POLITICA GENERALĂ PRIVIND PROTECŢIA DATELOR PERSONALE

1. INTRODUCERE

Această Politică privind prelucrarea şi protecţia datelor cu caracter personal (denumită în continuare "**Politica**") defineşte procedura de prelucrare şi protecţie a datelor cu caracter personal în S&T Romania S.R.L., societate cu răspundere limitată organizată și funcționând în conformitate cu prevederile din România, cu sediul în România, Bucureşti, Str. Gh. Polizu nr. 58-60, Bucharest Corporate Center, etajul 10 și etajul 11, sector 1, înregistrată la Registrul Comerţului Bucureşti sub nr. J40/1620/1994, CUI RO5175054 (denumită în continuare "**S&T Romania S.R.L.**" sau "**Operator**"), şi stabileşte procedurile care vizează prevenirea şi evidențierea oricăror încălcări ale legii aplicabile cu privire la datele cu caracter personal.

Această Politică a fost elaborată în conformitate cu legislaţia României şi a Uniunii Europene, în special cu următoarele documente:

- Regulamentul General de Protecţia Datelor (RGPD), adoptat de Parlamentul European şi de Consiliul European la 27 Aprilie 2016;
- Orice altă lege locală privind protecţia datelor cu caracter personal ce se aplică în România.

2. SCOPUL POLITICII DE PROTECŢIE A DATELOR

Scopurile principale ale Policitilor sunt:

- Stabilirea unei proceduri, precum şi a termenilor şi condiţiilor privind prelucrarea datelor cu caracter personal, inclusiv procedurile care vizează prevenirea încălcării legilor şi procedurilor de realizare a controlului intern în conformitate cu legislaţia aplicabilă privind datele cu caracter personal;
- Prezentarea personalului S&T Romania SRL responsabil cu prelucrarea datelor cu caracter personal a Politicii legii aplicabile cu privire la datele cu caracter personal şi a cerinţelor ASBISC privind prelucrarea datelor cu caracter personal;
- Stabilirea responsabilităţilor pentru personalul care prelucrează datele cu caracter personal în cazul nerespectării legii aplicabile privind datele cu caracter personal.
- Respectarea dreptului subiecţilor de a fi informaţi asupra modalităţii în care ASBISC prelucrează datele lor cu caracter personal.

Astfel, scopul acestei Politici este să explice care sunt datele cu caracter personal pe care le prelucrăm, de ce le prelucrăm, precum și ce facem cu acestea. Având in vedere faptul că informațiile personale aparțin fiecărui utilizator, facem tot posibilul să le stocăm în siguranță și să le prelucrăm cu atenție. Nu oferim informații unor părți terțe fără a ne îndeplini obligația prealabilă de informare.

3. DOMENIUL DE APLICARE SI MODIFICAREA POLITICII DE PROTECTIE A DATELOR

Această politică de protecție a datelor se aplică S&T România SRL și angajaților companiei. Politica privind protecția datelor se extinde la toate prelucrările de date cu caracter personal.

Această politică de protecție a datelor poate fi modificată doar sub coordonarea directa a Coordonatorului cu Protectia Datelor (DPC) din cadrul S&T România SRL, orice modificare fiind validata de catre Ofiterul de

Protectie a Datelor (DPO) desemnat la nivelul grupului S&T. Modificările vor fi raportate imediat la nivel de grup S&T utilizând procesul de modificare a politicilor.

Cea mai recentă versiune a politicii de protecție a datelor poate fi accesată cu informațiile privind confidențialitatea datelor pe site-ul S&T România: www.snt.ro

4. DEFINIŢII DE BAZĂ

În sensul prezentei Politici, se folosesc următoarele definiţii:

"Responsabil cu Protecţia Datelor (RPD)" înseamnă o persoană care este responsabilă cu monitorizarea aplicării RGPD şi a altor legi aplicabile privind protecţia persoanelor vizate de prelucrarea datelor cu caracter personal şi care exercită funcţiile care îi sunt atribuite de prezenta Politică şi de altă legislaţie aplicabilă, furnizează consultanţă managementului S&T Romania SRL şi comunică între societăţile din grupul S&T cu privire la protecţia datelor cu caracter personal.

"Date cu caracter personal" înseamnă orice informaţii privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale ale acelei persoane;

"Prelucrare" înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea

"Restricţionarea prelucrării" înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

"Creare de Profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

"Operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal. In sensul prezentei Politici, prin operator de înţelege S&T Romania SRL;

"Persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

"Destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă;

"Parte terţă" înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

"Consimţământ" al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

"Încălcarea securităţii datelor cu caracter personal" înseamnă o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

"Date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

"Prelucrarea transfrontalieră" înseamnă fie prelucrarea datelor cu caracter personal care are loc în contextul activităţilor sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puţin două state membre; sau fie prelucrarea datelor cu caracter personal care are loc în contextul activităţilor unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puţin două state membre.

5. PRINCIPII DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

a. Corectitudinea și legalitatea

S&T România SRL protejeaza drepturile individuale ale persoanelor fizice ("Persoana vizata") cu ocazia prelucrarii datelor cu caracter personal, datele cu caracter personal fiind colectate și prelucrate în mod legal și corect.

