Personuppgiftsbiträdesavtal

Personuppgifter som Nord Node behandlar för sina kunders räkning (artikel 28 i dataskyddsförordningen)

Version 1.0 · Gäller från: 24 september 2026

> Detta dokument utgör en del av Avtalet mellan Nord Node AB och Kunden. Det gäller när en Beställning har undertecknats och gäller inte för användning av Nord Nodes webbplats.

1. Bakgrund och tillämpningsområde

1.1 Detta personuppgiftsbiträdesavtal (**"Biträdesavtalet"**) utgör en del av Avtalet mellan Nord Node AB, org.nr 559493-4936 (**"Nord Node"** eller **"Biträdet"**), och Kunden (**"den Personuppgiftsansvarige"**). Det gäller när Nord Node behandlar personuppgifter för Kundens räkning vid tillhandahållandet av Tjänsterna.

1.2 Biträdesavtalet uppfyller kraven i artikel 28.3 i förordning (EU) 2016/679 (**"dataskyddsförordningen"**) och gäller tillsammans med lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

1.3 Biträdesavtalet gäller inte personuppgifter som Nord Node behandlar som personuppgiftsansvarig för egna ändamål, såsom kundadministration, fakturering och loggning av säkerheten i Nord Nodes egna system. Den behandlingen beskrivs i Nord Nodes integritetspolicy.

2. Definitioner

2.1 Begrepp som "personuppgifter", "behandling", "personuppgiftsansvarig", "personuppgiftsbiträde", "registrerad", "personuppgiftsincident" och "tillsynsmyndighet" har den betydelse som anges i artikel 4 i dataskyddsförordningen. **"Dataskyddslagstiftning"** avser dataskyddsförordningen och den kompletterande nationella lagstiftning som gäller för behandlingen. **"Underbiträde"** avser ett annat personuppgiftsbiträde som Nord Node anlitar för att behandla Kundens personuppgifter. Övriga begrepp har den betydelse som anges i Allmänna villkor.

3. Roller och Kundens ansvar

3.1 Kunden är personuppgiftsansvarig och Nord Node är personuppgiftsbiträde för de personuppgifter som beskrivs i bilaga 1. Om Kunden själv är personuppgiftsbiträde åt en annan personuppgiftsansvarig är Nord Node Kundens underbiträde, och Kunden ansvarar för att dess instruktioner överensstämmer med den personuppgiftsansvariges instruktioner.

3.2 Kunden ansvarar för att den behandling som Kunden instruerar Nord Node att utföra har en rättslig grund, att de registrerade har fått den information som krävs och att de personuppgifter som Kunden lämnar har samlats in på ett lagligt sätt.

3.3 Kundens egna avtal med Leverantörer av Tredjepartstjänster, såsom Microsoft Customer Agreement och Microsofts Products and Services Data Protection Addendum, reglerar Leverantörens behandling av

personuppgifter i Kundens egen molnmiljö. När Nord Node administrerar en sådan miljö är Nord Node personuppgiftsbiträde endast i fråga om Nord Nodes egen administrativa åtkomst och verksamhet.

4. Instruktioner

4.1 Nord Node får endast behandla personuppgifterna enligt Kundens dokumenterade instruktioner, även när det gäller överföringar till tredjeland, om inte unionsrätten eller en medlemsstats nationella rätt som Nord Node omfattas av kräver annat. I sådant fall ska Nord Node informera Kunden om det rättsliga kravet innan behandlingen, såvida inte sådan information är förbjuden med hänvisning till ett viktigt allmänintresse.

4.2 Kundens instruktioner vid tidpunkten för detta Biträdesavtal framgår av Avtalet, inklusive detta Biträdesavtal och bilaga 1. Kunden får lämna kompletterande eller ändrade instruktioner skriftligen genom en Behörig kontaktperson. Om nya instruktioner påverkar Tjänsternas omfattning eller kostnad gäller punkt 4.2 i Allmänna villkor.

4.3 Nord Node ska omedelbart informera Kunden om en instruktion enligt Nord Nodes uppfattning strider mot Dataskyddslagstiftningen. Nord Node får avbryta den berörda behandlingen tills Kunden bekräftar eller ändrar instruktionen.

5. Sekretess och personal

5.1 Nord Node ska säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av lagstadgad tystnadsplikt, och att de får lämplig utbildning i dataskydd och informationssäkerhet.

