ANEXA III

FIȘĂ DE PRELUCRARE A DATELOR

Condiții speciale în temeiul Acordului General privind Prelucrarea Datelor

Articolul 28 din Regulamentul UE 2016/679 („RGPD”)

Între

Operatorul de date, astfel cum este identificat în Acord, reprezentat de reprezentantul său legal învestit cu puterile necesare,

și

Persoana împuternicită de operator, astfel cum este identificată în Acord, reprezentată de reprezentantul său legal învestit cu puterile necesare,

De asemenea, Operatorul și Împuternicitul pot fi denumiți împreună „Părțile” și individual „Partea”.

AVÂND ÎN VEDERE CĂ

I. Părțile au semnat Acordul General privind Prelucrarea Datelor cu Caracter Personal („Acordul”), care reglementează termenii și metodele prelucrării datelor cu caracter personal efectuate de Împuternicit în contextul furnizării Serviciilor care fac obiectul Contractului;
II. În temeiul Acordului menționat mai sus, prelucrarea datelor cu caracter personal aferentă furnizării unor Servicii specifice este reglementată prin Fișe de Prelucrare a Datelor, care definesc caracteristicile operaționale, categoriile de date prelucrate, scopurile, măsurile de securitate aplicate și eventuala implicare a Subîmputerniciților;
III. Prezenta Fișă de Prelucrare a Datelor detaliază elementele Serviciului în conformitate cu Acordul. Aceasta integrează și completează prevederile generale ale Acordului, constituind o parte integrantă și obligatorie între Părți;
IV. În cazul unui conflict între prevederile prezentei Fișe de Prelucrare a Datelor și cele ale Acordului, prevederile Acordului vor prevala, cu excepția cazului în care Fișa de Prelucrare a Datelor prevede în mod expres excepții convenite între Părți;
V. Pentru aspectele care nu sunt reglementate în mod expres în prezentul document, se aplică prevederile și definițiile din Acord și din Contract, care se consideră pe deplin încorporate prin trimitere.

Având în vedere toate cele de mai sus, Părțile prezintă, în tabelul următor, specificațiile prelucrării Datelor cu Caracter Personal aferente Serviciului, inclusiv informații privind scopurile, categoriile de date prelucrate, măsurile de securitate aplicate și orice alt detaliu relevant în sensul Acordului.

	DESCRIERE
SERVICIU	Servicii de Arhivare (LTA)
ENTITATEA PRESTATOARE	**Namirial S.p.A. (pentru serviciul de arhivare electronică furnizat în România în temeiul Legii nr. 135/2007, Entitatea Prestatoare este Namirial S.r.l., autorizată ca administrator de arhivă electronică)** Atunci când Entitatea Prestatoare nu coincide cu Furnizorul identificat în Oferta Comercială, aceasta acționează ca Subîmputernicit Intra-Grup în numele Furnizorului, operând în temeiul unor acorduri intra-grup preexistente între societățile Grupului Namirial, conforme cu articolul 28 din RGPD.
NATURA PRELUCRĂRII	Împuternicitul poate prelucra Datele cu Caracter Personal ale Clientului obținute în contextul furnizării activităților de asistență și întreținere, în limitele strict necesare pentru executarea serviciilor prevăzute în Contract, sub forma: colectării, înregistrării, organizării sau structurării,

