2026

FORT S.A.: Politică generală privind securitatea informațiilor

Cuprins

1. POLITICA GENERALĂ PRIVIND SECURITATEA INFORMAȚIILOR

Această Politică generală privind securitatea informatiilor a fost adoptată la nivelul

FORT S.A.

De către: Delia Alina Necula

În calitate de: Director General

2. INTRODUCERE. OBIECTIV, SCOP ȘI UTILIZATORI

FORT S.A. (referită în cele ce urmează ca "***Societatea***" sau "***FORT***") este un furnizor român de servicii de cybersecurity și securitate a informațiilor, specializat în teste de penetrare, audituri de securitate, evaluări de conformitate și servicii SOC. Cu experiență în proiecte desfășurate pentru organizații din domenii reglementate și critice, FORT furnizează servicii menite să identifice vulnerabilități, să reducă riscurile cibernetice și să sprijine conformitatea cu cerințele de securitate și reglementare aplicabile. În desfășurarea activității sale, Societatea realizează operațiuni de prelucrare de date cu caracter personal.

Având în vedere preocuparea Societății pentru respectarea legislației, în general, și a normelor destinate să asigure un nivel ridicat de protecție a persoanelor fizice în ceea ce privește datele cu caracter personal ale acestora, în special, se impune adoptarea acestei politici generale menită să reglementeze cerințele generale aplicabile la nivelul Societății în asigurarea securității informațiilor.

Această Politică privind securitatea informațiilor (referită în cele ce urmează ca "***Politica***") se aplică tuturor datelor cu caracter personal prelucrate de Societate, în format electronic și/sau în format fizic. Totodată această Politică reglementează o serie de cerințe esențiale cu privire la utilizarea echipamentelor de lucru, inclusiv a stațiilor de lucru și a dispozitivelor electronice utilizate în exercitarea atribuțiilor și responsabilităților deținute în cadrul Societății.

Politica stabilește o serie de reguli generale ce trebuie respectate cu privire la orice date cu caracter personal prelucrate de către Societate, alături de seturi de cerințe specifice aplicabile în funcție de suportul de stocare utilizat.

Utilizatorii acestui document sunt:

(i) toți angajații, permanenți sau temporari, ai Societății;

(ii) toți contractorii/colaboratorii sau alte persoane care lucrează în numele Societății, în baza unui contract încheiat cu Societatea, cu perioadă determinată sau nedeterminată, indiferent de perioada de timp stabilită, prin care se stabilesc atribuții și responsabilități în legătură cu operațiuni de prelucrare desfășurate în numele Societății (în această categorie vor intra deopotrivă, spre exemplu, și persoanele fizice constituite ca persoane fizice autorizate și care încheie un contract de colaborare cu Societatea cât și persoanele fizice care ar beneficia, pentru o perioadă determinată limitată în timp, de un program de internship în cadrul Societății, conform prevederilor legale aplicabile).

Această Politică se aplică împreună cu Politica Generală privind Protecția Datelor cu Caracter Personal, precum și cu celelalte politici și proceduri aplicabile la nivelul Societății, toate aceste documente constituindu-se în documente cu caracter obligatoriu și a căror respectare este imperios necesară. Prevederile Politicii Generale privind Protecția Datelor cu Caracter Personal cu privire la consecințele aplicabile în cazul nerespectării prevederilor politicilor și procedurile instituite la nivelul Societății în materia protecției datelor cu caracter personal rămân pe deplin aplicabile.

Definițiile formulate în cadrul Secțiunii 4 din Politica Generală protecția datelor cu caracter personal rămân aplicabile.

3. CERINȚE DE BAZĂ CU PRIVIRE LA STOCAREA DATELOR CU CARACTER PERSONAL

Astfel cum se indică în Politica Generală a Societății cu privire la prelucrarea datelor cu caracter personal, respectarea limitărilor legate de stocare este un principiu obligatoriu de urmat pentru toate activitățile de prelucrare realizate de Societate.

3.1. Cum se determină perioada de stocare. Acțiuni de îndeplinit odată ce perioada de stocare a expirat

Odată ce scopul prelucrării a fost stabilit cât de precis cu putință, va fi posibilă determinarea perioadei pentru care Societatea poate stoca datele în cauză, prin raportare la scopul respectiv. Perioada de stocare se determină cu luarea în considerare – pe lângă scopul prelucrării – a prevederilor legale (în special din domeniul protecției datelor cu caracter personal), având în vedere, de asemenea, obligațiile de stocare a unor anumite date, termenele de prescripție aplicabile şi practicile recomandate în materie.

Perioada de stocare a datelor va fi stabilită încă dinainte de momentul colectării. Este interzis oricărui angajat sau colaborator al Societății să stocheze datele cu caracter personal (*inclusiv pe propria staţie de lucru ori în propria căsuţă de email etc.)* după expirarea perioadei de stocare.

Odată ce scopul prelucrării a fost îndeplinit (odată ce a expirat durata necesară îndeplinirii scopului prelucrării), datele nu mai pot fi păstrate într-o formă care să permită identificarea persoanei vizate.

Aceasta înseamnă că datele vor trebui, fie (i) să fie șterse, fie (ii) să fie anonimizate. Nu este suficientă criptarea sau pseudonimizarea datelor cu caracter personal pentru ca această cerință să fie îndeplinită.

