Vårt samarbeid med ny underleverandør SD Worx Mauritius Limited

Juni 2026

Innholdsfortegnelse

1. Påvirkning og fordeler

1.1 Hvilke tjenester vil bli levert av SD Worx Mauritius i vårt nordiske tilbud?

SD Worx-konsernet har besluttet å involvere SD Worx Mauritius i utvalgte tekniske, operative og infrastrukturrelaterte aktiviteter som støtter vårt nordiske tilbud.
Innledningsvis vil dette hovedsakelig omfatte global teknisk støtte og backoffice-aktiviteter for SD Worx-plattformer og felles tjenester.

I praksis kan dette inkludere:

- håndtering av hendelser,
- overvåking,
- teknisk feilsøking,
- integrasjoner,
- datautveksling,
- støtte til konfigurasjon,
- teknisk veiledning i bruk av plattformene og feilsøking,
- støtte knyttet til identitet og tilgang,
- dokumentasjon, testing, utrulling og støtte ved lansering av versjoner.

For løsninger som deles mellom ulike SD Worx-markeder (for eksempel SD Worx HR, SD Connect, mysdworx, Master Data Management, integrasjonsplattformer og fremtidige smartautomatiserings- eller KI-støttede verktøy), kan kolleger i Mauritius også bidra med:

- produktutvikling,
- teknisk støtte på andre- og tredjelinjenivå,
- IT-drift,
- systemutvikling og -teknikk,
- sikkerhetsrelaterte aktiviteter,
- arbeidsverktøy og tjenester for SD Worx-ansatte,
- virksomhetsstøttesystemer (enterprise tooling).

Omfanget er ikke uttømmende og kan utvikle seg over tid i takt med videreutvikling av SD Worx-plattformer og konsernfelles tekniske tjenester.

1.2 Hva er bakgrunn for SD Worx Group sin beslutning?

Siden 2016 har SD Worx gjort strategiske investeringer i talent-huber i Mauritius og Spania. Disse hubene huser mange dyktige medarbeidere som spiller en viktig rolle i å støtte våre operasjoner. SD Worx har som mål å utnytte disse verdifulle ressursene for de nordiske tjenestene fra og med 2026. SD Worx Mauritius vurderes som best egnet til å levere de nødvendige tjenestene.

.

1.3 Hva er fordelene?

Et samarbeid med SD Worx Mauritius gjør det mulig for SD Worx å øke skalaen, benytte den beste tilgjengelige kompetansen internasjonalt og oppnå kostnadseffektiviseringer i et svært konkurransepreget marked og under krevende makroøkonomiske rammebetingelser.

1.4 Hvordan vil dette påvirke meg som kunde og mine ansatte?

i forventer ingen påvirkning på din daglige bruk av SD Worx' tjenester og applikasjoner.
Vi er forpliktet til å sikre kontinuitet og levere tjenester av samme høye kvalitet.

1.5 Vil tidsforskjell påvirke tjenestene?

Nei. Det er en tidsforskjell på to timer mellom Mauritius og sentraleuropeisk tid og tre timer mellom Mauritius og østeuropeisk tid, men arbeidstidene til teamene i Mauritius er tilpasset arbeidstidene til deres europeiske kunder. Det vil ikke påvirke tilgjengeligheten.

1.6 Leverer SD Worx Mauritius allerede tjenester til andre europeiske land?

SD Worx Mauritius leverer allerede tjenester til ulike deler av SD Worx-konsernet, men har foreløpig ikke utvidet disse tjenestene til det nordiske tilbudet. Fra og med 2026 planlegger vi å starte samarbeidet for svenske, norske og finske kunder.

2. Databeskyttelse og internasjonale overføringer

A. Sted for lagring og overføringsmekanisme

2.1 Vil samarbeidet med SD Worx Mauritius påvirke lokasjonen for våre datasentre og SaaS-tjenester?

Lokasjonen for datasentre og SaaS-tjenester påvirkes ikke av denne utvidelsen og vil fortsatt være innenfor EØS.