"Legalitatea" – presupune identificarea bazei legale înainte de prelucrarea datelor cu caracter personal. Acestea sunt denumite adesea „condițiile de prelucrare", de exemplu, consimțământul.

"Corectitudinea" – pentru ca prelucrarea datelor să fie corectă, operatorul de date trebuie să facă anumite informații disponibile pentru Persoanele vizate. Aceasta se aplică indiferent dacă datele cu caracter personal au fost obținute direct de la persoanele vizate sau din alte surse.

b. Restricţii la un anumit scop („limitări legate de scop")

Datele cu caracter personal sunt prelucrate numai în scopul definit înainte de inceperea colectarii Datelor. Modificările ulterioare ale scopului sunt posibile doar cu titlu exceptional, într-o măsură limitată și necesită o fundamentare.

c. Transparenta

Persoana vizată este informată cu privire la modul în care sunt prelucrate datele sale. În general, datele cu caracter personal sunt colectate direct de la persoana în cauză. Atunci când datele sunt colectate, Persoana vizată trebuie să fie conștientă sau să fie informată despre:

- Identitatea Operatorului de Date,
- Scopul prelucrării datelor,
- Terțe părți sau categorii de terțe părți cărora le-ar putea fi transmise datele.

d. Reducerea prelucrarii datelor și economia colectarii datelor („reducerea la minimum a datelor”);

Înainte de prelucrarea datelor cu caracter personal, trebuie determinat dacă și în ce măsură prelucrarea datelor cu caracter personal este necesară pentru atingerea scopului pentru care este efectuată. Atunci când scopul permite acest lucru și unde cheltuielile implicate sunt proporționale cu scopul urmărit, sunt utilizate date anonime sau statistice. Datele cu caracter personal nu sunt colectate în avans și stocate în scopuri potențiale viitoare, cu excepția cazului în care acest lucru este impus sau permis de legislația in vigoare.

e. Ștergerea

Datele personale care nu mai sunt necesare după expirarea perioadelor legate de procesele legale sau de afaceri sunt șterse. În cazul în care sunt identificate indicii cu privire la existenta unor interese care necesită protejarea sau legate de importanța istorică a acestor date în cazuri individuale, este posibil ca S&T România sa păstreze datele până când interesele care merită protejate au fost clarificate în mod legal, sau arhiva corporativă a evaluat datele pentru a determina dacă trebuie păstrate în scopuri istorice/ arhivistice. Atunci cand stergerea datelor poate avea impact asupra sistemelor informatice ale S&T Romania, datele vor fi anonimizate ireversibil, astfel incat sa nu mai existe indicii care sa poata conduce la identificarea persoanei vizate.

f. Precizia faptică; actualizarea datelor („exactitate”)

Datele cu caracter personal trebuie să fie corecte, complete și, dacă este necesar, să fie actualizate. S&T Romania SRL ia măsuri adecvate pentru a se asigura că datele eronate sau incomplete sunt șterse, corectate, completate sau actualizate.

g. Confidențialitatea și securitatea datelor („integritate și confidențialitate”).

Datele cu caracter personal sunt supuse obligatiilor legale de pastrare a secretului datelor. Acestea trebuie să fie tratate ca fiind confidențiale de fiecare angajat al S&T Romania SRL și sunt asigurate măsuri organizatorice și tehnice adecvate pentru a preveni accesul neautorizat, prelucrarea sau distribuția ilegală, precum și pierderea accidentală, modificarea sau distrugerea.

h. Principiul răspunderii conform GDPR

GDPR include prevederi care promovează răspunderea și guvernanța. Acestea completează cerințele de transparență ale GDPR. Principiul răspunderii din Articolul 5 (2) din GDPR vă solicită să demonstrați că respectați principiile și specifică explicit că aceasta este responsabilitatea dvs.

S&T ROMANIA va dovedi conformitatea cu principiile de protecția datelor prin implementarea politicilor de protecția datelor, respectarea codurilor de conduită, implementarea unor măsuri tehnice și organizaționale, precum și adoptarea unor tehnici precum protecția datelor prin design, DPIAs, procedura de notificare a încălcării și planuri de răspuns la incidente.

4. TEMEIURILE PRELUCRARII DATELOR

Colectarea, prelucrarea și utilizarea datelor cu caracter personal este permisă numai în temeiurile enumerate mai jos:

a. Date despre clienti si parteneri

a.1. Prelucrarea datelor pentru executarea unui contract

Datele personale ale persoanelor de contact si reprezentantilor clienților, furnizorilor și partenerilor pot fi procesate pentru a stabili, executa și inceta un contract. Înainte desemnarea contractului - în timpul fazei de inițiere a contractului - datele personale pot fi prelucrate pentru a pregăti ofertele sau comenzile de cumpărare sau pentru a îndeplini alte cerințe din perspectiva care se referă la încheierea contractului. Persoanele de contact pot fi contactate în timpul procesului de pregătire a contractului, utilizând doar informațiile pe care acestea le-au furnizat pentru contactare. Orice restricții solicitate de persoanele de contact respective trebuie să fie respectate.

a.2 Consimțământul ca temei al prelucrarii datelor

Atunci cand este necesar consimtamantul persoanelor vizate, Datele pot fi prelucrate după primirea acordului persoanei vizate. Consimtamantul trebuie obținut în scris sau în format electronic în scopul documentării. În anumite circumstanțe, cum ar fi conversațiile telefonice, consimțământul poate fi dat verbal. Este obligatorie documentarea acordarii consimțământului.