Ștergerea semnifică distrugerea definitivă a tuturor datelor cu caracter personal, inclusiv a tuturor copiilor acestora, în format fizic sau electronic, astfel încât acestea să nu mai poată fi recuperate.

Anonimizarea înseamnă înlăturarea oricărei posibilități ca persoana la care se referă informațiile în cauză să poată fi identificată, astfel încât să nu mai fie posibil ca informațiile să îi fie atribuite unei anumite persoane. De aceea, datele criptate și datele pseudonomizate nu echivalează cu ștergerea datelor: rămâne posibilă decriptarea lor sau accesul la lista de pseudonime și semnificația lor (datele de identificare ale persoanei vizate).

Societatea poate implementa, conform propriului calendar și opțiuni, sisteme care permit ștergerea automată a datelor cu caracter personal/ marcarea datelor cu caracter personal odată cu expirarea perioadei de stocare. Acolo unde aceasta nu va fi aplicabil sau nu va fi posibil, după caz, Societatea se va asigura că datele sunt șterse manual atunci când se împlinește perioada de stocare.

Persoanele vizate trebuie informate inclusiv despre perioada de stocare a datelor cu caracter personal care se referă la acestea. Pentru mai multe detalii cu privire la informarea persoanelor vizate, vedeți

Capitolul 4 din Procedurile aplicabile la nivelul Societății – *Procedură privind respectarea Obligațiilor referitoare la informarea persoanei vizate.*

3.2. Unde este prevăzută perioada de stocare pentru prelucrările în curs

Prelucrările în curs au deja stabilită o perioadă de stocare în nomenclatorul arhivistic al Societății. De asemenea, această perioadă este prevăzută în registrul de evidenţă al prelucrărilor de date cu caracter personal realizate de Societate.

3.3. Stocarea datelor cu caracter personal în temeiul unei obligații legale

Anumite acte normative obligă Societatea să stocheze anumite documente care conțin date cu caracter personal. Aceasta înseamnă că perioada de stocare va fi cea prevăzută în legile respective.

Pentru evitarea oricărui dubiu, inclusiv în cazul în care este prevăzută de lege (chiar și cu titlu obligatoriu), perioada de stocare va fi înscrisă în nomenclatorul arhivistic al Societății şi în registrul de evidenţă a operaţiunilor de prelucrare de date cu caracter personal realizate de aceasta.

3.4. Exemple privind limitările legate de stocare

Prelucrarea datelor privind reprezentanții sau persoanele de contact ale asociatului / reprezentantului persoane juridice nu ar trebui să mai aibă loc ulterior încetării raporturilor dintre reprezentantul/persoana de contact și societatea ce este asociat / reprezentant, pentru o perioadă mai lungă decât cea impusă de prevederile legale aplicabile (*i.e. prevederile Legii societăților și dispozițiile ce reglementează termenele de prescripție a răspunderii Societății).* Aceeași cerință se aplică și în cazul reprezentanților sau persoanelor de contact ale partenerilor comerciali (furnizori, clienți, etc.)

Prelucrarea datelor partenerilor comerciali (*e.g. furnizori și/sau prestatori de servicii)* nu ar trebui să continue după încetarea raporturilor cu aceștia, pentru o perioadă mai lungă decât ar putea fi justificat prin prisma termenelor de prescripție a răspunderii Societății, mai puțin în cazurile în care prelucrarea poate fi justificată, cum ar fi existența unui litigiu în curs cu privire la aspecte ce derivă din contractele încheiate cu aceștia.

Datele angajaților și ale colaboratorilor ar trebui șterse sau anonimizate după ce raporturile de muncă ori, după caz, de colaborare, dintre aceștia și Societate au încetat, cu excepția cazurilor și pentru perioada în care este necesară prelucrarea pentru constatarea, exercitarea și apărarea drepturilor Societății în instanță sau înaintea altor organe ori a situațiilor în care legislația din diverse domenii (*eg, contabilitate, arhivare*) impune Societății să stocheze anumite documente care conțin date privitoare la angajații săi (inclusiv din trecut) (*i.e. informații și documente ce constituite dosarele de personal, pentru 75 de ani*).

4. REGULI DE BAZĂ CU PRIVIRE LA UTILIZAREA TERMINALELOR (STAȚIILOR) DE LUCRU

Utilizarea terminalelor (stațiilor de lucru) de către destinatarii acestei Politici va urma regula de bază conform căreia orice activitate suspectă identificată în cadrul oricărei interfețe a unui terminal de lucru, indiferent de natura și durata activității identificate, va fi notificată de îndată în atenția departamentului Tehnologia Informației și Asistență Tehnică (Digital & IT). Aceeași regulă se aplică și în cazul identificării oricărei activități sau elemente de orice natură, suspecte, în contextul primirii și transmiterii de

corespondențe electronice, atât în circuit închis (în cadrul sistemelor Societății) cât și în circuit deschis (expeditori și/sau destinatari din afara Societății).

4.1. Contul de utilizator și parola

Fiecare utilizator va primi, corespunzător terminalului de lucru utilizat, din partea persoanei desemnate din cadrul departamentului IT, o parolă de acces la contul de utilizator, prin intermediul căruia poate utiliza terminalul de lucru încredințat și poate accesa documente și informații, conform drepturilor de acces conferite.