5.2 Nord Node ska begränsa åtkomsten till personuppgifterna till personal som behöver den för att tillhandahålla Tjänsterna.

6. Säkerhet

6.1 Nord Node ska vidta och upprätthålla de tekniska och organisatoriska åtgärder som beskrivs i bilaga 2 för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, i enlighet med artikel 32 i dataskyddsförordningen.

6.2 Nord Node får uppdatera åtgärderna i bilaga 2 över tid för att återspegla den tekniska utvecklingen, förutsatt att uppdateringarna inte sänker den samlade skyddsnivån.

6.3 Kunden ansvarar för säkerheten i de delar av Kundens miljö som Nord Node inte förvaltar, samt för att bedöma om åtgärderna i bilaga 2 är lämpliga för Kundens behandling.

7. Underbiträden

7.1 Kunden ger Nord Node ett allmänt skriftligt förhandstillstånd att anlita Underbiträden. De Underbiträden som anlitas vid tidpunkten för detta Biträdesavtal anges i bilaga 3. De Underbiträden som vid varje tidpunkt anlitas, med namn, vilken behandling de utför, var behandlingen sker och eventuell överföringsmekanism, anges i Nord Nodes förteckning över underbiträden, som Nord Node håller aktuell och lämnar till Kunden på begäran.

7.2 Nord Node ska underrätta Kunden minst 30 dagar innan ett nytt Underbiträde anlitas eller ett befintligt ersätts, via e-post till Kundens Behöriga kontaktperson eller genom annan överenskommen kanal. Underrättelsen ska ange Underbiträdets namn, var behandlingen sker, vilken behandling det ska utföra och vilken överföringsmekanism som eventuellt används.

7.3 Kunden får skriftligen invända mot ändringen på skäliga dataskyddsgrunder inom underrättelsetiden. Parterna ska då diskutera invändningen i god tro. Om Nord Node inte kan erbjuda ett rimligt alternativ får Kunden säga upp de berörda Tjänsterna med verkan från den dag då det nya Underbiträdet skulle börja behandla Kundens personuppgifter, utan att betala avgifter för förtida upphörande av de berörda

Förvaltade tjänsterna. Avgifter för Abonnemang ska fortfarande betalas i enlighet med Leverantörens villkor för åtagandeperioden.

7.4 I en nödsituation, till exempel om ett befintligt Underbiträde plötsligt inte kan leverera, får Nord Node anlita ett ersättande Underbiträde med kortare varsel och ska då underrätta Kunden så snart som möjligt. Kundens rätt att invända enligt punkt 7.3 gäller fortfarande.

7.5 Nord Node ska genom skriftligt avtal ålägga varje Underbiträde dataskyddsförpliktelser som ger minst samma skyddsnivå som detta Biträdesavtal, särskilt i fråga om säkerhet. Nord Node ansvarar fullt ut gentemot Kunden för att dess Underbiträden fullgör sina förpliktelser.

7.6 På begäran ska Nord Node ge Kunden en kopia av de relevanta dataskyddsvillkoren i avtalet med ett Underbiträde. Kommersiell information får då strykas.

8. Överföring till länder utanför EU/EES

8.1 Nord Node ska behandla och lagra personuppgifterna inom EU/EES, om inte annat anges i bilaga 3 eller i förteckningen över underbiträden, eller Kunden instruerar annat.

8.2 Nord Node får överföra personuppgifter till ett land utanför EU/EES, eller tillåta ett Underbiträde att göra det, endast i enlighet med kapitel V i dataskyddsförordningen, till exempel:

(a) till ett land, eller en certifierad organisation, som omfattas av ett beslut om adekvat skyddsnivå från Europeiska kommissionen, såsom ramverket för dataskydd mellan EU och USA (EU–US Data Privacy Framework); eller

(b) med stöd av Europeiska kommissionens standardavtalsklausuler (genomförandebeslut (EU) 2021/914), tillsammans med en bedömning av lagstiftningen i mottagarlandet och kompletterande åtgärder vid behov.

8.3 Om support eller åtkomst från länder utanför EU/EES är tekniskt möjlig (till exempel via ett Underbiträdes globala supportfunktion) anges detta i bilaga 3 och, för det enskilda Underbiträdet, i förteckningen över underbiträden.

8.4 Om ett beslut om adekvat skyddsnivå som tillämpas enligt denna punkt ogiltigförklaras ska Nord Node informera Kunden och utan onödigt dröjsmål tillämpa en annan överföringsmekanism eller upphöra med överföringen.