a.3. Prelucrarea datelor în conformitate cu obligatia legală

Prelucrarea datelor cu caracter personal este permisă și în cazul în care legislația aplicabila solicită, impune sau permite acest lucru. Tipul și amploarea procesării datelor trebuie să fie necesare pentru activitatea legală de prelucrare a datelor și trebuie să respecte dispozițiile legale relevante.

a.4. Prelucrarea datelor în conformitate cu interesele legitime

Datele cu caracter personal pot fi procesate și în cazul în care acest lucru este necesar pentru un interes legitim al S&T România SRL. Interesele legitime sunt în general de natură juridică (de exemplu, colectarea creanțelor restante) sau comerciale (de exemplu, evitarea încălcărilor contractului). Datele cu caracter personal nu pot fi prelucrate în scopul unui interes legitim dacă, în cazuri individuale, există dovezi conform cărora interesele persoanei vizate merită protecție și că aceasta are prioritate. Înainte de prelucrarea datelor, este necesar să se determine dacă există interese care merită protejate.

a.5. Prelucrarea datelor sensibile

S&T Romania SRL nu prelucrează nicio informaţie referitoare la rasă, naţiune, opinii politice, credinţe religioase sau filosofice, intimitate, viaţă privată.

Datele cu caracter personale sensibile pot fi prelucrate numai dacă legea impune acest lucru sau dacă persoana vizată și-a dat consimțământul în mod expres. Aceste date pot fi, de asemenea, prelucrate dacă o asemenea prelucrare este obligatorie pentru recunoașterea, exercitarea sau apărarea drepturilor legale referitoare la persoana vizată. Dacă în cadrul S&T există planuri de prelucrare a datelor extrem de sensibile, DPO si Coordonatorul cu Protectia Datelor (DPC) trebuie informati în prealabil.

Dacă datele cu caracter personal sunt colectate, prelucrate și utilizate pe site-uri web sau în aplicații, persoanele vizate trebuie să fie informate despre aceasta printr-o declarație de confidențialitate și, dacă este cazul, să i se pună la dispoziție informații despre cookie-uri. Declarația de confidențialitate și orice informație privind

modulele cookie trebuie să fie integrate astfel încât să fie ușor de identificat, direct accesibile și disponibile în mod consecvent pentru persoanele vizate.

b. Datele angajatului/viitorilor angajati

b.1. Prelucrarea datelor pentru relația de muncă

În relațiile de muncă, datele cu caracter personal pot fi prelucrate, dacă este necesar, pentru inițierea, executarea și încetarea contractului de muncă. La inițierea unui raport de muncă, datele personale ale solicitanților vor fi procesate. În cazul în care candidatul este respins, datele sale trebuie șterse în conformitate cu perioada de păstrare necesară, cu excepția cazului în care solicitantul a fost de acord să rămână la dosar pentru un viitor proces de selecție pentru o perioadă de 12 luni de la data aplicării. De asemenea, este necesar consimțământul pentru utilizarea datelor pentru procesele de aplicare suplimentare sau înainte de partajarea aplicației cu alte companii din grup.

În raportul de muncă existent, prelucrarea datelor trebuie să se refere întotdeauna la scopul contractului de muncă dacă nu se aplică niciuna dintre următoarele circumstanțe pentru prelucrarea datelor autorizate.

Dacă în timpul procedurii de solicitare ar trebui să fie necesară colectarea de informații despre un solicitant de la o terță parte, trebuie respectate cerințele legilor naționale corespunzătoare. În caz de îndoială, trebuie obținut un acord de la persoana vizată.

Trebuie să existe o autorizație legală pentru prelucrarea datelor cu caracter personal care au legătură cu relația de muncă, dar care nu a făcut parte inițial din executarea contractului de muncă. Acestea pot include cerințe legale, reglementări colective cu reprezentanții angajaților, consimțământul angajatului sau interesul legitim al companiei.

b.2. Prelucrarea datelor în conformitate cu obligatia legală

Prelucrarea datelor personale ale angajaților este permisă și în cazul în care legislația națională solicita si impune acest lucru. Tipul și amploarea procesării datelor trebuie să fie necesare pentru activitatea legală de prelucrare a datelor și trebuie să respecte dispozițiile legale relevante. Dacă există o anumită flexibilitate juridică, trebuie luate în considerare interesele angajatului care merită protejate.

b.3. Consimțământul la prelucrarea datelor

Acolo unde este necesar, Datele angajatului pot fi prelucrate după consimțământul persoanei în cauză. Declarațiile de consimțământ trebuie prezentate în mod voluntar. Acordul involuntar este nul. Declarația de consințământ trebuie obținută în scris sau în format electronic și va fi păstrată de operator. În anumite circumstanțe, consimțământul poate fi dat verbal, caz în care trebuie să fie documentat ulterior corespunzător. În cazul furnizării informate și voluntare de date de către partea relevantă, se poate presupune existența unui acord, dacă legislația națională nu solicită consimțământul expres.