2.2 Omfatter dette en internasjonal overføring av personopplysninger?

Ja. Selv om systemene og primær drift fortsatt er lokalisert innenfor EØS, kan fjernaksess fra Mauritius til personopplysninger lagret i EØS anses som en begrenset overføring etter kapittel V i GDPR. SD Worx behandler derfor slik tilgang som en overføring som krever et egnet overføringsgrunnlag der dette er relevant.

Mauritius er per i dag ikke omfattet av en adekvansbeslutning etter artikkel 45 i GDPR. For relevant intern tilgang innen konsernet, eller overføring til SD Worx Mauritius, baserer SD Worx seg på egnede garantier etter artikkel 46 i GDPR – primært EUs standard personvernbestemmelser (Standard Contractual Clauses, SCCs) som inngår i SD Worx' konserninterne databehandleravtaler.

2.3 Hvilken overføringsmekanisme gjelder for tilgang fra SD Worx Mauritius?

Den aktuelle overføringsmekanismen er basert på SD Worx' konserninterne databehandleravtaler, som inkluderer de nyeste gjeldende EU-standard personvernbestemmelsene (Standard Contractual Clauses, SCC) for overføringer til konsernselskaper lokalisert utenfor EØS.

SD Worx har også gjennomført en vurdering av overføringskonsekvenser (Transfer Impact Assessment, TIA), som gjelder for enhver tilgang eller overføring til SD Worx Mauritius. Et TIA-dokument er tilgjengelig som en del av informasjonsgrunnlaget til kunder.

.

2.4 Er det nødvendig for kunder å signere separate SCC-er med SD Worx fordi SD Worx Mauritius er lokalisert utenfor EØS?

Nei. Kunder er ikke pålagt å inngå separate SCC-er med SD Worx som følge av at SD Worx Mauritius er lagt til som en underdatabehandler utenfor EØS.

Involveringen av SD Worx Mauritius som en tilknyttet underdatabehandler endrer ikke rollefordelingen i henhold til gjeldende kundeavtale eller databehandleravtale (DPA). Du som kunde forblir behandlingsansvarlig for dine personopplysninger, og det relevante SD Worx-selskapet er fortsatt ansvarlig for behandlingen som utføres av deres godkjente underdatabehandlere i samsvar med DPA.

Ettersom kunden har inngått avtale med et SD Worx-selskap etablert innenfor EØS, anses ikke kundeforholdet i seg selv som en internasjonal overføring etter kapittel V i GDPR. SCC-er er en overføringsmekanisme etter artikkel 46 i GDPR og kreves mellom en behandlingsansvarlig

eller databehandler i EØS (dataeksportør) og en mottaker i et tredjeland (utenfor EØS), med mindre et annet gyldig overføringsgrunnlag foreligger.

Den relevante internasjonale overføringen oppstår når SD Worx gjør personopplysninger tilgjengelige for, eller overfører personopplysninger til, SD Worx Mauritius, som er lokalisert utenfor EØS. Denne videreoverføringen håndteres innenfor SD Worx' kontraktsmessige rammeverk gjennom konserninterne databehandleravtaler, inkludert gjeldende EU-standard personvernbestemmelser (SCC-er).

2.5 Endrer bruken av SD Worx Mauritius rollen til SD Worx eller kunden under databehandleravtalen (DPA)?

Ettersom dette er en videreoverføring mellom selskaper i SD Worx-konsernet som opptrer som databehandlere i samme behandlingskjede, implementeres SCC-er mellom det relevante SD Worx-selskapet i EØS og SD Worx Mauritius. Kunden behøver derfor ikke å signere separate SCC-er for denne overføringen.