9. Bistånd vid de registrerades rättigheter

9.1 Med beaktande av behandlingens art ska Nord Node genom lämpliga tekniska och organisatoriska åtgärder hjälpa Kunden att besvara begäranden från registrerade som utövar sina rättigheter enligt kapitel III i dataskyddsförordningen.

9.2 Om Nord Node direkt från en registrerad tar emot en begäran som avser Kundens personuppgifter ska Nord Node utan onödigt dröjsmål vidarebefordra den till Kunden och inte själv besvara den, annat än genom att hänvisa den registrerade till Kunden, om inte Kunden instruerar annat.

10. Personuppgiftsincidenter

10.1 Nord Node ska underrätta Kunden utan onödigt dröjsmål, och i vart fall inom 48 timmar, efter att ha fått vetskap om en personuppgiftsincident som berör Kundens personuppgifter.

10.2 Underrättelsen ska, i den mån informationen finns tillgänglig, beskriva:

(a) incidentens art, inklusive kategorier av och ungefärligt antal registrerade och personuppgiftsposter som berörs;

(b) namn och kontaktuppgifter för Nord Nodes kontaktperson;

(c) de sannolika konsekvenserna av incidenten; och

(d) de åtgärder som vidtagits eller föreslagits för att hantera incidenten och mildra dess potentiella negativa effekter.

Om all information inte finns tillgänglig vid den första underrättelsen ska Nord Node lämna den i omgångar utan ytterligare onödigt dröjsmål.

10.3 Nord Node ska vidta de åtgärder som skäligen krävs för att begränsa incidenten och dess effekter, och ska hjälpa Kunden att fullgöra sina skyldigheter att anmäla incidenten till tillsynsmyndigheten och informera de registrerade enligt artiklarna 33 och 34 i dataskyddsförordningen. Kunden ansvarar för att besluta om och göra sådana anmälningar.

10.4 Att Nord Node lämnar en underrättelse eller bistånd innebär inte ett medgivande av fel eller ansvar.

11. Konsekvensbedömningar och förhandssamråd

11.1 Med beaktande av behandlingens art och den information som Nord Node har tillgång till ska Nord Node hjälpa Kunden med konsekvensbedömningar avseende dataskydd och förhandssamråd med tillsynsmyndigheten enligt artiklarna 35 och 36 i dataskyddsförordningen, i den mån de avser Tjänsterna.

12. Granskning och information

12.1 Nord Node ska ge Kunden tillgång till den information som krävs för att visa att artikel 28 i dataskyddsförordningen och detta Biträdesavtal efterlevs, inklusive en beskrivning av Nord Nodes säkerhetsåtgärder, relevanta policyer samt eventuella certifieringar eller revisionsrapporter.

12.2 Om Kunden skäligen anser att den lämnade informationen är otillräcklig, eller om en tillsynsmyndighet kräver det, får Kunden genomföra en granskning, inklusive inspektion, själv eller genom en oberoende revisor som omfattas av tystnadsplikt och som inte är konkurrent till Nord Node. Kunden ska meddela granskningen minst 30 dagar i förväg, om inte en kortare tid krävs av en tillsynsmyndighet eller efter en personuppgiftsincident. Granskning får ske högst en gång per tolvmånadersperiod, om inte en personuppgiftsincident har inträffat eller tillsynsmyndigheten kräver det.

12.3 Granskningen ska genomföras under normal arbetstid, utan att i onödan störa Nord Nodes verksamhet, och utan åtkomst till andra kunders data eller till Nord Nodes konfidentiella information som saknar betydelse för Kunden. Vardera Parten står för sina egna kostnader. Nord Node får debitera tid för bistånd vid granskningar som överstiger en Arbetsdag per år enligt sina timpriser, utom när granskningen visar att Nord Node har gjort sig skyldigt till ett väsentligt brott mot detta Biträdesavtal.

12.4 Om en granskning avser ett Underbiträde får Nord Node tillmötesgå begäran genom att tillhandahålla Underbiträdets revisionsrapporter eller certifieringar.

13. Begäranden från myndigheter

13.1 Om en myndighet begär åtkomst till Kundens personuppgifter ska Nord Node hänvisa myndigheten till Kunden och utan onödigt dröjsmål underrätta Kunden, om det inte är förbjudet enligt lag. Nord Node får endast lämna ut uppgifterna om det krävs enligt lag och ska begränsa utlämnandet till vad som krävs.