	consultării, selectării, ștergerii sau distrugerii.
SCOPUL PRELUCRĂRII	Încheierea Contractului și prestarea serviciilor care fac obiectul Contractului.
MODALITATEA DE FURNIZARE	*SaaS (Shared/Private)*
CATEGORII DE PERSOANE VIZATE	• Clienți finali; • Utilizatori ai serviciilor; • Furnizori; • Angajați.
CATEGORII DE DATE CU CARACTER PERSONAL PRELUCRATE	Datele cu Caracter Personal prelucrate de Împuternicit în numele Operatorului aparțin următoarelor categorii. **DATE COMUNE ȘI CATEGORII SPECIALE DE DATE:** • Date de identificare (prenume, nume, data nașterii, locul nașterii, țara, sexul, codul fiscal/CNP, adresa de domiciliu, nume de utilizator); • Date de contact (e-mail, număr de telefon); • Date de navigare (adresă IP, date de jurnal); • Date financiare (informații de facturare); • Date privind apartenența la societate/organizație; • Alte date (inclusiv categorii speciale) prezente în documentele transmise spre arhivare. • Orice alte date cu caracter personal (atât comune, cât și speciale, conform articolelor 4 și 9 din Regulament) necesare pentru executarea serviciilor prevăzute în contract: • Pentru arhivarea PEC: datele conținute în mesajele de Poștă Electronică Certificată (PEC) încredințate Împuternicitului.
LOCUL DE STOCARE A DATELOR	Datele sunt stocate pe serverele Împuternicitului și/sau ale Subîmputerniciților, situate în Uniunea Europeană/SEE.
DURATA PRELUCRĂRII DATELOR CU CARACTER PERSONAL	Prelucrarea Datelor cu Caracter Personal pentru furnizarea Serviciilor va avea următoarea durată: întreaga durată a Contractului cu Operatorul; întreaga durată a Acordului cu Operatorul dacă, din orice motiv, este mai lungă decât durata Contractului. După expirarea perioadelor menționate mai sus, Împuternicitului îi este permisă păstrarea în continuare a Datelor cu Caracter Personal în măsura în care aceasta constituie respectarea unor obligații legale specifice sau a unor ordine ale Autorităților competente. Păstrarea Datelor cu Caracter Personal este, de asemenea, permisă exclusiv în măsura în care acestea sunt necesare Împuternicitului pentru a dovedi, a valorifica sau a-și apăra un drept, pentru o perioadă de maximum 10 ani.
MĂSURI DE SECURITATE	A se vedea Anexa III-A – MĂSURI TEHNICE ȘI ORGANIZATORICE DE SECURITATE
SUBÎMPUTERNICIȚI	Entitatea Prestatoare a Serviciului (identificată în rândul de mai sus) utilizează, pentru furnizarea Serviciului, alte societăți din Grupul Namirial și terți selectați care oferă

	garanții de confidențialitate a datelor. Lista actualizată este furnizată în Anexa III-B, împărțită în Tabelul A (societățile din Grupul Namirial implicate în furnizarea serviciului, care operează în temeiul unor acorduri intra-grup preexistente, conforme cu articolul 28 din RGPD și separate de prezentul Acord) și Tabelul B (Subîmputerniciți terți). Unii dintre acești terți pot opera și în afara Spațiului Economic European (SEE), inclusiv în Statele Unite. Pentru a asigura conformitatea cu RGPD (articolele 44-49) și cu reglementările privind protecția datelor cu caracter personal, Furnizorul poate utiliza mecanisme adecvate pentru transferul datelor. Aceste entități sunt selectate în conformitate cu prevederile Acordului, primesc instrucțiuni precise privind prelucrarea datelor și desfășoară numai activitățile necesare, cu respectarea directivelor furnizate. Lista actualizată a acestor entități este furnizată în Anexa III-B la prezentul document.

ANEXA III - A

MĂSURI TEHNICE ȘI ORGANIZATORICE DE SECURITATE

Măsurile de securitate descrise în prezenta Anexă se aplică în completarea celor prevăzute în Acord și constituie un nivel suplimentar de protecție pentru prelucrarea reglementată de Fișa de Prelucrare la care sunt anexate. Acestea sunt aplicate și aplicabile Entității Prestatoare a Serviciului menționate în Contract, care poate coincide sau nu cu Împuternicitul.