Prin „consimțământ" se intelege ca persoana vizata si-a dat acordul pentru prelucrarea datelor cu caracter personal cu privire la propria persoana. Persoana vizată își poate retrage consimțământul în orice moment prin trimiterea unui email la: privacy@snt.ro;

b.4. Prelucrarea datelor în baza unui interes legitim

Datele personale pot fi procesate și în cazul în care este necesar să se impună un interes legitim al S&T România SRL. Interesele legitime sunt în general de natură juridică (*de exemplu, depunerea, aplicarea sau apărarea împotriva unor actiuni legale*) sau financiare (*de exemplu, evaluarea întreprinderilor*).

Datele cu caracter personal nu pot fi prelucrate pe baza unui interes legitim dacă, în cazuri individuale, există dovezi că interesele angajatului merită protecție. Înainte de procesarea datelor, trebuie să se determine dacă există interese care merită protejate.

Măsurile de control care necesită prelucrarea datelor angajatului pot fi luate numai dacă există o obligație legală in acest sens sau dacă există un motiv legitim. Chiar dacă există un motiv legitim, trebuie examinată și proporționalitatea măsurii de control. Interesele justificate ale S&T Romania SRL (de exemplu, respectarea dispozițiilor legale și a reglementarilor interne ale societății) trebuie să fie cântărite in raport cu interesele angajatului care trebuie protejate si care pot fi afectate de măsura de control ce urmeaza a fi adoptata. Interesul legitim al companiei și orice interese ale angajatului care merită protejat trebuie să fie identificate și documentate înainte de luarea oricăror măsuri. În plus, trebuie luate în considerare orice cerințe suplimentare din legislația națională (de exemplu, drepturile de co-decizie pentru reprezentanții angajaților și drepturile de informare ale persoanelor vizate).

b.5. Prelucrarea datelor personale sensibile

Datele personale sensibile pot fi procesate numai în anumite condiții. Datele personale sensibile sunt date despre originea rasială și etnică, convingerile politice, convingerile religioase sau filozofice, calitatea de membru al unei uniuni/formatiuni și sănătatea și viața sexuală a persoanei vizate. În conformitate cu legislația națională, alte categorii de date pot fi considerate sensibile sau conținutul categoriilor de date poate fi completat diferit. Mai mult, datele care se referă la o infracțiune pot fi procesate numai în conformitate cu cerințele speciale din legislația națională.

Prelucrarea trebuie permisă în mod expres sau prescrisă de legislația națională. În plus, prelucrarea poate fi permisă dacă este necesar ca autoritatea responsabilă să își îndeplinească drepturile și obligațiile în domeniul dreptului muncii. Angajatul poate, de asemenea, să consimtă în mod expres prelucrarea.
Dacă există planuri de prelucrare a datelor personale sensibile, Coordonatorul cu Protectia Datelor (DPC) trebuie informat în prealabil.

b.6. Telecomunicații și internet

Echipamentele telefonice, adresele de e-mail, intranetul și internetul împreună cu rețelele sociale interne sunt furnizate de companie în primul rând pentru misiuni legate de muncă. Ele sunt un instrument și o resursă a

companiei. Acestea pot fi utilizate în cadrul reglementărilor legale aplicabile și al politicilor interne ale companiei. În cazul utilizării autorizate în scopuri personale, legile privind secretul telecomunicațiilor și legile naționale privind telecomunicațiile trebuie să fie respectate, dacă este cazul.

Pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor, S&T Romania poate implementa măsuri de protecție automate, inclusiv analiza traficului, în vederea detectării vectorilor sau modelelor de atac și prevenirii acestora, ca și în cazul răspunsului la incidentele de securitate informatică.

Pentru asigurarea unui grad ridicat al securității informatice și în vederea soluționării incidentelor de securitate informatică, utilizarea echipamentelor telefonice, a adreselor de e-mail, a rețelelor intranet / internet și a rețelelor sociale interne poate fi înregistrată pentru o perioadă temporară.
Evaluările acestor date si identificarea/profilarea unei anumite persoane poate fi făcuta doar într-un caz concret și justificat de încălcări suspectate a legilor in vigoare sau politicilor S&T România. Evaluările pot fi efectuate numai de către departamentele de investigare, asigurându-se, în același timp, respectarea principiului proporționalității.

S&T Romania nu va prelucra date cu caracter personal în absența unuia dintre motivele de mai sus. Aceeași regulă se aplică, de asemenea, în cazul în care scopul colectării, prelucrării și utilizării datelor cu caracter personal trebuie să fie modificat față de scopul inițial.

S&T Romania SRL nu foloseşte 'cookie'-uri pe site-ul său (*un „cookie" reprezinta o cantitate mică de date care include adesea un identificator unic care este trimis pe browser-ul calculatorului de pe server unui site internet şi este stocat pe hard disk-ul unui utilizator. Permite unui site internet să-şi amintească lucruri cum ar fi preferinţele utilizatorului, sau ce se găseşte în coşul de cumpărături al utilizatorului*).

5. TRANSMITEREA DATELOR CU CARACTER PERSONAL

Transmiterea datelor cu caracter personal către destinatarii din afara sau în interiorul S&T România SRL face obiectul cerințelor de autorizare pentru prelucrarea datelor cu caracter personal în conformitate cu secțiunea 5. Beneficiarul datelor trebuie să fie obligat să utilizeze datele numai în scopurile definite.