14. Återlämnande och radering

14.1 När Tjänsterna upphör ska Nord Node, enligt Kundens val, återlämna personuppgifterna till Kunden eller göra dem tillgängliga för export enligt punkt 15 i Allmänna villkor, och därefter radera dem.

14.2 Nord Node ska radera personuppgifterna, inklusive kopior, inom 60 dagar efter utgången av den exportperiod som anges i punkt 15.3 i Allmänna villkor. Uppgifter i säkerhetskopior raderas när säkerhetskopiorna löper ut enligt den normala säkerhetskopieringscykeln, dock senast 90 dagar efter nämnda raderingsdag. Fram till raderingen skyddas uppgifterna enligt detta Biträdesavtal.

14.3 Nord Node får behålla personuppgifter i den mån det krävs enligt unionsrätten eller en medlemsstats nationella rätt. I sådant fall ska Nord Node hålla uppgifterna konfidentiella och endast behandla dem för det ändamål som lagen kräver.

14.4 På begäran ska Nord Node skriftligen bekräfta raderingen.

15. Ansvar

15.1 Ansvaret mellan Parterna för brott mot detta Biträdesavtal regleras av punkt 19 i Allmänna villkor, inklusive den höjda beloppsbegränsningen i punkt 19.6.

15.2 Vardera Parten ansvarar för administrativa sanktionsavgifter som en tillsynsmyndighet påfört den. Ingen av Parterna får kräva den andra Parten på ersättning för sådana avgifter, utom när en sanktionsavgift som påförts en Part har orsakats av den andra Partens brott mot detta Biträdesavtal eller mot Dataskyddslagstiftningen. Det belopp som då kan krävas omfattas av punkt 15.1.

15.3 Denna punkt begränsar inte någon av Parternas ansvar gentemot registrerade enligt artikel 82 i dataskyddsförordningen. Om en Part har betalat full ersättning till en registrerad får den Parten kräva tillbaka den del av ersättningen från den andra Parten som motsvarar den andra Partens del av ansvaret, i enlighet med artikel 82.5 i dataskyddsförordningen.

16. Register och samarbete

16.1 Nord Node för ett register över alla kategorier av behandling som utförs för Kundens räkning i enlighet med artikel 30.2 i dataskyddsförordningen.

16.2 Vardera Parten ska på begäran samarbeta med tillsynsmyndigheten.

17. Kostnader för bistånd

17.1 Bistånd enligt punkterna 9, 11 och 12 som går utöver vad som normalt ingår i Tjänsterna, och som inte har orsakats av Nord Nodes avtalsbrott, får debiteras enligt de timpriser som anges i Beställningen. Nord Node ska om möjligt informera Kunden om den förväntade kostnaden i förväg. Bistånd enligt punkt 10 i samband med en personuppgiftsincident som Nord Node har orsakat debiteras inte.

18. Giltighetstid och rangordning

18.1 Detta Biträdesavtal gäller så länge Nord Node behandlar personuppgifter för Kundens räkning, även efter att Avtalet har upphört och till dess att uppgifterna har återlämnats eller raderats.

18.2 I frågor som rör behandling av personuppgifter har detta Biträdesavtal företräde framför övriga dokument som ingår i Avtalet.