B. Vurdering av dataoverføring og tilhørende sikringstiltak.

2.6 Hvor ofte gjennomgås vurderingen av overføringskonsekvenser?

SD Worx overvåker relevante juridiske og faktiske utviklinger som kan påvirke internasjonale overføringer og vurderingen av overføringskonsekvenser (TIA). Når ny informasjon er relevant i henhold til SCC-ene, herunder klausul 14, vurderer SD Worx på nytt om forholdene kan påvirke sannsynligheten for tilgang fra offentlige myndigheter eller effektiviteten av de sikkerhetsmekanismene det er basert på.

2.7 Hva er hovedrisiko som er identifisert i overføringskonsekvenser (TIA), og hvordan håndteres dette?

Hovedrisikoene identifisert i vurderingen av overføringskonsekvenser (TIA) knytter seg til tilgang fra offentlige myndigheter, lavere praktisk håndheving og mer begrensede muligheter for effektive rettsmidler sammenlignet med EØS.

Fra et operasjonelt perspektiv er den viktigste risikoen at autorisert personell i Mauritius kan ha fjernaksess til data om kundens ansatte, som identifikasjonsdata, offentlige identifikatorer, ansettelsesopplysninger og lønnsdata, der dette er nødvendig for å utføre deres oppgaver. Mer konkret vurderte analysen at mauritisk lovgivning inneholder unntak knyttet til nasjonal sikkerhet, forsvar og offentlig sikkerhet, og at det er begrenset offentlig tilgjengelig informasjon om myndighetenes faktiske tilgang til private data. Det ble også konstatert at regulatorisk tilsyn og praktiske mekanismer for rettsmidler er mer begrensede enn i EØS.

Disse risikoene reduseres gjennom kontraktsmessige, tekniske og organisatoriske sikkerhetstiltak. Overføringen er omfattet av EUs standard personvernbestemmelser (SCC-er) og av konsernets system for informasjonssikkerhetsstyring. Kundedata lagres ikke i hvile i Mauritius, data er kryptert under overføring, og tilgang er rollebasert, begrenset til tjenstlig behov og gjenstand for jevnlig gjennomgang. I tillegg er ansatte underlagt konfidensialitetsforpliktelser, og SD Worx Mauritius opererer innenfor SD Worx' konsernfelles rammeverk for sikkerhets- og personvernkontroller.

TIA-en konkluderer med at sannsynligheten for tilgang fra offentlige myndigheter er lav, at SD Worx Mauritius så langt ikke har mottatt slike forespørsler, og at de implementerte tilleggstiltakene reduserer den gjenværende risikoen til et akseptabelt nivå.

C. Tilgang for offentlige myndigheter

2.8 Har SD Worx Mauritius mottatt forespørsler fra offentlige myndigheter om tilgang til kundedata?

Nei. Siden etableringen av SD Worx Mauritius i 2016 har SD Worx-konsernet ikke mottatt noen forespørsler fra offentlige myndigheter i Mauritius om tilgang til kundedata.

2.9 Hvordan sikres data mot tilgang fra lokale myndigheter i Mauritius?

SD Worx Mauritius er lokalisert utenfor EØS, og mulig tilgang fra offentlige myndigheter er derfor særskilt vurdert som en del av SD Worx' vurdering av dataoverføringer. Samtidig anvender SD Worx

en konsistent, konsernfelles tilnærming til håndtering av forespørsler fra offentlige myndigheter, uavhengig av hvilket land forespørselen kommer fra

Mauritius er generelt anerkjent som en stabil, demokratisk jurisdiksjon. Offentlig tilgjengelige rangeringer basert på EIU sitt demokratiindeks for 2026 klassifiserer Mauritius som et «fullverdig demokrati» med en score på 8,23. Denne landkonteksten er relevant, men SD Worx baserer seg ikke utelukkende på denne faktoren. Beskyttelsen av kunders personopplysninger er primært forankret i kontraktsmessige, tekniske og organisatoriske sikkerhetstiltak, inkludert SCC-er, vurdering av dataoverføringer, tilgangskontroller, logging, kryptering og SD Worx' konsernfelles sikkerhetsrammeverk.