În cazul în care datele sunt transmise unui destinatar din afara S&T România SRL către o țară terță, această țară trebuie să accepte să mențină un nivel de protecție a datelor echivalent cu această politică de protecție a datelor. Acest lucru nu se aplică în cazul în care transmiterea se bazează pe o obligație legală. O obligație legală de acest tip se poate baza pe legile țării domiciliate a societății Grupului care transmite datele. În subsidiar, legile țării domiciliate a societății din grup pot recunoaște scopul transmiterii datelor în baza obligației legale a unei țări terțe.

În cazul în care datele sunt transmise de o terță parte S&T România SRL, trebuie să se asigure că datele pot fi utilizate în scopul dorit.
Dacă datele cu caracter personal sunt transferate de la o companie a Grupului cu sediul social în Uniunea Europeană / Spațiul Economic European către o societate a Grupului cu sediul social în afara Spațiului Economic

European (țara terță), societatea care importă datele este obligată să coopereze cu orice anchetă făcută de autoritatea de supraveghere competentă din țara în care își are sediul social partea care exportă datele și de a se conforma observațiilor autorității de supraveghere cu privire la prelucrarea datelor transmise. Același lucru este valabil și pentru transmiterea datelor de către companiile din grupuri din alte țări. Dacă fac parte dintr-un sistem internațional de certificare pentru respectarea regulilor corporative obligatorii privind protecția datelor, acestea trebuie să asigure cooperarea cu birourile și agențiile de audit relevante. Participarea la astfel de sisteme de certificare trebuie să fie convenită cu responsabilul cu protecția datelor.

În cazul în care un subiect de date pretinde că această politică de protecție a datelor a fost încălcată de societatea din Grup care se află într-o țară terță care importa datele, compania Grupului cu sediul în Spațiul Economic European care exportă datele se angajează să sprijine partea în cauză, ale căror date au fost colectate în Spațiul Economic European, pentru a stabili faptele și pentru a-și afirma drepturile în conformitate cu această politică împotriva societății de grup care importă datele.

6. PRELUCRAREA DATELOR PRIVIND CONTRACTELE

Prelucrarea datelor în numele său înseamnă că un furnizor este angajat să proceseze date cu caracter personal, fără a-și asuma responsabilitatea pentru procesul de afaceri afiliat. În aceste cazuri, un acord privind prelucrarea datelor în numele acestuia trebuie încheiat cu furnizori externi și S&T România. Clientul își păstrează întreaga responsabilitate pentru performanța corectă a procesării datelor. Furnizorul poate procesa date personale numai conform instrucțiunilor clientului. La emiterea ordinului, departamentul care plasează comanda trebuie să se asigure că sunt îndeplinite următoarele cerințe:

a) Furnizorul trebuie ales pe baza capacității sale de a acoperi măsurile tehnice și organizatorice de protecție necesare.
b) Ordinul trebuie trimis în scris. Instrucțiunile privind prelucrarea datelor și responsabilitățile clientului și furnizorului trebuie să fie documentate.
c) Trebuie luate în considerare standardele contractuale privind protecția datelor furnizate de responsabilul cu protecția datelor.
d) Înainte de începerea prelucrării datelor, clientul trebuie să aibă încredere că furnizorul își va respecta obligațiile. Un furnizor poate documenta conformitatea cu cerințele de securitate a datelor, în special prin prezentarea unei certificări adecvate.În funcție de riscul de prelucrare a datelor, revizuirile trebuie repetate în mod regulat pe durata contractului.
e) În cazul procesării transfrontaliere a datelor din contracte, trebuie îndeplinite cerințele naționale relevante pentru divulgarea datelor cu caracter personal în străinătate. În special, datele cu caracter personal din Spațiul Economic European pot fi procesate într-o țară terță numai dacă furnizorul poate dovedi că are un standard de protecție a datelor echivalent cu această politică de protecție a datelor. Instrumentele adecvate pot fi:
    i. Acordul privind clauzele contractuale standard ale UE pentru prelucrarea datelor din contracte în țările terțe cu furnizorul și cu orice subcontractanți.
    ii. Participarea furnizorului la un sistem de certificare acreditat de UE pentru asigurarea unui nivel suficient de protecție a datelor.

iii. Recunoașterea regulilor corporative obligatorii ale furnizorului pentru a crea un nivel adecvat de protecție a datelor de către autoritățile de supraveghere responsabile pentru protecția datelor.

7. DREPTURILE PERSOANEI VIZATE

Persoana vizată ale cărui date cu caracter personal sunt prelucrate de S&T Romania SRL au următoarele drepturi:

- ✓ **Dreptul de a fi informat** – să obţină de la S&T Romania SRL următoarele informaţii:
  - i. identitatea şi datele de contact ale S&T Romania SRL, ale reprezentanţilor, şi ale responsabilului cu protecţia datelor;
  - ii. scopurile şi temeiul juridic al prelucrării datelor cu caracter personal, interesele legitime ale S&T Romania SRL;
  - iii. categoriile de date cu caracter personal;
  - iv. destinatarii datelor cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale (dacă există) şi referirea la garanţiile şi mijloacele corespunzătoare;
  - v. perioada de stocare a datelor cu caracter personal şi criteriile folosite pentru a determina acea perioadă, sub rezerva că S&T Romania SRL păstrează şi prelucrează datele cu caracter personal atâta timp cât legile şi reglementările legale impun acest lucru. Prelucrarea datelor cu caracter personal încetează imediat daca nu mai există niciun motiv pentru o astfel de prelucrare;
  - vi. din ce sursă provin datele cu caracter personal (în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată);
- ✓ dacă furnizarea de date cu caracter personal este o cerinţă legală sau contractuală, sau o cerinţă necesară pentru a încheia un contract, precum şi dacă persoana vizată este obligată să furnizeze date cu caracter personal şi a posibilelor consecinţe ale neîndeplinirii de furnizare a acestor date.
- ✓ **Dreptul de acces la datele cu caracter personal** - să obţină de la S&T Romania SRL confirmarea dacă datele cu caracter personal sunt prelucrate sau şi dreptul de a primi o copie a oricărei înregistrări care conţine datele sale cu caracter personal;
- ✓ **Dreptul la rectificare** - să obţină de la S&T Romania SRL fără întârzieri nejustificate rectificarea unor date cu caracter personal inexacte cu privire la el/ea, completarea datelor cu caracter personal incomplete, inclusiv prin furnizarea unei declaraţii suplimentare;
- ✓ **Dreptul la ştergerea datelor ("dreptul de a fi uitat")** - să obţină de la S&T Romania SRL ştergerea datelor cu caracter personal fără întârzieri nejustificate (dacă datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate; persoana vizată îşi retrage consimţământul; datele cu caracter personal au fost prelucrare ilegal etc.);
- ✓ **Dreptul la restricţionarea** prelucrării dacă datele cu caracter personal sunt inexacte; prelucrarea este ilegală şi persoana vizată solicită restricţionarea utilizării datelor cu caracter personal în locul ştergerii

lor; datele cu caracter personal nu mai sunt necesare în scopul prelucrării, dar ele sunt solicitate pentru constatarea, exercitarea sau apărarea unui drept în instanţă; persoana vizată s-a opus prelucrării pentru intervalul de timp când se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate;

- ✓ **Dreptul la portabilitatea datelor** – să primească datele cu caracter personal într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date cu caracter personal unui alt operator fără obstacole din partea S&T Romania SRL (dacă prelucrarea se bazează pe consimţământ sau pe un contract, iar prelucrarea este efectuată prin mijloace automate);
- ✓ **Dreptul la opoziţie** în orice moment al prelucrării datelor cu caracter personal (inclusiv crearea de profiluri pe baza respectivelor dispoziţii şi au fost date cu caracter personal prelucrate în scopuri de marketing direct);
- ✓ **Dreptul la retragerea consimţământului** în orice moment, fără a afecta legalitatea prelucrării bazate pe consimţământ, înainte de retragerea sa. Astfel persoana vizată înţelege şi este de acord că, în cazul retragerii, nu se poate ajunge la scopul prelucrării datelor cu caracter personal;
- ✓ **Dreptul de a depune o plângere la o autoritate de supraveghere**, Biroul Comisarului pentru protecţia Datelor cu Caracter Personal, în cazul în care persoana vizată decide că drepturile sale sunt încălcate;
- ✓ **Dreptul la o cale de atac eficientă** împotriva unei autorităţi de supraveghere, S&T Romania SRL sau alt procesator;
- ✓ **Dreptul la despăgubiri** de la S&T Romania SRL sau de la un alt procesator pentru prejudiciul suferit.

8. CONFIDENŢIALITATEA PROCESĂRII

Datele personale sunt considerate infromatii confidentiale si vor fi tratate ca atare. Orice colectare, prelucrare sau utilizare neautorizată a acestor date de către angajați este interzisă. Prelucrarea datelor cu caracter personal este confidenţială. Ea va fi efectuată numai de persoanele care acţionează sub autoritatea S&T Romania SRL şi numai pe baza instrucţiunilor acesteia.

Orice procesare de date efectuată de un angajat, care nu a fost autorizată să fie desfasurata ca parte a îndatoririlor sale legitime, este considerate ca fiind neautorizată. Se aplică principiul *"necesitatea de a cunoaște"*. Angajații pot avea acces la informații personale in functie de adecvarea acestui acces la tipurile de date si de scopul determinat. Acest lucru se bazeaza pe defalcarea și separarea atentă a atributiilor angajatilor S&T Romania și presupune punerea în aplicare a rolurilor și responsabilităților pentru fiecare angajat.

Angajaților li se interzice să utilizeze date cu caracter personal în scopuri private sau comerciale, să le dezvăluie persoanelor neautorizate sau să le pună la dispoziție în orice alt mod. Superiorii ierarhici își informează angajații la începutul relației de muncă cu privire la obligația de a proteja secretul datelor.

In cazul utilizarii neautorizate a datelor personale, angajatii pot fi sanctionati in conformitate cu legislatia aplicabila si cu reglementarile in vigoare in cadrul S&T România.

Obligația mentinerii confidentialitatii datelor personale rămâne în vigoare și după încheierea perioadei de angajare, sanctiunile aplicabile in caz de incalcare a obligtiei de confidentialitate fiind cele prevazute de cadrul legislativ in vigoare.