18.3 Svensk lag ska tillämpas på detta Biträdesavtal och tvister ska lösas enligt punkt 24 i Allmänna villkor.

Bilaga 1 — Beskrivning av behandlingen

Uppgift	Beskrivning
Föremål och varaktighet	Tillhandahållande av Tjänsterna enligt Avtalet, under Avtalets giltighetstid och till dess att personuppgifterna har återlämnats eller raderats enligt punkt 14.
Behandlingens art och ändamål	Administration, support, övervakning, underhåll och säkerhetsförvaltning av Kundens miljö; servicedesk och ärendehantering via kundportalen; enhetshantering, uppdateringar och programdistribution; administration av identiteter och behörigheter; hantering av de inloggningsuppgifter som används för att administrera Kundens miljö; skydd för slutpunkter och e-post; säkerhetskopiering och återställning när det har beställts; incidenthantering; migrerings- och projektarbete; anskaffning och driftsättning av Tredjepartstjänster och Hårdvara, enligt Beställningen.
Kategorier av registrerade	Kundens anställda, konsulter och andra Användare; personer vars uppgifter finns i Kundens e-post, filer, system och, när säkerhetskopiering har beställts, säkerhetskopior (till exempel Kundens egna kunder, leverantörer och kontakter); för skolor och förskolor, elever och vårdnadshavare när de är Användare eller förekommer i Kundens data.
Kategorier av personuppgifter	Identitets- och kontaktuppgifter (namn, e-post, telefon, titel, användarnamn); uppgifter om portalkonton och innehåll i ärenden, inklusive beskrivningar, bilagor och korrespondens; uppgifter om konton, autentisering och åtkomst (gruppmedlemskap, roller, registrering för flerfaktorsautentisering, inloggningsloggar); enhets- och slutpunktsuppgifter (enhetsnamn, serienummer, IP-adress, inloggad användare, installerad programvara, konfigurationsstatus, uppdateringsstatus, telemetri om processer och nätverkstrafik när Tanium Threat Response eller motsvarande modul har beställts, plats om funktionen aktiverats för borttappade enheter); säkerhetslarm och utredningsdata; inloggningsuppgifter som används för att administrera Kundens miljö, lagrade i ett krypterat valv; innehåll i e-post, filer och annan data som lagras i Kundens miljö, i den mån Nord Node tar del av det för att utföra en uppgift eller innehar det i säkerhetskopior inom en beställd modul för säkerhetskopiering.
Känsliga personuppgifter	Nord Node avser inte att som sådana behandla särskilda kategorier av personuppgifter (artikel 9 i dataskyddsförordningen) eller uppgifter om lagöverträdelser (artikel 10). Sådana uppgifter kan dock finnas i Kundens e-post, filer, ärenden och säkerhetskopior, som Nord Node endast får ta del av enligt punkt 10.2 i Allmänna villkor. Kunden ska ange i Beställningen om Kundens miljö innehåller betydande mängder sådana uppgifter (till exempel hälsouppgifter eller uppgifter om barn), så att lämpliga ytterligare åtgärder kan avtalas.
Behandlingsåtgärder	Lagring, åtkomst, hämtning, kopiering (inklusive säkerhetskopiering när det har beställts), konfiguration, ändring, återställning, överföring mellan system (migreringar), begränsning och radering.
Plats	EU/EES, med förbehåll för bilaga 3.
Lagringstid	Under Tjänsternas giltighetstid och enligt punkt 14; ärendedokumentation sparas i 24 månader efter avslut om inte Kunden instruerar annat; lagringstid för säkerhetskopior enligt Beställningen; Nord Nodes loggar över administrativa åtgärder i Kundens miljö sparas i 12 månader.

