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	*Serviciu de distribuție electronică înregistrată certificată (SERC) și Serviciu calificat de distribuție electronică înregistrată certificată (SERCQ)*
ENTITATEA PRESTATOARE	**Uanataca SAU** 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 în contextul furnizării serviciului, în limitele strict necesare pentru executarea serviciilor prevăzute în Contract, sub forma: colectării, înregistrării, organizării sau structurării, consultării, prelucrării, selectării, extragerii, comparării, utilizării, comunicării, ștergerii sau distrugerii.

FIȘĂ DE PRELUCRARE A DATELOR

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.
CATEGORII DE DATE CU CARACTER PERSONAL PRELUCRATE	Datele cu Caracter Personal prelucrate de Împuternicit în numele Operatorului aparțin următoarelor categorii: **DATE COMUNE:** • **Date personale (nume, prenume, e-mail, data nașterii, locul nașterii, cetățenia, sexul, codul fiscal/CNP, adresa de reședință/domiciliu);** • **Date de contact (e-mail, număr de telefon);** • **Date de navigare (adresă IP);** • **Alte date posibile: date prezente în comunicările certificate.** **CATEGORII SPECIALE DE DATE CU CARACTER PERSONAL:** • **Alte date posibile: categorii speciale de date prezente în comunicările certificate.**
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: • Audituri interne periodice pentru a controla și verifica dacă starea Sistemului de Management al Securității Informației este adecvată și conformă cu legea; • Angajații sunt instruiți să înțeleagă fluxurile de comunicare și, fără autentificare prealabilă, nu vor avea acces la datele prelucrate; • Fluxurile de comunicare sunt protejate prin utilizarea rețelelor private virtuale (VPN). Astfel, conexiunile stabilite prin VPN vor proteja informațiile schimbate, acestea fiind criptate între cele două capete ale tunelului; • Pentru fiecare serviciu oferit se elaborează proceduri pentru a stabili întinderea și frecvența copiilor de siguranță criptate (AES256) ale datelor prelucrate, cu specificarea duratei de păstrare. În aceste cazuri se vor stabili numărul de copii necesare și durata de păstrare.
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 cazul unei încălcări a securității datelor, Uanataca dispune de un proces de gestionare a incidentelor IT care funcționează după cum urmează: • O echipă responsabilă, pe baza unei analize aprofundate a incidentelor IT anterioare, va elabora un plan de acțiune constând în măsuri preventive pentru limitarea repetării unor astfel de episoade; • La detectarea unui incident fizic sau tehnic, acesta va fi clasificat și încadrat în categoriile corespunzătoare, necesare pentru a determina gravitatea și prioritatea tratamentului care trebuie implementat; • Ulterior, prin procesul de notificare a incidentelor, vor fi evidențiate acțiunile imediate care trebuie întreprinse pentru a asigura capacitatea de restabilire promptă a disponibilității și a accesului la datele cu caracter personal afectate; • Uanataca prevede, de asemenea, întocmirea unui registru al incidentelor IT, în care este necesar să existe cât mai multe informații despre incident, respectiv: • Data și ora incidentului; • Tipul și gravitatea incidentului; Resursele afectate; Originile posibile; Starea incidentului; Acțiunile întreprinse pentru rezolvarea problemei; Cine a efectuat acțiunile de mai sus; Data și ora rezolvării și închiderii incidentului.