1. MĂSURI TEHNICE DE SECURITATE

TIPUL MĂSURII	DESCRIERE
Măsuri pentru asigurarea confidențialității, integrității, disponibilității și rezilienței permanente a sistemelor și serviciilor de prelucrare	Procesul de verificare a integrității pachetelor de informații și a documentelor în cadrul serviciului include: • Verificarea consistenței numărului de documente (respectiv compararea numărului de documente efectiv stocate în Sistemul de Arhivare cu numărul de înregistrări din structura bazei de date pentru un anumit Producător de Documente); • Verificarea validității instrumentelor de integritate aplicate documentelor și indexurilor pachetelor (respectiv verificarea semnăturii digitale și a mărcii temporale pe un procent selectat de documente și indexuri XML (IPdA) prezente în Sistemul de Arhivare pentru un anumit Producător de Documente). • În ceea ce privește verificările de lizibilitate, Sistemul de Arhivare StrongDox include mecanisme automatizate care, într-un interval de cinci ani, efectuează o serie de verificări pe bază de eșantion, utilizând un algoritm pseudoaleatoriu. Eșantionarea ia în considerare setul complet de ID-uri ale documentelor arhivate. Eșantionul selectat reprezintă o parte semnificativă statistic din toate documentele arhivate pentru fiecare Producător de Documente. • Asupra documentelor selectate se efectuează următoarele verificări: • Verificarea integrității, efectuată prin recalcularea automată a hash-ului documentului și compararea acestuia cu hash-ul stocat la momentul creării Pachetului de Arhivare. • După fiecare operațiune de control, se generează un Raport de Control semnat digital de Responsabilul Serviciului de Arhivare, stocat în Sistemul de Arhivare StrongDox. Eventualele proceduri suplimentare solicitate de Producătorul de Documente sunt descrise în Fișa Serviciului relevantă.
Măsuri pentru asigurarea capacității de restabilire la timp a disponibilității și accesului la datele cu caracter personal în cazul unui incident fizic sau tehnic	În faza de restabilire din Planul de Continuitate a Activității se desfășoară toate activitățile necesare pentru reconstruirea sistemului informatic și, dacă este necesar, pentru activarea stațiilor de lucru de urgență prin utilizarea unui sediu secundar. • Pentru a asigura o împărțire și o executare eficientă a sarcinilor, Grupul de Intervenție pentru Restabilirea Sistemului (GI-RS) este structurat pe medii, permițând o specializare mai mare și o împărțire mai precisă în subfaze. • Procesul este automatizat în cadrul sistemului și definit intern în Manualul de Arhivare.

Măsuri de protecție a datelor pe durata stocării	Serviciul de arhivare a documentelor conform legii (LTA) permite oricărei organizații să stocheze digital orice tip de document (de exemplu, administrative, contabile, contracte, informări etc.). **Serviciul a fost conceput și implementat cu respectarea deplină a Liniilor Directoare AgID privind crearea, gestionarea și conservarea documentelor digitale (adoptate în mai 2021) și a prevederilor aplicabile ale DPCM din 3 decembrie 2013, în vigoare din aprilie 2014. Pentru serviciul de arhivare furnizat în România de Namirial S.r.l., serviciul respectă, de asemenea, Legea nr. 135/2007 privind arhivarea documentelor în formă electronică și Normele tehnice aprobate prin Ordinul președintelui Autorității pentru Digitalizarea României (ADR) nr. 20.717/2024.** • Mai jos este prezentată o scurtă descriere a componentelor serviciului: • Application Front End • Core Service Layer (Web Services) • Bază de date, bazată pe NoSQL, pentru stocarea datelor • Data Repository, Object Storage prin protocolul S3.
Măsuri pentru asigurarea înregistrării evenimentelor	**Departamentele de Producție și de Dezvoltare Software ale Namirial sunt responsabile de infrastructură și sisteme și efectuează monitorizare online și verificări la nivel de aplicație/sistem prin indicatorii și controalele definite în Sistemul de Management al Securității Informației (ISMS).** • Namirial utilizează software și instrumente de gestionare a evenimentelor de securitate pentru a monitoriza securitatea și continuitatea operațională a componentelor esențiale ale sistemului de arhivare. • Acestea includ IBM QRadar, operat de Yarix S.p.A. (Montebelluna), care gestionează un Security Operations Center (SOC) 24/7, monitorizând sistemul pe tot parcursul anului. • În cazul unor incidente critice de securitate sau de continuitate, Yarix contactează cu promptitudine personalul desemnat al Namirial pentru atenuarea riscurilor. • Din punct de vedere operațional, Biroul de Arhivare Namirial utilizează ZenDesk pentru gestionarea solicitărilor de servicii de la Distribuitori și Clienți finali. Fiecare solicitare generează un tichet care este alocat și gestionat de echipă, care asigură suportul de prim nivel. Dacă este necesar suport de dezvoltare software, solicitarea este redirecționată către Jira Service Desk, gestionat de Echipa Cloud.
Măsuri pentru asigurarea configurării sistemului, inclusiv a configurării implicite	Sistemele de Arhivare sunt livrate prin servicii cloud, prin diverse configurații stocate în baza de date. Toate configurațiile sunt automatizate și centralizate în AWS System Manager și sunt moștenite la fiecare reîncărcare a sistemului.
Măsuri interne de gestionare și guvernanță IT și de securitate cibernetică	Sistemul este certificat în conformitate cu ISO/IEC 27001.