În aceeași zi lucrătoare în care utilizatorului îi este încredințat terminalul de lucru utilizat, acesta va schimba parola furnizată cu o parolă confidențială, pe care nu o va încredința și/sau divulga nimănui. Parola nou stabilită va respecta următoarele cerințe în mod cumulativ:

(i) minim 8 caractere, printre care se vor regăsi litere mari, litere mici, cifre și caractere speciale (*e.g.* ”!”, ”&”);

(ii) nu se pot repeta mai mult de 3 caractere, în grup, preluate din denumirea contului de utilizator.

. Utilizatorul nu va modifica denumirea contului de utilizator.

Parolele nu vor conține elemente sau valori care sunt cunoscute general ca fiind utilizate în compunerea parolelor de acces sau care au fost compromise în contextul utilizării contului de utilizator în cadrul sistemului informatic al Societății sau în cadrul oricărui alt program informatic / aplicație / cont de utilizator deținut în platforme terțe de către utilizatorul căruia i se adresează această Politică. Spre exemplu, utilizatorii se vor abține în mod special de la utilizarea de parole care includ, fără a se limita la:

- Parole deținute în cadrul unor incidente de securitate anterioare;
- Cuvinte/Sintagme/Expresii de dicționar;
- Caractere repetitive sau secvențiale;
- Elemente de context (denumiri ale serviciilor furnizate de Societate sau ale oricăror elemente conexe activității desfășurate de Societate).

Este recomandabil ca utilizatorul să procedeze la modificarea parolei cel târziu la 6 luni de la momentul ultimei actualizări a parolei, sau mai devreme în orice situație în care identifică orice suspiciune de acces neautorizat, indiferent de eșecul sau succesul unei eventuale încercări de acces.

Utilizatorul trebuie să păstreze parola setată secretă și să nu o dezvăluie nimănui. Nu este permisă notarea parolei pe orice suport fizic sau electronic.

Nu este permisă utilizarea funcției ”*Remember Password”*.

Nu este permisă utilizarea parolei setate pentru contul de utilizator în cadrul terminalului de lucru pentru orice alt cont de utilizator pe care utilizator îl creează în cadrul oricărei aplicații informatice utilizate pe terminalul de lucru sau pe orice dispozitiv electronic personal.

4.2. Utilizarea acceptată a datelor și sistemelor Societății

Datele și sistemele informatice ale Societății vor fi utilizate doar în scopuri subsumate atribuțiilor și responsabilităților ce incumbă fiecărui utilizator, în funcție de poziția și rolul utilizatorului în cadrul

Societății. Orice utilizare a datelor, sistemelor și dispozitivelor Societății trebuie să respecte politicile, standardele, procedurile și liniile directoare ale Societății, precum și orice acorduri de licență și legislație aplicabilă.

Utilizatorilor le este strict interzis:

(i) să încerce să acceseze / să acceseze terminale, stații de lucru și/sau orice alte echipamente care nu au fost în mod specific încredințate spre utilizare, conform indicațiilor și instrucțiunilor primite din partea departamentului IT;

(ii) să încerce să instaleze / să instaleze aplicații informatice sau orice programe pe terminalele de lucru pe care le utilizează; în cazul în care exercitarea atribuțiilor de muncă deținute impune descărcarea / instalarea unei aplicații informatice specifice, utilizatorul va solicita asistență din partea departamentului IT;

(iii) să ruleze aplicații informatice neautorizate pentru a fi utilizate în cadrul sistemului informatic al Societății (fișiere executabile care nu necesită instalare în sistem);

(iv) să folosească dispozitive și/sau echipamente de orice natură neaprobate și/sau aplicații externe care nu au fost aprobate în prealabil și cu privire la care nu s-au furnizat instrucțiuni și indicații de utilizare din partea departamentului IT;

(v) să dezactiveze sau să întreprindă orice încercare de anihilare a sistemelor / setărilor de securitate instalate și rulate pe terminalele de lucru;

(vi) să conecteze dispozitive periferice la terminalul de lucru, fără a obține aprobarea prealabilă și/sau asistență din partea departamentului IT, după caz;

(vii) să permită accesul, utilizarea sau vizualizarea oricăror informații stocate pe terminalul de lucru, de către o terță persoană neautorizată;

(viii) să utilizeze terminalul de lucru, precum și orice aplicație informatică instalată pe terminalul de lucru, inclusiv dar fără a se limita la aplicația de e-mail, pentru scopuri ce nu se subsumează atribuțiilor și sarcinilor de lucru, inclusiv dar fără a se limita la scopuri personale;

(ix) să acceseze, de pe terminalul de lucru, orice sursă web ce prezintă suspiciuni de legitimitate sau securitate;

(x) să utilizeze, chiar și contextul îndeplinirii unor atribuții și responsabilități de lucru, website-uri publice de stocare a datelor (*e.g. OneDrive, Dropbox, GoogleDrive, WeTransfer, etc.*); utilizatorii au obligația de a folosi în mod exclusiv instrumente aprobate la nivelul Societății pentru asigurarea transferului de date sigur și confidențial; în cazuri excepționale în care utilizarea unor instrumente precum cele referite anterior ca fiind furnizate prin intermediul unor surse publice de stocare a datelor este permisă, în baza aprobării prealabile primite din partea departamentului IT, datele trebuie partajate în format criptat iar cheia de criptare trebuie păstrată și transmisă în mod separat și distinct, către destinatar;

(xi) să transmită informații ce constituie date cu caracter personal prelucrate de către Societate, către alte persoane din cadrul Societății sau către terțe persoane, prin intermediul unor canale de comunicare

ce nu se află sub controlul deplin al Societății, cum ar fi dar fără a se limita la SMS sau programe de mesagerie instant, inclusiv dar fără a se limita la, *WhatsApp, Facebook Messenger, Viber*, etc.