9. SECURITATEA PRELUCRĂRII

Datele personale sunt protejate împotriva accesului neautorizat și împotriva prelucrării sau divulgării ilegale, precum și pierderii accidentale, modificării sau distrugerii. Acest lucru se aplică indiferent dacă datele sunt prelucrate electronic, pe suport de hârtie sau prin alte mijloace. Înainte de introducerea noilor metode de prelucrare a datelor, în special a noilor sisteme informatice, sunt definite și implementate măsuri tehnice și organizatorice de protecție a datelor cu caracter personal. Aceste măsuri trebuie să se bazeze pe stadiul tehnicii, pe riscurile procesării și pe necesitatea de a proteja datele (determinate de procesul de clasificare a informațiilor).

În special, structura organizatorică responsabilă se poate consulta cu Ofiterul de Securitate a Informatiei și cu responsabilul pentru protecția datelor. Măsurile tehnice și organizatorice pentru protecția datelor personale fac parte din managementul securității informațiilor corporative și sunt adaptate în mod continuu la evoluțiile tehnice și schimbările organizaționale.

Accesul la datele cu caracter personal este oferit numai acelor angajaţi ai S&T Romania SRL care au nevoie de astfel de date cu caracter personal pentru a-şi îndeplini sarcinile legate de oricare dintre scopurile prelucrării menţionate mai sus (inclusiv departamentul resurse umane, departamentul Juridic, departamentul Financiar, IT, Administrativ). Orice acces la datele cu caracter personal pentru alţi angajaţi care nu au drepturi de accesare în conformitate cu prezenta Politică este interzis.

Angajaţii S&T Romania SRL care au acces la datele cu caracter personal au dreptul să prelucreze numai acele date de care au nevoie pentru a-şi îndeplini responsabilităţile specifice de muncă legate de oricare dintre scopurile de prelucrare menţionate mai sus.

Documentele care conţin date cu caracter personal sunt stocate în departamentele structurale ale S&T Romania SRL ai căror angajaţi au acces la datele cu caracter personal legat de îndeplinirea atribuţiilor lor oficiale şi sunt responsabili de interacţiunea datele relevante ale persoanei vizate.

O persoană care prelucrează date cu caracter personal în numele S&T Romania SRL respectă principiile şi regulile de prelucrare a datelor cu caracter personal stabilite prin prezenta Politica.

Dacă S&T Romania SRL autorizează o altă persoană cu prelucrarea datelor cu caracter personal, S&T Romania SRL este responsabilă faţă de persoana vizată de prelucrarea datelor cu caracter personal pentru faptele sau omisiunile acelei persoane. O persoană care prelucrează date cu caracter personal în numele S&T Romania SRL este responsabilă faţă de S&T Romania SRL.

Toate datele cu caracter personal trebuie să fie tratate cu cea mai înaltă securitate și trebuie păstrate:
într-o cameră închisă cu cheia cu acces controlat; și/sau

- într-un sertar sau dulap închis cu cheia; și/sau

- dacă sunt computerizate, parola protejată conform cerințelor din politica de control al accesului; și/sau
- stocate în medii de calculator (detașabile) care sunt criptate în conformitate standardele in domeniu;

10. CONTROLUL PROTECTIEI DATELOR

Respectarea politicii de protecție a datelor și a legilor aplicabile privind protecția datelor este verificată în mod regulat prin intermediul auditurilor de protecție a datelor precum și al altor controale. Realizarea acestor controale este responsabilitatea responsabilului cu protecția datelor, a coordonatorilor de protecție a datelor și a altor unități ale grupului cu drepturi de audit sau a auditorilor externi angajați.

Rezultatele controalelor privind protecția datelor sunt raportate responsabilului cu protecția datelor. Managementul S&T România SRL este informat despre rezultatele primare ca parte a sarcinilor de raportare ale responsabilului cu protectia datelor cu caracter personal. La cerere, rezultatele controalelor privind protecția datelor vor fi puse la dispoziția autorității responsabile de protecția datelor. Autoritatea responsabilă cu protecția datelor poate efectua propriile controale de conformitate cu reglementările din această politică, conform legislației naționale.

Ca o completare a celor expuse mai sus, S&T ROMANIA SRL detine o certificare a Sistemului de Management al Securității Informației conform standardului ISO/IEC 27001:2013 si este auditata periodic.

11. REȚINEREA ȘI ELIMINAREA DATELOR

S&T ROMANIA SRL nu va păstra Datele personale într-o formă care permite identificarea persoanelor vizate pentru o perioadă mai lungă decât este necesar, în legătură cu scopurile pentru care datele au fost colectate inițial.

S&T ROMANIA SRL poate stoca datele perioade mai lungi conform termenelor imperative de prescriptive aplicabile si cu implementarea unor măsuri tehnice și organizaționale adecvate pentru a proteja drepturile și libertățile Persoanelor vizate.

Datele personale trebuie să fie eliminate în siguranță în conformitate cu al șaselea principiu al GDPR – prelucrate într-un mod adecvat pentru a menține securitatea, cu protejarea „drepturilor și libertăților" persoanelor vizate. Orice eliminare a datelor va fi efectuată în conformitate cu procedura de eliminare sigură.

12. INCIDENTE DE PROTECȚIE A DATELOR

Toți angajații sunt obligati să informeze imediat superiorul sau Coordonatorul cu Protectia Datelor (DPC) cu privire la cazurile de încălcare a acestei politici de protecție a datelor sau alte reglementări privind protecția datelor cu caracter personal (incidente de protecție a datelor), indiferent dacă este vorba despre o încalcare a confidentialității, a integrității datelor sau a disponibilității acestora. Conducatorul structurii organizatorice este obligat să informeze imediat Coordonatorul cu Protectia Datelor (DPC) cu privire la incidentele de protecție a datelor.