Bilaga 2 — Tekniska och organisatoriska säkerhetsåtgärder

Område	Åtgärder
Styrning	Dokumenterad informationssäkerhetspolicy som fastställts av ledningen och ses över minst årligen; utsedd person med ansvar för informationssäkerhet och dataskydd; riskbedömning av nya tjänster och Underbiträden.
Personal	Sekretessåtaganden för all personal och alla underleverantörer; bakgrundskontroller som står i proportion till rollen, där lagen tillåter det; utbildning i säkerhet och dataskydd vid anställningens början och minst årligen; åtkomst tas bort skyndsamt när ett uppdrag upphör.
Identitet och åtkomst	Personliga namngivna konton, inga delade administratörskonton; nätfiskeresistent eller appbaserad flerfaktorsautentisering för all åtkomst till Nord Nodes system, leveransplattformar och Kundens miljöer; minsta möjliga och rollbaserad behörighet; privilegierad åtkomst tilldelas vid behov eller tidsbegränsat där plattformen stöder det, och förmedlas genom lösningen för privilegierad åtkomsthantering när den modulen används; behörighetsgenomgångar minst kvartalsvis; nödkonton under Kundens kontroll.
Hantering av inloggningsuppgifter	Inloggningsuppgifter som används för att administrera Kundens miljö lagras i ett krypterat lösenordsvalv med separat lagring per Kund, skyddat med flerfaktorsautentisering. Valvet bygger på en arkitektur där innehållet krypteras på enheten, så att valvleverantören inte kan läsa det. Inloggningsuppgifter lagras aldrig i klartext i ärenden, e-post, chatt eller dokumentation och byts vid personalförändringar och vid misstänkt röjande.
Plattform för enhetshantering	Förvaltningsagenter distribueras endast till enheter som omfattas av Tjänsterna. Administrativa åtgärder i plattformen loggas och kan härledas till en namngiven tekniker. Skript och paket granskas innan de distribueras till flera enheter. Administratörsåtkomst till plattformen är begränsad till behörig personal och skyddas med flerfaktorsautentisering.
Fjärråtkomst och fjärrsupport	Fjärråtkomst sker endast genom verktyg som Nord Node har godkänt. Fjärrstyrning av en Användares enhet kräver att Användaren accepterar sessionen och kan avslutas av Användaren när som helst; Nord Node använder inte obevakad fjärrstyrning. Konfiguration av enheter, säkerhetspolicyer, programdistribution och fjärradering sker genom förvaltningsplattformarna, som registrerar de åtgärder som vidtas. Varje fjärrsupportsession dokumenteras i serviceärendet med uppgift om tekniker, enhet, tidpunkt och syfte.
Plattform för ärendehantering	Ärenden lagras i Nord Nodes plattform för tjänstehantering med åtskillnad mellan Kunder, rollbaserad åtkomst för Nord Nodes personal och portalkonton begränsade till de Användare som Kunden har godkänt.
Säkerhet i enheter och infrastruktur	Nord Nodes egna enheter är förvaltade, krypterade, uppdaterade och skyddade med EDR; säkra konfigurationsbaslinjer; säkerhetsuppdateringar installeras inom de tider som anges i Tjänstebeskrivningen.
Kryptering	Kryptering under överföring (TLS 1.2 eller senare) för all fjärrförvaltning, plattformsåtkomst och dataöverföring; kryptering i vila för Nord Nodes enheter, dokumentationsplatser och, när en modul för säkerhetskopiering har beställts, säkerhetskopior.
Loggning och övervakning	Loggning av administrativa åtgärder i Nord Nodes system och leveransplattformar och, där plattformen stöder det, i Kundens miljö; loggar skyddas mot ändring och sparas i minst 12 månader; larm vid misstänkt aktivitet granskas under supporttid, om inte en modul för hanterad detektion och respons har beställts.

Område	Åtgärder
Säkerhetskopiering och kontinuitet (när modulen har beställts)	Säkerhetskopieringsjobb övervakas varje Arbetsdag och fel åtgärdas; återställningstester med den frekvens som anges i Beställningen och minst kvartalsvis; säkerhetskopior lagras inom EU/EES om inte annat anges i Beställningen; kryptering av säkerhetskopior i vila.
Nord Nodes egen kontinuitet	Nord Nodes verksamhetsdata finns i Microsoft 365 och i leveransplattformarna och förlitar sig på dessa plattformars motståndskraft tillsammans med kvarhållningsregler. Nord Node upprätthåller en dokumenterad rutin för att återställa sin leveransförmåga, inklusive åtkomst till kunddokumentation och inloggningsuppgifter.
Incidenthantering	Dokumenterad rutin för säkerhetsincidenter och personuppgiftsincidenter, inklusive bedömning, begränsning, underrättelse till Kunder inom de tider som anges i Biträdesavtalet och uppföljning efter incidenten.
Dataminimering och separation	Kunddata hålls logiskt åtskild per Kund i varje plattform; Kunddata kopieras inte till Nord Nodes system om det inte behövs för Tjänsterna; test- och demomiljöer använder inte Kundens personuppgifter.
Fysisk säkerhet	Kunddata lagras inte i lokaler som Nord Node kontrollerar, utom på krypterade enheter; Underbiträdens datacenter har erkända säkerhetscertifieringar, såsom ISO/IEC 27001.
Radering och destruktion	Säker radering av data när Tjänsterna upphör; certifierad radering eller fysisk destruktion av lagringsmedia, med dokumentation av processen.
Hantering av Underbiträden	Bedömning av säkerhet och dataskydd innan ett Underbiträde anlitas; skriftliga avtal som uppfyller artikel 28.4 i dataskyddsförordningen; genomgång av varje Underbiträdes certifieringar och förteckningar över egna underbiträden; regelbunden uppföljning.

Bilaga 3 — Godkända Underbiträden

Nord Node anlitar följande Underbiträden. Förteckningen över underbiträden, som Nord Node håller aktuell och lämnar till Kunden på begäran, anger de Underbiträden som gäller vid varje tidpunkt och utgör en del av denna bilaga 3.