I tillegg forblir produksjonsdata lagret innenfor EØS. Lokale myndigheter kan derfor ikke få direkte tilgang til disse, og må eventuelt pålegge SD Worx Mauritius å hente ut data. SD Worx gir verken direkte eller ubegrenset tilgang til sine systemer eller kundedata til myndigheter i Mauritius. Eventuell tilgang må derfor skje gjennom en formell forespørsel, som vil bli vurdert i tråd med SD Worx' gjeldende juridiske og styringsmessige prosesser (se neste punkt).

2.10 Hva skjer dersom SD Worx mottar en forespørsel fra offentlige myndigheter om tilgang til data som er tilgjengelige fra Mauritius?

Dersom en rettslig bindende forespørsel mottas, vil SD Worx vurdere den juridiske gyldigheten, omfanget og forholdsmessigheten av forespørselen. Dersom det foreligger rimelige grunner til å anse forespørselen som ulovlig, uforholdsmessig eller for vidtrekkende, vil SD Worx bestride forespørselen eller forsøke å begrense den.

Der det er juridisk og kontraktsmessig tillatt, vil SD Worx varsle berørt kunde så snart som praktisk mulig og gi relevant informasjon om forespørselen. Dersom varsling er juridisk forbudt, vil SD Worx gjøre rimelige anstrengelser for å få opphevet dette forbudet. Der det er hensiktsmessig, kan SD Worx også anmode myndigheten om å rette forespørselen direkte til kunden. Dersom utlevering er rettslig påkrevd, vil SD Worx kun utlevere et minimum av nødvendige opplysninger.

D. Videre underdatabehandlere og videreoverføringer

2.11 Vil SD Worx Mauritius benytte ytterligere underdatabehandlere eller overføre data videre?

Nei. Involveringen av SD Worx Mauritius innebærer ikke at SD Worx Mauritius selvstendig engasjerer ytterligere underdatabehandlere for de nordiske tjenestene, eller at det benyttes

underdatabehandlere som er spesifikke for Mauritius og kun knyttet til aktivitetene som utføres derfra.

Dersom SD Worx benytter underdatabehandlere, håndteres dette i utgangspunktet gjennom SD Worx' konsernfelles anskaffelsesprosesser og standard styringspraksis for underdatabehandlere. Eventuelle slike underdatabehandlere vil fortsatt være underlagt gjeldende kundeavtale, avtalt prosess for varsling om underdatabehandlere, samt gjeldende krav til personvern.

3. Tilgang til personopplysninger

3.1 Hvilke personopplysninger kan SD Worx Mauritius få tilgang til?

Ansatte i SD Worx Mauritius kan få tilgang til alle typer personopplysninger som er angitt i vår avtale. De relevante kategoriene av personopplysninger som behandles, er de som er beskrevet i gjeldende avtale, databehandleravtale (DPA) og tjenestebeskrivelse for skyløsningen.

Avhengig av tjenestene og støtterollen kan personell i SD Worx Mauritius teknisk sett få tilgang til personopplysninger som behandles i de aktuelle SD Worx-tjenestene. Dette kan omfatte kategorier av personopplysninger som allerede behandles for deg, og – der det er relevant – særlige kategorier av personopplysninger dersom slike behandles i den aktuelle tjenesten. Tilgang gis ikke som generell eller ubegrenset tilgang til alle ansatte, men er knyttet til rolle, støttebehov og operasjonelt formål etter prinsippet om tjenstlig behov.

3.2 Hva betyr «tilgang basert på tjenstlig behov» i praksis?

«Tjenstlig behov» innebærer at tilgang er rollebasert og kun gis der det er nødvendig for et definert operasjonelt eller teknisk formål. Tilgangsrettigheter er knyttet til den ansattes rolle, det aktuelle støtteomfanget og oppgaven som skal utføres. Disse administreres gjennom SD Worx' konsernfelles systemer for identitets- og tilgangsstyring.

