna normalt används eller lagras.

Kompletta säkerhetskopior av systemen ska sparas i högst två år innan de roteras på ett sådant sätt att säkerhetskopior äldre än två år förstörs.

5 Ange särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

5.1 Personuppgifter och känsliga uppgifter i applikationsdatabaser

Alla känsliga uppgifter i applikationsdatabaserna (inklusive personuppgifter) måste lagras krypterade.

Tillgång till hårdvara och kryptonycklar ska hanteras via en process där minst två (2) personer i kombination krävs för att hantera de nycklar som används för skydd av personuppgifter och känsliga uppgifter i databaser.

5.2 Personuppgifter och känsliga uppgifter under transport

All kommunikation mellan system och applikationer ska skyddas med teknik baserad på asymmetrisk och symmetrisk kryptering.

5.3 Automatisk registrering av personuppgifter

Personuppgiftsbiträde ska genomföra en automatisk hämtning och registrering av Microsoft SID som är läsbart från AD:t. Detta för att möjliggöra domäninloggning med e-legitimationen.

6 Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem

Loggar måste sparas i minst tio (10) år innan de rensas (ändring från Personuppgiftsbiträdesavtal, avsnitt 7.5).

I loggar ska det framgå vilka personer som har och har haft tillgång till personuppgifter och vid ändring av personuppgifter ska det framgå vad som har ändrats.

Exempel på loggar som Pointsharps personal kommer att hantera som innehåller personuppgifter:

- Behörigheter för åtkomst till personuppgifter och ändringar i behörigheterna.
- Logisk åtkomst till Tjänsten.
- Alla ändringar av personuppgifter i Tjänsten.
- Felsökningsloggar för applikationer.

Endast personal hos Personuppgiftsansvarig som har utsetts till en roll som ger tillgång till personuppgifter ska ha tillgång till loggarna.

6.1 Spårningsloggning (trace logging)

I samband med felsökning kan det finnas behov av att slå på spårningsloggning för de olika applikationerna för att få information som är mer detaljerad och för att underlätta felsökning. Dessa spårningsloggar innehåller personuppgifter och måste därför hanteras med största försiktighet.

Så snart spårningsloggar har analyserats måste de omgående raderas i systemen och på alla andra tillfälliga lagringsplatser eller lagringsmedia som används för analysen.

7 Lokalisering och överföring av Personuppgifter till Tredje land

Personuppgifter får inte överföras till eller behandlas i tredje land.

8 Övriga Instruktioner angående Behandling av Personuppgifter som utförs av biträdet/ biträdena

8.1 Avvikelser och kompletteringar av skrivningar i Personuppgiftsbiträdesavtalets huvuddokument

Stycke 7.5:

Rensning av loggfiler får ske först efter tio (10) år istället för de angivna fem (5) åren.

Stycke 16.1:

För Personuppgiftsbiträdesavtalet gäller samma uppsägningstid som för huvudavtalet mellan parterna, se Kundavtalsvillkor avsnitt 18.1.

POINTSHARP

Website
https://www.pointsharp.com

Classification:	Public
Publ. No.:	PSC-Lg22-13
Document version:	1.0
Document status:	Final
OID:	
Published:	07 Jun 2022