4.3. Protecția fizică a terminalelor de lucru și a oricăror dispozitive încredințate de către Societate

Orice angajat și/sau colaborator în cadrul Societății trebuie să ia și să mențină măsuri adecvate pentru a asigura protecția fizică a terminalelor de lucru precum și a oricăror dispozitive electronice sau de altă natură încredințate de către Societate și care sunt purtătoare de informații.

Utilizatorii au obligația, în orice moment, de a-și securiza în mod adecvat dispozitivele mobile și terminalele de lucru mobile (*e.g. laptop*) împotriva furtului sau deteriorării, trebuie să păstreze în permanență dispozitivele sub supraveghere. Atunci când supravegherea dispozitivelor nu poate fi asigurată în mod nemijlocit, cum ar fi situația în care dispozitivul trebuie lăsat în camera de hotel în care se află cazat utilizatorul aflat în exercitarea sarcinilor de serviciu, utilizatorul se va asigura că dispozitivul este securizat (*e.g. se va lăsa în seiful din camera de hotel sau se va închide într-un sertar cu cheie și va lua cheia în posesie)*. Dispozitivele nu se vor lăsa în nicio situație nesupravegheate, în locuri private sau publice, sau în autoturism (chiar dacă acesta este încuiat). Atunci când călătoriți, este necesar să transportați dispozitivul sau dispozitivele în bagajul de mână. Dispozitivele lăsate în birou peste noapte trebuie să fie securizate (*e.g. încuiate în dulapuri sau încuiate birourile)*.

Dispozitivele mobile nu vor fi utilizate în locuri în care ecranul poate fi vizualizat cu ușurință de către terțe persoane (*e.g. într-un tren, într-o cafenea*, etc.) Pentru laptop-uri se recomandă utilizarea filtrelor de ecran pentru asigurarea confidențialității (*privacy filters*).

4.4. Predarea dispozitivelor de lucru la momentul încetării raporturilor contractuale cu Societatea

La momentul încetării raporturilor contractuale cu Societatea, respectiv în ultima zi în care contractul de muncă/colaborare existent între angajat/colaborator/contractor și Societate este în vigoare și angajatul/colaboratorul se află în exercitarea atribuțiilor (*e.g. nu este în concediu de odihnă/fără plată)*, angajatul/contractorul/colaboratorul are obligația să asigure predarea dispozitivului de lucru ce i-a fost furnizat de către Societate.

Anterior predării dispozitivului de lucru, angajatul/colaboratorul/contractorul are obligația să se asigure că orice documente/informații/date gestionate în exercitarea atribuțiilor desemnate de către Societate sunt salvate în cadrul partițiilor corespunzătoare din cadrul sistemului informatic al Societății și niciun un document/informație/dată de orice natură nu este păstrată local.

Totodată, anterior predării dispozitivului de lucru, acesta va fi curățat de orice conținut de uz personal.

De asemenea, angajatul/colaboratorul/contractorul are obligația ca, anterior predării dispozitivului de lucru, să procedeze la solicitarea dezabonării de la orice comunicări comerciale ce ar putea fi transmise pe viitor pe adresa de e-mail profesională. În același sens, angajatorul/colaboratorul/contractorul are obligația să elimine adresa de e-mail profesională de pe orice platforme ar fi fost folosită, în scop profesional sau personal (*e.g. platforme de servicii de transport, platforme de intermediere pentru servicii de livrare produse alimentare, etc*.).

Dispozițiile de mai sus se aplică în mod corespunzător pentru orice dispozitiv și accesoriu furnizat angajatului/colaboratorului/contractorului de către Societate pentru exercitarea atribuțiilor desemnate.

Predarea dispozitivului de lucru se face către coordonatorul departamentului HR, moment în care se semnează un Proces-verbal de predare a dispozitivului de lucru. Prin semnarea Procesului-verbal, angajatul/colaboratorul/contractorul atestă că predarea dispozitivului de lucru este făcută în deplină conformitate cu prevederile Politicii Generale a Societății privind securitatea informațiilor, inclusiv din perspectiva obligației ce incumbă angajatului/colaboratorului/contractorului de a curața dispozitivul de absolut orice documente/informații/date de uz personal.

Modalitatea în care Societatea va gestiona adresa de e-mail și conturile de utilizator ce au create pentru uzul angajatului/colaboratorului/contractului, în exercitarea atribuțiilor sale profesionale, este la aprecierea Societății și va fi stabilită de la caz la caz, având în vedere totodată și poziția deținută de angajat/colaborator/contractor în Societate, în deplină conformitate cu prevederile legale aplicabile. Prevederile acestui paragraf rămân aplicabile și în cazurile în care angajatul/colaboratorul/contractorul Societății părăsește intempestiv locul de muncă sau nu poate fi găsit de către reprezentanții Societății. Societatea va depune toate diligențele pentru ca gestionarea adresei de e-mail și a conturilor de utilizator să fie realizate astfel încât să nu se aducă sau să se aducă minime atingeri drepturilor și libertăților angajatului/colaboratorului/contractorului Societății.