Măsuri pentru asigurarea păstrării limitate a datelor	În cazul unei solicitări de restituire a tuturor Pachetelor de Arhivare păstrate, Producătorul de Documente (Utilizatorul) poate solicita distribuirea din sistemul StrongDox, fie prin utilizarea filtrelor interfeței web, fie printr-o metodă WebService dedicată. Fiecare Pachet de Distribuire conține un Index al Pachetului de Distribuire (IPdD), generat conform UNI SInCRO 11386:2010 și semnat digital de Responsabilul Serviciului de Arhivare. Acest pachet servește drept raport oficial de distribuire și include un fișier XSLT pentru redarea corespunzătoare a IPdD.
Măsuri pentru asigurarea responsabilității	Modelul Organizațional de Gestionare a Urgențelor (MOGE) definește alocarea responsabilităților între diferitele roluri de business implicate în procesele și activitățile de gestionare a continuității activității.
Măsuri pentru a permite portabilitatea datelor și a asigura ștergerea	Structura primară de date care asigură interoperabilitatea pentru Serviciile de Arhivare Namirial este Pachetul de Arhivare, generat conform regulilor tehnice aplicabile Sistemelor de Arhivare și conform standardului UNI SInCRO 11386:2020.

ANEXA III - B

SUBÎMPUTERNICIȚI

Prezenta Anexă enumeră Subîmputerniciții aprobați la data semnării Fișei de Prelucrare a Datelor relevante, în temeiul Acordului.

Entitățile enumerate au fost selectate pe baza criteriilor de experiență, fiabilitate și a garanțiilor de conformitate cu reglementările aplicabile, în special cu prevederile articolului 28 din Regulamentul UE 2016/679.

Acestea operează sub autoritatea Împuternicitului, respectând instrucțiunile primite și adoptând măsuri de securitate adecvate pentru protecția Datelor cu Caracter Personal prelucrate.

Lista Subîmputerniciților poate fi actualizată în timp, în conformitate cu prevederile Acordului.

TABELUL A

SOCIETĂȚILE DIN GRUPUL NAMIRIAL IMPLICATE ÎN FURNIZAREA SERVICIULUI

DENUMIREA SOCIETĂȚII	ADRESA	LOCUL PRELUCRĂRII	DOMENIUL DE ACTIVITATE
Namirial SPA	Via Caduti sul Lavoro 4 – Senigallia (AN) Italy	SEE	Furnizor de servicii

TABELUL B

SUBÎMPUTERNICIȚI TERȚI

DENUMIREA SOCIETĂȚII	ADRESA	LOCUL PRELUCRĂRII	DOMENIUL DE ACTIVITATE
AWS EMEA SARL (alternativ, la alegerea Clientului)	Luxembourg, 38 Avenue John F. Kennedy L-1855	SEE	**Servicii cloud** (în conformitate cu prevederile Manualului Operațional, în funcție de zona geografică relevantă: https://static.namirial.com/docs/en/long-term-archiving-practice-statement.pdf, Secțiunea 8.3)
Outscale Sasu (alternativ, la alegerea Clientului)	1 rue Royale, 92210, Saint-Cloud, France	SEE	**Servicii cloud** (în conformitate cu prevederile Manualului Operațional, în funcție de zona geografică relevantă: https://static.namirial.com/docs/en/long-term-archiving-practice-statement.pdf, Secțiunea 8.3)
GTS TELECOM SRL (alternativ, la alegerea Clientului)	92-96 Izvor Street, 1st floor office A, and 2nd floor office A and B, 5thdistrict, Bucharest	SEE	**Servicii cloud** (în conformitate cu prevederile Manualului Operațional, în funcție de zona geografică relevantă: https://static.namirial.com/docs/en/long-term-archiving-practice-statement.pdf, Secțiunea 8.3)
Atlassian B.V.	Singel 236 1016 AB	SEE	Gestionarea tichetelor de suport

	Amsterdam, Netherlands		
Zendesk Inc.	989 Market St, San Francisco, CA 94103	SEE	Gestionarea tichetelor de suport
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Belgium	SEE	Sincronizarea tichetelor de suport
Var Group S.p.A. (Yarix)	Via della Piovola, 138 - 50053 Empoli FI	SEE	SOC (Security Operation Center) și MOC (Monitoring Operation Center)
MongoDB Limited	Building Two, Number One Ballsbridge, Dublin 4, Ireland	SEE	Servicii cloud
Dynatrace S.r.l.	Viale Enrico Forlanini, 23 20134 Milan, Italy	SEE	Monitorizarea jurnalelor