Dette innebærer også at teknisk tilgangsmulighet ikke er det samme som ubegrenset operasjonell bruk. For eksempel kan enkelte infrastruktur- eller tredjelinjestøtteroller ha administrativ tilgang til systemer eller komponenter hvor kundedata finnes, uten at de behandler slike data i sitt daglige arbeid, med mindre det er nødvendig for en spesifikk autorisert oppgave.

SD Worx benytter en strukturert modell for rollebasert tilgangskontroll for å sikre at tilgang til systemer og data er strengt begrenset og forsvarlig administrert.

Tilgang gis basert på prinsippene om minste privilegium, tjenstlig behov og oppgavefordeling, og kun etter korrekt autentisering og autorisasjon. Brukertilgang defineres gjennom roller, brukergrupper og regler for datatilgang.

Tilgang forvaltes gjennom hele livssyklusen, inkludert formell forespørsel og godkjenning, periodiske gjennomganger og rettidig tilbakekalling. All tilgang sikres med mekanismer som Single Sign-On (SSO) og flerfaktorautentisering (MFA), og brukeraktivitet loggføres og overvåkes.

3.3 Kan personell i SD Worx Mauritius få tilgang til levende lønnsdata i klartekst?

Det er en mulighet. I enkelte støtte- eller infrastruktursituasjoner kan tilgang til produksjonssystemer eller data i klartekst være teknisk mulig dersom dette er nødvendig for en autorisert oppgave. Slik tilgang er ikke ment som del av normal forretningsbehandling og er underlagt rollebasert tilgangskontroll, godkjenningskrav, logging og overvåking.
For privileged or production access, access is granted based on business need and managed under SD Worx's identity and access management controls. Privileged access should be handled through the applicable privileged access process and audit trail, including session recording where applicable under the relevant platform and control framework.

3.4 Kan lokalt IT- eller infrastrukturpersonell i Mauritius få tilgang til databaser, tickets, SFTP/filoverføring eller applikasjonsdata?

Tilgang avhenger av rolle og operasjonelt behov. Slikt personell får ikke generell tilgang til kundedata.

Eksempel 1: Databaseadministratorer kan ha tilgang til databaser for overvåking, vedlikehold og sikkerhetskopiering.

Tilsvarende kan enkelte server- eller tredjelinjesupportroller ha administrativ tilgang til infrastrukturkomponenter, som for eksempel en SFTP-server, noe som i en supportsituasjon kan innebære en teknisk mulighet til å få tilgang til filer. Slik tilgang styres gjennom rollebasert autorisasjon, er underlagt gjeldende rammeverk for tilgangsstyring og loggføres i samsvar med SD Worx sine sikkerhetskontroller.

Eksempel 2: Server- eller tredjelinjestøtte kan ha administrativ tilgang til komponenter som SFTP-servere, som kan gi teknisk mulighet for tilgang i støttesituasjoner, noe som i supportsituasjoner kan innebære en teknisk mulighet til å få tilgang til filer. Disse behandler imidlertid ikke slike opplysninger som en del av sin daglige virksomhet. Tilgang er begrenset basert på rolle, og all tilgang loggføres i samsvar med våre sikkerhetskontroller.

All tilgang er rollebasert, kontrollert og loggført.

3.5 Vil kundedata bli lagret lokalt i Mauritius?

Nei. Kundedata forblir lagret innenfor EØS. Samarbeidet innebærer kun kontrollert fjernaksess der det er nødvendig.

4. Sikkerhetsrutiner og kontroller

4.1 Sikkerhet som en del av våre daglige prosesser

Beskyttelse av kundedata er en grunnleggende prioritet i SD Worx. Dette sikres gjennom et omfattende kontrollrammeverk basert på ISO 27001 og uavhengige revisjoner (ISAE 3402, ISAE 3000).