5. CERINȚE SPECIFICE PRIVIND SECURITATEA DATELOR CU CARACTER PERSONAL STOCATE PE SUPORTURI FIZICE

Acest Capitol se aplică tuturor datelor cu caracter personal prelucrate de Societate și stocate în format fizic, cum ar fi cele reprezentate de sau conținute în documente în format hârtie, în fotografii printate și în orice alte documente sau suporturi fizice (denumite în continuare, împreună, *Documentele*).

5.1. Primirea de Documente

Orice documente ce sunt destinate unei persoane din cadrul Societății vor fi predate către persoanele desemnate din cadrul recepției ce deservește Societatea sau vor fi predate personal către persoana indicată ca destinatar. Personalul din cadrul recepției ce deservește Societatea va înmâna orice documente primite în numele Societății, în calitate de expeditor, imediat sau la finalul unei zile lucrătoare, către o persoană desemnată în acest sens de către Societate.

Angajații și/sau colaboratorii Societății ce cunosc că trebuie să primească documente ce constau în sau încorporează date cu caracter personal vor furniza expeditorilor instrucțiuni precise cu privire la livrarea și înmânarea documentelor, inclusiv dar fără a se limita la instrucțiuni cu privire la imperativul livrării documentelor în plicuri sau folii opace, netransparente și sigilate, astfel încât conținutul documentelor livrate să nu poată fi consultat, cu voie sau fără voie, de către orice persoană terță ce ar intra în posesia documentelor.

Orice angajat și/sau colaborator al Societății ce intră în posesia unui document ce nu îi este destinat va preda documentul la recepția ce deservește Societatea, astfel încât documentul să fie înregistrat și transmis către destinatarul indicat, fără ca acest document să fie consultat de către persoanele ce își desfășoară activitatea în cadrul recepției ce deservește Societatea.

În nicio situație, un angajat și / sau colaborator al Societății nu va consulta un document ce nu îi este destinat.

5.2. Crearea / copierea Documentelor

Politica Societății este de a limita cât mai mult posibil stocarea de date cu caracter personal în format fizic.

În cadrul fiecărui departament al Societății, se stabilesc următoarele situații/scopuri în care este permisă înregistrarea de date cu caracter personal în format fizic:

(i) întocmirea dosarelor de personal ale angajaților – operațiune ce se poate efectua exclusiv de către persoanele ce dețin atribuții specifice departamentului de resurse umane;

(ii) operațiuni corporative (*spre exemplu, întocmire Hotărâri ale Adunării Generale în format fizic, spre semnare de către acționari)* – operațiune ce se poate efectua exclusiv de către persoanele ce dețin atribuții specifice departamentului de asistență juridică;

(iii) operațiuni comerciale (*spre exemplu, semnarea olografă a unui contract comercial)* – operațiunea ce se poate efectua exclusiv de către persoanele ce dețin atribuții specifice departamentului de asistență juridică sau departamentului financiar;

Societatea poate stabili și alte situații, suplimentar celor de mai sus.

Pentru scopul acestei Secțiuni 5.2., este asimilată înregistrării de date cu caracter personal în format fizic imprimarea unor documente existente în format electronic.

Înregistrarea de date cu caracter personal în format fizic va fi realizată doar în măsura necesară (*e.g., nu veți imprima / fotocopia mai multe pagini din Documente sau mai multe exemplare din Documente decât aveți nevoie; nu veți include într-un Document creat alte date cu caracter personal decât cele strict necesare ținând cont de scopul Documentului).*

Toate Documentele care au fost create vor fi distruse imediat ce nu mai sunt necesare și relevante. Dispozițiile din Secțiunea 5.5. – *Distrugerea documentelor* se aplică în mod corespunzător.

În cazul în care au fost imprimate Documente ce constau în sau încorporează date cu caracter personal, persoana care a dat comanda de imprimare are obligația de a le colecta imediat de la imprimantă, spre a evita riscul ca o persoană neautorizată să aibă acces la acestea. Dacă din eroare intrați în posesia unui Document care nu vă este destinat, nu îl veți consulta, ci îl veți returna în locul de unde l-ați luat.

Este interzis să fie scoase în afara incintei Societății Documente ce conțin date cu caracter personal, cu excepția situațiilor în care acest lucru este necesar pentru îndeplinirea atribuțiilor deținute de către angajatul/colaboratorul/contractorul ce scoate documente în afara incintei Societății.

5.3. Stocarea Documentelor și accesul la acestea

Ca regulă, în perioadele în care nu este strict necesar și relevant accesul la ele, angajații/colaboratorii/contractorii Societății vor depune toate diligențele ca documentele să fie păstrate într-un spațiu fizic securizat, în măsura în care un astfel de spațiu securizat este disponibil.

Documentele nu vor fi lăsate niciodată nesupravegheate într-un loc accesibil terților. Pe perioada în care sunt necesare pentru consultare ori modificare, Documentele vor fi ținute într-o manieră care să nu permită vizualizarea / accesarea acestora de către persoane neautorizate.

Când nu sunt necesare pentru consultare ori modificare, și în orice caz cel mai târziu în fiecare zi la terminarea programului, fiecare persoană care deține Documente va depune toate diligențele pentru a se asigura că Documentele sale, fie originale, fie copii, sunt depozitate în fișete sigure, și în măsura posibilului, securizate. Societatea poate desfășura activități de audit pentru a verifica respectarea acestei oblligații.