	În final, pentru rezolvarea incidentului IT, se întocmește un document explicativ al procedurii care trebuie implementată în cazul unei încălcări a securității datelor, luând în considerare diferitele scenarii posibile.
Măsuri de protecție a datelor pe durata stocării	Uanataca va monitoriza evoluția instrumentelor și mecanismelor existente de control al programelor malware (antimalware, antiphishing, antispam, analiza web și a e-mailurilor) pentru a îmbunătăți protecția activelor informaționale. **Monitorizarea va permite:** • efectuarea de analize automate și periodice pentru detectarea oricărui tip de malware; • efectuarea de verificări automate ale atașamentelor de e-mail și ale descărcărilor de pe web, întrucât acestea pot conține coduri malițioase; • blocarea accesului la anumite aplicații sau site-uri web pe baza politicii de confidențialitate, creând astfel „liste negre” de prevenție; • permiterea accesului la anumite aplicații sau site-uri web pe baza politicii de confidențialitate, creând astfel „liste albe”; • analizarea și detectarea eventualelor pagini web care pot conține amenințări ce ar putea pune în pericol datele prelucrate.
Măsuri pentru asigurarea înregistrării evenimentelor	**Pentru angajații și colaboratorii Uanataca este prevăzută o fază de înregistrare în care vor fi create conturi specifice cu domeniul uanataca.com.** • Aceste măsuri de înregistrare se aplică și conturilor cu acces direct la VPN-urile Uanataca pentru munca la distanță. • Uanataca s-a dotat cu software (Kibana + ElasticSearch) pentru gestionarea evenimentelor de securitate și monitorizarea utilizatorilor. Acest software este configurat în regim on-premise, direct pe serverele Uanataca. • Acest sistem de gestionare prevede că persoanele vizate își pot accesa conturile prin introducerea unei parole, care trebuie să îndeplinească anumite cerințe pentru a fi suficient de dificil de ghicit sau de descifrat. • Uanataca prevede, de asemenea, elaborarea de proceduri pentru asigurarea păstrării arhivelor centralizate, permițând accesul la acestea numai prin autentificare cu doi factori, constând în introducerea unei parole și a unui PIN. De asemenea, având în vedere că dispozitivele de acces pot aparține Uanataca sau angajatului ori colaboratorului, se disting mai multe tipuri de acces: acces simplu de lucrător, care va avea acces la informațiile conținute în arhive, e-mailuri, wiki-uri, pentru desfășurarea activității de muncă, inclusiv la distanță; acces de administrare, prin VPN, cu autentificare cu doi factori (parolă plus cheie privată RSA), pentru cei care dețin roluri administrative de nivel superior; în final, acces special. Acest tip de acces, care trebuie autorizat în prealabil, va fi acordat pentru realizarea unor activități specifice și limitate în timp.

Măsuri pentru asigurarea configurării sistemului, inclusiv a configurării implicite	Proiectele de dezvoltare vor fi gestionate prin REDMINE, un instrument integrat de gestionare a tichetelor, codului sursă și documentației (wiki). Este un software open-source, web-based, de management de proiect și urmărire a erorilor, descărcat și configurat direct pe serverele interne ale Uanataca. Codul sursă al aplicațiilor va fi menținut la zi prin depozite de gestionare a datelor (GIT). Autentificarea pentru accesul la depozite se va realiza prin introducerea numelui de utilizator și a parolei (deținute de fiecare utilizator care prelucrează date), prin canale de comunicare criptate. Fiecare proiect, atât REDMINE, cât și GIT, va avea roluri de acces diferite, cum ar fi: Administrator, Product Owner, dezvoltator. Modificările și iterațiile codului vor fi efectuate în ramuri independente în cadrul aceluiași manager de cod sursă.
Măsuri interne de gestionare și guvernanță IT și de securitate cibernetică	Uanataca dispune de un Comitet Tehnic de Securitate care va îndeplini următoarele funcții: pregătirea standardelor de securitate, în conformitate cu liniile directoare elaborate; pregătirea procedurilor de securitate, pentru implementarea controalelor derivate din standardele de mai sus și în conformitate cu Comitetul de Securitate; dezvoltarea și elaborarea procedurilor derivate din planurile operaționale de continuitate a activității. Sistemul respectă certificarea ISO/IEC 27001.
Măsuri pentru asigurarea păstrării limitate a datelor	Păstrarea informațiilor și a datelor este clasificată din perspectiva păstrării și ștergerii informațiilor deținute de Uanataca. Pentru respectarea acestei cerințe, se vor întocmi documente pentru fiecare țară, luând în considerare diferitele regimuri juridice care trebuie respectate, pentru a identifica următoarele termene: Perioada de păstrare: se referă la perioada minimă în care Uanataca trebuie să păstreze informațiile furnizate de utilizatori; Perioada maximă de ștergere: se referă la perioada maximă după care Uanataca trebuie să șteargă informațiile menționate. Această perioadă începe din momentul expirării perioadei de păstrare.
Măsuri pentru asigurarea responsabilității	Pentru a asigura securitatea datelor prelucrate, Uanataca va numi un Responsabil de Securitate cu următoarele funcții: 1. Pregătirea analizei de risc. 2. Centralizarea tuturor acțiunilor Sistemului de Management al Securității Informației (ISMS) al Uanataca. 3. Comunicarea Politicii de Securitate întregului personal și părților interesate. 4. Desfășurarea de instruiri privind ISMS și clasificarea informațiilor conform criteriilor de clasificare definite în reglementările corespunzătoare. 5. Coordonarea și monitorizarea acțiunilor desfășurate de Responsabilii de Risc. 6. Notificarea întregului personal care intră în Uanataca cu privire la obligațiile privind respectarea Politicii de