În cazurile de:

- Transmitere necorespunzătoare a datelor cu caracter personal către terțe părți,
- Acces neadecvat la datele cu caracter personal sau
- Pierdere, distrugere sau alterare a datelor cu caracter personal,

conducătorul structurii organizaționale în cauza întocmește, de urgenta, rapoartele de sesizare, conform regulilor de stabilite pentru Gestionarea Incidentelor de Securitate a Informațiilor, astfel încât să poată fi luate măsurile urgente pentru limitarea afectării titularilor de date cu caracter personal și pentru respectarea obligațiilor de raportare și notificare a incidentelor către autoritatea de supraveghere.

13. RESPONSABILITĂȚI ȘI SANCȚIUNI

Conducerea S&T România SRL precum și angajații și prepușii acestora sunt responsabili de prelucrarea datelor în zona lor de responsabilitate. Prin urmare, acestia sunt obligati să se asigure că sunt îndeplinite cerințele legale pentru protecția datelor și cele conținute în politica de protecție a datelor (de exemplu, obligațiile naționale de raportare). Organele de conducere au responsabilitatea de a se asigura că există măsuri organizaționale, resurse umane și tehnice pentru ca orice prelucrare a datelor să fie efectuată în conformitate cu protecția datelor. Respectarea acestor cerințe reprezinta responsabilitatea conducatorilor de structure organizatorice.

Coordonatorul cu Protectia Datelor (DPC) de la nivelul S&T România este informat de îndată despre controalele efectuate de autoritățile de supraveghere cu privire la protecția a datelor. Acesta, la randul sau, va informa Ofiterul de Protectia Datelor (DPO) desemnat la nivelul grupului S&T.

Coordonatorul cu Protectia Datelor (DPC) este persoana de contact local din cadrul S&T România. Acesta poate efectua verificări și familiarizează angajații S&T România cu conținutul politicilor de protecție a datelor. Departamentele responsabile de procesele și proiectele de afaceri informează în timp util Coordonatorul cu Protectia Datelor (DPC) cu privire la noile prelucrări de date cu caracter personal. Pentru planurile de prelucrare a datelor care pot prezenta riscuri speciale pentru drepturile individuale ale persoanelor vizate, Coordonatorul cu Protectia Datelor (DPC) sunt informati înainte de începerea procesării. Acest lucru se aplică în mod obligatoriu datelor cu caracter personal sensibile. Managerii se asigură că angajații lor sunt suficient de instruiți în protecția datelor.

Prelucrarea necorespunzătoare a datelor cu caracter personal sau alte încălcări ale legilor privind protecția datelor pot conduce la cereri de despăgubire pentru prejudicii. Încălcările pentru care angajații individuali sunt responsabili pot conduce la sancțiuni prevazute in dreptul muncii.

14. OFIȚERUL DE PROTECȚIA DATELOR (DPO)

Ofiterul de Protectia Datelor (DPO) numit la nivelul grupului de firme S&T, fiind independent din punct de vedere al ordinelor profesionale, isi desfasoara activitatea pentru respectarea legislatiei in vigoare privind protecția datelor. El este responsabil pentru politica de protecție a datelor și supraveghează respectarea acesteia. Ofițerul de Protectia Datelor are linie de raportare directă către Consiliul de Administrație al grupului S&T în cadrul careia isi desfasoara activitatea.

Responsabilul de Protecția Datelor (DPC) din cadrul S&T Romania, ca si reprezentant local, informează fără întârziere Ofiterul de Protectia Datelor (DPO) al Grupului S&T cu privire la orice risc de protecție a datelor. Orice

persoană vizată poate aborda Coordonatorul cu Protectia Datelor (DPC), în orice moment să ridice preocupări, să pună întrebări, să solicite informații sau să depună plângeri legate de protecția datelor sau de problemele de securitate a datelor. Dacă se solicită, preocupările și plângerile vor fi tratate în mod confidențial.

În cazul în care coordonatorul de date în cauză nu poate rezolva o plângere sau remedia încălcarea politicii de protecție a datelor, Ofiterul de Protectie a Datelor (DPO) este consultat de îndată. Deciziile luate de Ofiterul de Protectia Datelor (DPO) pentru remedierea încălcărilor privind protecția datelor trebuie să fie susținute de conducerea societății în cauză. Anchetele autorităților de supraveghere sunt întotdeauna raportate responsabilului cu protecția datelor.

Datele de contact ale responsabililor cu protecția datelor și ale personalului sunt următoarele:
S&T Romania, Ofițer de Protecție a Datelor (DPO).
E-mail: privacy@snt.ro;
Fax: +40 21 2085800
Mobil: +40 756079018
S&T Group, Ofițer de Protecție a Datelor (DPO)
E-mail: privacy@snt-world.com

15. Data intrarii in vigoare.Modificare

Prezenta Politică intră în vigoare la 25 Mai 2018.

S&T Romania SRL poate schimba sau modifica prezenta politică periodic. Acest lucru se poate întâmpla, de exemplu, din cauza schimbărilor de lege, sau dacă S&T Romania SRL îşi modifică afacerea sau practicile sale.