Kontroller er integrert i:

- mennesker (roller og ansvar)
- prosesser (policyer og rutiner)
- teknologi (kryptering, overvåking og tilgangsstyring)

I tillegg opprettholder SD Worx konsernfelles styringsrammeverk for både sikkerhet og personvern. Disse rammeverkene fastsetter minimumskrav og gjennomgås og oppdateres løpende for å reflektere utviklende risikoer, lovkrav og beste praksis.

Sikkerhetskontroller er ikke bare sentralt definert, men implementeres også konsekvent på tvers av land, forretningsenheter og løsninger, med fleksibilitet til å ivareta lokale regulatoriske krav der det er nødvendig. Dette sikrer et ensartet beskyttelsesnivå samtidig som etterlevelse opprettholdes i alle regioner vi opererer i.

Kontrollene overvåkes og forbedres kontinuerlig gjennom risikovurderinger, revisjoner og jevnlig testing, noe som sikrer at SD Worx opprettholder et høyt nivå av sikkerhetsmodenhet og robusthet.

4.2 Hvilke tekniske og organisatoriske tiltak gjøres? Hvordan følges etterlevelse opp?

SD Worx Mauritius opererer under SD Worx' konsernfelles sikkerhetsrammeverk. Det er ikke ment at virksomheten skal operere under en separat eller mindre omfattende sikkerhetsmodell for aktivitetene som omfattes av dette samarbeidet.

SD Worx Mauritius opererer under samme sikkerhetsrammeverk som konsernet, inkludert:

- tilgangsstyring
- logging og overvåking
- hendelseshåndtering
- kryptering
- styring av leverandører og IKT-kjede

SD Worx Mauritius er inkludert i konsernets ISMS og ISO 27001-sertifisering. Dokumentasjon som SoA og sikkerhetsmateriale er tilgjengelig.

Relevante kontroller omfatter blant annet tilgangsstyring, konfidensialitetsforpliktelser, styring av informasjonssikkerhet, logging og overvåking, hendelseshåndtering, kontroll av leverandører og IKT-forsyningskjede, sikker autentisering, håndtering av privilegert tilgang, sårbarhetsstyring, kryptering og forebygging av datalekkasjer. Disse kontrollene er dokumentert i SD Worx' sikkerhetsdokumentasjon, inkludert gjeldende tekniske og organisatoriske tiltak (TOMs), ISO 27001-sertifiseringsdokumentasjon, Statement of Applicability samt nordisk whitepaper for sikkerhet og personvern.

SD Worx i Norden og SD Worx Mauritius er sertifisert med de samme kontrollene.

4.3 Hvordan logges og overvåkes tilgang?

Logging skjer på applikasjons-, server- og tilkoblingsnivå. Overvåking skjer 24/7 via SOC-tjenester.

SD Worx opprettholder logging- og overvåkingskontroller som en del av sitt sikkerhetsrammeverk. For det nordiske skymiljøet opprettholdes logger på applikasjons-, server- og tilkoblingsnivå for å sikre loggintegritet og konfidensialitet. Systemlogger videresendes til en tredjeparts SOC-tjeneste for døgnkontinuerlig overvåking, og potensielle avvik eller sikkerhetshendelser håndteres i samsvar med SD Worx' kontroller i henhold til ISO 27001/ISO 27701.

Systemlogger gjøres tilgjengelige ved revisjoner, med gjeldende oppbevaringsperiode beskrevet i relevant sikkerhetsdokumentasjon. Mer detaljert dokumentasjon om systemlogging kan gjøres tilgjengelig via relevante kundekanaler eller på forespørsel der dette er tilgjengelig.

4.4 Blir privilegerte sesjoner loggført, og kreves det kundespesifikk godkjenning før tilgang til produksjonsmiljøet gis?