În situația încetării raporturilor de serviciu sau a altor raporturi cu Societatea (*e.g. demisie, concediere, etc.*), persoana în cauză va returna de îndată orice Documente deținute în posesia sa precum și orice chei de acces deținute (*e.g. chei ale fișetelor, cartele de acces în camera de depozitare, etc.*), dacă există, nemaifiindu-i permis accesul.

5.4. Trimiterea Documentelor

Nu vor fi transmise Documente decât atunci când este strict necesar (*i.e., când nu se poate atinge altfel scopul urmărit)*. În astfel de cazuri, Documentele vor fi transmise printr-o metodă adecvată naturii datelor cu caracter personal și a riscurilor, asigurându-se permanent securitatea lor. Ambalajul/cutia în care Documentele sunt stocate pe durata transportului nu va dezvălui conținutul acestora. Pentru a evita riscul pierderii, al alterării, al distrugerii sau al furtului lor, Documentele vor fi scoase din incinta Societății într-un mod organizat (*e.g. în mape, dosare, cutii, capsate, prinse cu agrafe, etc.*).

Ca regulă, Documentele vor fi transmise în copie electronică (*e.g. scan-uri)*, iar nu fizică. Copiile electronice ale Documentelor vor fi transmise prin canale securizate, cum ar fi email-uri securizate, rețele securizate sau printr-un stick USB sau CD criptat. Numai când aceasta nu este posibil, Documentele pot fi transmise în format fizic (original, dacă este strict necesar, potrivit celor mai de mai sus, sau copie). De asemenea, ca regulă, se va evita utilizarea faxului pentru transmiterrea Documentelor, în special atunci când nu se poate cunoaște dinainte cine este persoana care va ridica faxul.

Ca regulă, nu vor fi scoase Documente originale din incinta Societății și nici copii de siguranță ale acestora. În situațiile strict excepționale în care este necesar să fie ridicate originale sau copii de siguranță, pentru a evita o încălcare a securității datelor prin pierderea accesului la ele, sunteți obligat(ă) să vă asigurați că există cel puțin o copie fizică sau electronică a acestora în posesia Societății.

În toate cazurile, Documentele vor fi scoase din incintele Societății numai în măsura strict necesară, *eg*, dacă este necesară transmiterea doar a unor pagini dintr-un dosar al unui angajat, numai acelea vor fi scoase.

Ori de câte ori este posibil, datele care nu sunt necesare (*eg*, numele clientului) vor fi anonimizate (confidențializate).

Trebuie să vă asigurați că Documentele vor fi primite doar de destinatari sau de persoanele care îi reprezintă, și nu de un alt membru al personalului destinatarului/ altă persoană (*eg*, se va scrie pe fiecare plic exact în atenția cui este trimis).

5.5. Distrugerea Documentelor

Imediat ce nu mai sunt necesare, orice copii fizice ale Documentelor (cu excepția originalelor) vor fi distruse de persoana care le-a utilizat. Pentru evitarea oricărui dubiu, această obligație nu se aplică în legătură cu Documentele care potrivit legii trebuie păstrate, în format fizic, pentru o anumită perioadă de timp. Aceste Documente, imediat ce nu mai sunt necesare, vor fi predate persoanei responsabile cu arhivarea documentelor, pentru a fi arhivate.

Prin excepție de la cele de mai sus, datele rezultate din activitățile de testare de securitate, inclusiv datele de testare și rapoartele aferente, vor fi păstrate pentru o perioadă de maximum trei (3) luni de la data acceptării raportului final de către client. La expirarea acestei perioade, datele de testare și rapoartele vor fi șterse în mod securizat, cu excepția cazului în care o obligație legală impune păstrarea acestora pentru o perioadă mai lungă.

Documentele originale sau copiile acestora din arhiva Societății (copiile de siguranță) pot fi distruse/șterse numai de persoane autorizate din cadrul Societății, respectiv de coordonatorii departamentelor constituite conform unor criterii de ierarhie a membrilor sau de către oricare membru al departamentelor ce nu sunt constituite conform unor criterii de ierarhie, conform atribuțiilor deținute.

La distrugerea originalelor Documentelor Societății va fi încheiat un proces-verbal. Persoanele responsabile conform celor de mai sus se vor asigura că odată cu distrugerea oricăror originale ale Documentelor sunt distruse și toate copiile acestora, astfel încât limitările legate de stocare să fie respectate.

Documentele vor fi distruse folosind un *shredder*, sau prin orice alt mod care să asigure că Documentele nu mai pot fi reconstituite/recuperate. Sub nicio formă Documentele nu vor fi aruncate în coșul e gunoi (fie și rupte sau mototolite) sau în alte locuri.

Pentru a evita riscul duplicării Documentelor, orice fotocopii (inclusiv print-uri după scan-uri) ale Documentelor vor fi distruse imediat ce nu mai sunt necesare. Sub nicio formă Documentele nu vor fi aruncate la coș (chiar și rupte ori mototolite) sau folosite pentru alte scopuri (de exemplu notarea anumitor informații în zonele libere ale Documentelor).

5.6. Copiile de siguranță ale Documentelor (copiile din arhiva Societății)

Toate Documentele vor avea copii de siguranță (în format electronic și/sau fizic), pentru a evita o încălcare a securității datelor prin pierderea accesului la acestea.