Gäller samtliga Kunder:

Underbiträde	Tjänst / ändamål	Plats för behandlingen	Överföringsmekanism
Microsoft Ireland Operations Ltd (och Microsofts närstående bolag)	Nord Nodes egen Microsoft 365-miljö (e-post, dokument, Teams och servicedokumentation); portalerna för Microsoft Intune, Entra ID och Microsoft Defender som används för att administrera Kundens miljö; Microsoft Quick Assist för fjärrsupportsessioner som Användaren accepterar	EU/EES (Microsofts EU Data Boundary); begränsad fjärråtkomst för Microsofts personal från länder utanför EU/EES för support och säkerhet	EU–US Data Privacy Framework och standardavtalsklausuler i Microsofts Data Protection Addendum
ServiceNow (ServiceNow Nederland B.V. / ServiceNow, Inc.)	Kundportal, ärendehantering, beställningar, uppföljning av servicenivåer, kunskapsbank och CMDB	Datacenterregion inom EU/EES; supportåtkomst från länder utanför EU/EES kan förekomma	EU–US Data Privacy Framework; standardavtalsklausuler i ServiceNows Data Processing Addendum
Tanium (Tanium Inc. och dess EMEA-bolag)	Plattform för enhetshantering: inventering, uppdateringar, programdistribution, konfigurationshantering, synlighet	Datacenterregion inom EU/EES; supportåtkomst från länder utanför	Standardavtalsklausuler i Taniums Data Processing Addendum

Underbiträde	Tjänst / ändamål	Plats för behandlingen	Överföringsmekanism
	och åtgärder på slutpunkter samt, när det har beställts, Tanium Threat Response	EU/EES kan förekomma	
Keeper Security (Keeper Security, Inc. / Keeper Security EMEA)	Krypterad lagring av de inloggningsuppgifter som används för att administrera Kundens miljö (Keeper MSP) och, när det har beställts, privilegierad åtkomsthantering (KeeperPAM). Innehållet i valven krypteras på enheten och kan inte läsas av leverantören	EU-region (Irland eller Frankfurt)	EU–US Data Privacy Framework; standardavtalsklausuler i Keepers personuppgiftsbiträdesavtal

Gäller endast när Kunden har beställt modulen:

Underbiträde	Tjänst / ändamål	Gäller	Plats för behandlingen	Överföringsmekanism
Veeam Software (inklusive Veeam Backup for Microsoft 365)	Säkerhetskopiering och återställning av Microsoft 365-data, servrar, virtuella maskiner och slutpunkter	Kunder som har beställt säkerhetskopiering på Veeam-plattform	EU/EES	Standardavtalsklausuler i Veeams dataskyddsvillkor, i tillämpliga fall
Rubrik (inklusive Rubrik Microsoft 365 Protection)	Säkerhetskopiering för större miljöer, oföränderlig lagring och cyberåterställning	Kunder som har beställt säkerhetskopiering på Rubrik	EU/EES	Standardavtalsklausuler i Rubriks dataskyddsvillkor, i tillämpliga fall
Microsoft 365 Backup	Inbyggd säkerhetskopiering av Exchange Online, SharePoint Online och OneDrive	Kunder som har beställt Microsoft 365 Backup	EU/EES (Microsofts EU Data Boundary)	Som för Microsoft ovan
Leverantör av hanterad detektion och respons	Säkerhetsövervakning och respons utanför Nord Nodes supporttid	Kunder som har beställt MDR; leverantören anges i Beställningen och läggs till i förteckningen över underbiträden innan tjänsten startar	Anges när leverantören anlitas	Anges när leverantören anlitas

När ett Underbiträdes egna dataskyddsvillkor, certifieringar eller förteckning över underbiträden har betydelse för Kundens bedömning lämnar Nord Node dem på begäran (punkt 7.6).

Kundens egna Microsoft 365-, Azure- eller andra molnmiljöer tillhandahålls Kunden direkt av Leverantören enligt Kundens eget avtal med Leverantören (se punkt 3.3). Leverantören är därför inte Nord Nodes Underbiträde för den data som lagras i dessa miljöer. Detta gäller även Microsoft Defender, Microsoft Entra ID, Microsoft Intune, Microsoft Sentinel och Microsoft Purview när Kunden innehar licenserna, även om Nord Node administrerar dem.

Relaterade dokument

Dokument	Webbadress
Förteckning över underbiträden	https://www.nordnode.se/sv/dam/nordnode/legal/final/document/nordnode-underbitraden-sv.pdf