Privilegert tilgang administreres gjennom SD Worx sitt rammeverk for tilgangskontroll og gis kun når det er nødvendig for et gyldig operasjonelt eller teknisk formål. Tilgang til produksjonsmiljøer, inkludert privilegert tilgang, krever formell godkjenning basert på forretningsbehov og følger IAM-kontroller som minste privilegium, funksjonssegregering og periodisk gjennomgang av privilegerte kontoer.

Aktiviteter med privilegert tilgang loggføres og overvåkes. Der privilegert tilgang skjer gjennom en plattform for håndtering av privilegert tilgang (PAM), gir plattformen et revisjonsspor og opptak av sesjoner i samsvar med gjeldende kontrollrammeverk.

Kundespesifikk godkjenning kreves ikke for hver enkelt tilgang til produksjonsmiljøet, med mindre dette er særskilt avtalt i kundekontrakten. Tilgang styres i stedet gjennom SD Worx sine interne kontroller for godkjenning, tilgangsstyring, logging og overvåking.

4.5 Er kryptering benyttet, og hvordan håndteres krypteringsnøkler?

Ja. SD Worx benytter krypteringskontroller for data under overføring og, der det er relevant, for data ved lagring. For det nordiske skymiljøet er lønnsapplikasjonenes databaser kryptert ved lagring der det er aktuelt, filoverføringer gjennomføres via kryptert SFTP, og nettverkstrafikk er beskyttet ved bruk av HTTPS og TLS.

For nordiske kunder lagres krypteringsnøkler i SD Worx sitt nordiske passordhvelv, som er plassert i SD Worx sine datasentre i Finland. Passordhvelvet har revisjonsspor og er underlagt prinsipper om minste privilegium og rollebasert tilgangsstyring. Kun navngitte personer har tilgang basert på rolle, for eksempel databaseadministratorer for databasenøkler og nettverksadministratorer for transportkrypteringsnøkler.

Avhengig av omfanget av støttetjenester kan enkelte databaseadministrasjonsroller utføres fra Mauritius. I slike tilfeller kan disse personene ha behov for tilgang til relevante nøkler for å utføre sine oppgaver, i henhold til gjeldende rollebaserte kontroller og logging.

4.6 Finnes det kontroller som hindrer lokal nedlasting, kopiering eller masseeksport av produksjonsdata?

SD Worx benytter lagdelte kontroller for å forhindre eller begrense uautorisert nedlasting, kopiering, eksport eller annen uttrekking av kundedata fra produksjonssystemer. Disse kontrollene omfatter tilgangsbegrensninger, forebygging av datalekkasjer (DLP), endepunktsikkerhet, begrensninger på bruk av flyttbare medier, autoriserte filoverføringskanaler samt logging og overvåking.

4.7 Hva skjer dersom det oppstår uautorisert tilgang eller en utvidelse av tilgangsrettigheter?

SD Worx følger en formalisert prosess for håndtering av sikkerhets- og personvernbrudd. Enhver mistenkt eller bekreftet uautorisert tilgang håndteres gjennom relevant hendelseshåndteringsprosess, inkludert vurdering, eskalering, begrensning av skade og varsling til kunde der dette kreves i henhold til gjeldende databehandleravtale og GDPR-krav.

4.8 Gjelder kundens revisjonsrettigheter også SD Worx Mauritius sitt kontrollmiljø?

Ja. Kundens revisjonsrettigheter etter gjeldende databehandleravtale gjelder for SD Worx sitt kontrollmiljø for tjenestene, inkludert der SD Worx benytter tilknyttede underdatabehandlere som SD Worx Mauritius til behandling av kunders personopplysninger.

SD Worx viderefører kontraktsmessig relevante krav til personvern og informasjonssikkerhet til sine underdatabehandlere, og forblir ansvarlig for deres etterlevelse i samsvar med gjeldende databehandleravtale.