Copiile de siguranță fizice se vor stoca în fișete fizice, în măsura posibilului, securizate, distincte de fișetele în cadrul cărora se depozitează originalele Documentelor.

Copiile de siguranță electronice se vor stoca într-un mediu securizat, fiind, în măsura posibilului, criptate.

Accesul la toate copiile de siguranță va fi realizat conform prevederilor din secțiunea 5.3. - *Stocarea Documentelor și accesul la acestea.*

Odată ce a expirat perioada de stocare a datelor cu caracter personal din Documente (inclusiv, dacă este cazul, perioada de stocare prevăzută în dispoziții legale obligatorii), copiile de siguranță vor fi distruse, împreună cu originalele, conform celor menționate mai sus.

6. CERINȚE SPECIFICE PRIVIND SECURITATEA DATELOR CU CARACTER PERSONAL STOCATE PE SUPORTURI ELECTRONICE

Acest Capitol se aplică tuturor datelor cu caracter personal în format electronic prelucrate de Societate, cum ar fi cele stocate pe CD-uri, DVD-uri, stick-uri USB, dischete, hard disk-uri (computere, laptopuri și alte posibile stații de lucru), servere ale Societății, *cloud,* etc. Toate aceste suporturi ale datelor cu caracter personal prelucrate de Societate sunt denumite în continuare, împreună, ***Documentele Electronice.***

Acest Capitol nu se aplică bazelor de date ale Societății, ci numai copiilor electronice ale unor documente care conțin date cu caracter personal, inclusiv cu privire la orice copii electronice sau orice alte versiuni electronice ale documentelor reglementate în Capitolul 5 - *Cerințe specifice privind securitatea datelor cu caracter personal stocate pe suporturi fizice.*

6.1. Crearea / copierea Documentelor Electronice

Politica Societății este de a limita cât mai mult posibil prelucrarea datelor cu caracter personal, inclusiv a acelora stocate în Documente Electronice.

Este interzisă crearea de Documente Electronice (inclusiv prin copierea / scanarea unui document preexistent), cu excepția cazului în care o astfel de acțiune este strict necesară. Fotografierea, duplicarea, transcrierea sau orice alte operațiuni similare de reproducere totală sau parțială realizate cu sau asupra Documentelor Electronice sunt asimilate copierii Documentelor Electronice.

Atunci când este permis, să se efectueze operațiunile menționate anterior, acestea vor fi realizate doar în măsura necesară (*eg, nu veți include într-un Document Electronic creat alte date cu caracter personal decât cele strict necesare; necesitatea se va analiza ținând cont de scopul Documentului Electronic respectiv*).

Toate Documentele Electronice care au au fost create vor fi distruse imediat ce nu mai sunt necesare și relevante. Dispozițiile din secțiunea *Distrugerea Documentelor Electronice* din acest capitol se aplică în mod corespunzător.

Este interzisă crearea de Documente Electronice, accesarea sau modificarea Documentelor Electronice ori crearea de copii ale acestora (de) pe orice terminale (laptop-uri, tablete, smartphone-uri etc.), altele decât terminalele Societății sau chiar de pe terminalele Societății, dar în afara incintelor acesteia, sau transmiterea lor pe adresa personală de e-mail sau pe propria adresă de serviciu de e-mail etc., deoarece aceste operațiuni vor afecta trasabilitatea datelor cu caracter personal și asigurarea securității acestora. Din aceleași motive, indiferent de terminalele utilizate, niciodată nu vor fi create mai multe exemplare ale Documentelor Electronice decât este strict necesar.

6.2. Stocarea Documentelor Electronice și accesul la acestea

Indiferent de persoana responsabilă, Documentele Electronice vor fi ținute într-un mod ordonat.

Nu vor exista scan-uri/ copii ale Documentelor Electronice salvate local pe fiecare stație de lucru – toate Documentele Electronice vor fi stocate pe un server dedicat în foldere relevante special create pentru salvarea Documentelor Electronice. Chiar dacă documentele vor fi salvate pe server-ul dedicat, accesul la server și respectiv, la folder, va fi limitat la persoanele care au nevoie de drepturi de acces pentru îndeplinirea atribuțiilor și sarcinilor de serviciu încredințate. Dreptul de acces va fi acordat în mod diferențiat după nevoia de vizualizare și/sau editare, după caz. Sub nicio formă nu i se va permite accesul la Documentele Electronice unei persoane neautorizate, din cadrul sau din afara Societății.

În perioadele în care nu este strict necesar și relevant accesul la ele, Documentele Electronice vor fi închise. Orice utilizator care părăsește terminalul, indiferent de perioadă, îl va bloca (*eg, utilizând funcția Lock this computer a sistemului de operare Microsoft Windows sau orice funcție ce servește acestui scop)*.

Numai persoanele care au nevoie de acces la Documentele Electronice pentru îndeplinirea atribuțiilor în cadrul Societății vor avea acces la acestea. Accesul este permis strict în măsura în care acesta este necesar și strict în măsura în care Documentele Electronice sunt relevante. De exemplu, un Angajat nu poate avea acces la Documente Electronice care conțin date cu caracter personal cu privire la un client de care este responsabil alt angajat, cu excepția cazului în care la rândul său prestează servicii respectivului client și datele cu caracter personal stocate de celălalt angajat sunt relevante și pentru el.