	Securitate și a cadrului său de reglementare. 7. Verificarea respectării Politicii de Securitate în gestionarea tuturor contractelor cu terții care intră în domeniul de aplicare al ISMS. 8. Organizarea, planificarea și desfășurarea auditurilor periodice ale ISMS. Uanataca va numi, de asemenea, Responsabili de Risc, care vor avea următoarele funcții: 1. vor fi responsabili de conducerea și controlul acțiunilor de îmbunătățire pentru minimizarea riscurilor; 2. vor controla acțiunile de minimizare a riscurilor, astfel încât să existe întotdeauna trasabilitatea acestora; 3. se vor coordona cu Responsabilul de Securitate pentru a raporta progresul lor în cadrul ISMS.
Măsuri pentru a permite portabilitatea datelor și a asigura ștergerea	Uanataca asigură ștergerea datelor prelucrate atunci când cerințele legale și contractuale nu mai sunt îndeplinite. Mai jos sunt prezentate câteva dintre cauzele care vor permite ștergerea informațiilor: 1. Încetarea condiției legitime a prelucrării, asociată cu încetarea raportului contractual care permite păstrarea acestor informații. 2. Expirarea termenului legal de păstrare a informațiilor și datelor prelucrate. Exercitarea drepturilor de către persoanele vizate. Persoanele vizate pot solicita în mod legitim ștergerea informațiilor lor personale deținute de Uanataca. Pentru această activitate se va lua în considerare legislația țării de origine a persoanei vizate. Pentru a răspunde acestor ipoteze, Uanataca a dezvoltat o procedură capabilă să asigure ștergerea datelor prin două metode diferite: 1. Informațiile pot fi distruse complet, dacă sunt în format hârtie, prin utilizarea de distrugătoare de documente sau prin servicii specializate de distrugere a informațiilor pe hârtie. 2. Informațiile digitale vor fi șterse din arhivele IT. Orice copii de siguranță care conțin copii ale acestor informații vor fi, de asemenea, șterse, astfel încât să nu poată fi reutilizate.

2. MĂSURI DE SECURITATE ORGANIZATORICE

TIPUL MĂSURII	DESCRIERE
Proceduri de testare, verificare și evaluare periodică a eficacității măsurilor tehnice și organizatorice pentru asigurarea securității prelucrării	Uanataca asigură autenticitatea și integritatea conținutului prin respectarea reglementărilor aplicabile privind semnătura electronică și prin aderarea la standardele internaționale. • Uanataca utilizează criptarea TLS pentru protocolul HTTPS în sistemele sale de comunicare, aplicând suite de criptare limitate, în care sunt permise numai protocoale considerate suficient de sigure pentru acces AES256 (TLS 1.2 sau superior). • Toți algoritmii utilizați de Uanataca pentru crearea și validarea semnăturilor digitale și electronice respectă

	„suita criptografică” ETSI TS 119 312. • Activitățile se desfășoară în cadrul controalelor aferente certificării ISO/IEC 27001.

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
Uanataca S.A.U.	Avenida Meridiana 350, piso 3 08027 Barcelona (Spania)	SEE/SUA	Furnizarea Serviciului SERCQ și SERC. Lista persoanelor împuternicite suplimentare poate fi consultată la următoarea adresă: https://www.evicertia.com/es/rgpd
Namirial Spa	Via Caduti sul Lavoro, 4 Senigallia (AN) 60019 - Italy	SEE	Servicii operaționale de grup: operațiuni tehnice locale, dezvoltare, suport, medii de testare, copii de siguranță, precum și servicii administrative, financiare, contabile și de suport corporativ.

TABELUL B

SUBÎMPUTERNICIȚI TERȚI

DENUMIREA SOCIETĂȚII	ADRESA	LOCUL PRELUCRĂRII	DOMENIUL DE ACTIVITATE
Atlassian Corporation	Amsterdam, Singel 236 1016 AB Amsterdam, Netherlands	SEE/SUA	Gestionarea tichetelor de suport
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)