În măsura posibilului, orice încercare de acces neautorizat la Documentele Electronice va fi înregistrată, spre a face posibilă identificarea de către Societate a persoanelor care au încercat să acceseze date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

În orice situație, operațiunile de accesare a Documentelor Electronice vor fi înregistrate, chiar dacă accesarea se face de către persoane autorizate.

Când nu sunt necesare pentru consultare ori modificare, și în orice caz cel mai târziu în fiecare zi la terminarea programului, fiecare persoană care utilizează Documente Electronice se va asigura că Documentele Electronice în cauză sunt salvate pe server-ul dedicat și închise pe stația de lucru pe care au fost create. Societatea va putea implementa un sistem automat prin care la finalul programului orice informații salvate local sau chiar pe server-ul dedicat, dar în alte fișiere decât cele relevante sunt șterse; prin urmare, este esențial să vă asigurați că orice Documente Electronice create au fost salvate pe server-ul dedicat în secțiunea corespunzătoare.

În fiecare zi la terminarea programului, fiecare Angajat și Colaborator va închide propria stație de lucru (*eg*, folosind funcția *Shut down* a sistemului de operare *Microsoft Windows*).

În cazul în care se impune părăsirea intempestivă a stațiilor de lucru (*e.g. alarmă de incendiu declanșată la nivelul clădirii în care își are premisele Societatea*, administratorul IT va proceda la blocarea / închiderea tuturor stațiilor de lucru de la distanță.

6.3. Trimiterea Documentelor Electronice

Pentru evitarea oricărui dubiu, prevederile din această secțiune (*Trimiterea Documentelor Electronice*) se aplică inclusiv transferului de Documente Electronice între departamentele/persoanele din cadrul Societății.

Nu vor fi transmise Documente Electronice decât atunci când este strict necesar (*ie*, când nu se poate atinge altfel scopul urmărit). În astfel de cazuri, Documentele Electronice vor fi trimise printr-o metodă adecvată naturii datelor cu caracter personal și a riscurilor, asigurându-se permanent securitatea lor.

Documentele Electronice de pe server, stick-uri USB etc., cel puţin în cazul în care este vorba despre documente conţinând categorii speciale de date cu caracter personal, date cu caracter personal cu un grad ridicat de sensibilitate (altele decât categoriile speciale de date cu caracter personal), date cu caracter personal privind condamnări penale, sancţiuni şi măsuri de securitate conexe şi date privitoare la minori, vor fi parolate. După consultarea Persoanei Responsabile, Societatea poate adopta reguli specifice care vor preciza detaliat ce tipuri de Documente Electronice vor fi parolate sau poate, după caz, să decidă parolarea tuturor Documentelor Electronice.

Ca regulă, Documentele Electronice vor fi transmise în copie electronică (*eg, scan-uri*), iar nu fizică (*ie*, *nu documente imprimate*). Copiile electronice ale Documentelor Electronice vor fi transmise prin canale securizate, cum ar fi email-uri securizate (prin excepţie, potrivit celor de mai jos), rețele securizate sau printr-un stick USB sau CD criptat.

Datele cu caracter personal din Documentele Electronice care nu sunt necesar a fi divulgate și nu sunt relevante pentru scopul urmărit vor fi anonimizate și numai datele/secțiunile de Documente Electronice /Documentele Electronice strict necesare și relevante vor fi transmise în formă neanonimă.

Din rațiuni de securitate și de evitare a duplicării datelor (care poate îngreuna trasabilitatea lor și, implicit, respectarea limitărilor legate de stocare), se va evita pe cât posibil transmiterea Documentelor Electronice prin email (inclusiv, dar fără a se limita la, transmiterea internă a Documentelor Electronice între departamente sau membri ai aceluiași departament al Societății). Email-ul standard (*ie*, nesecurizat) nu ar trebui niciodată folosit pentru transmiterea unor copii electronice ale Documentelor Electronice. În cazurile de excepție în care Documentele Electronice sunt transmise prin email, se vor aplica regulile de mai jos.

Societatea se va asigura că persoanele care trimit Documente Electronice prin email au acces la un email securizat (criptat) pentru aceasta, iar persoanele respective îl vor folosi.

În situația transmiterii unor copii electronice ale Documentelor Electronice prin e-mail, expeditorul va acorda o atenție deosebită faptului că (i) adresa de e-mail a destinatarului este scrisă corect și că (ii) orice e-mail-uri sunt transmise numai persoanelor care au cu adevărat nevoie de acces la Documentele Electronice în cauză. Dacă sunt transmise Documente Electronice către mai mulţi destinatari care nu îşi cunosc / nu ar fi necesar să își cunoască unii identitatea altora, se va utiliza funcţia *BCC* a programului de e-mail.

Atunci când sunt transmise copii electronice ale Documentelor Electronice criptate, indiferent dacă prin e-mail sau folosind alt canal, parolele pentru decriptare (cheile) trebuie să fie puternice. Aceste chei nu vor fi trimise împreună cu Documentele Electronice, ci separat, printr-un alt canal de comunicare (*eg, SMS sau apel telefonic*). Ele vor fi trimise doar destinatarului Documentelor Electronice și nu vor fi divulgate niciunei alte persoane.

Cerințele de securitate de mai jos cu privire la transmiterea prin e-mail a copiilor Documentelor Electronice se aplică în mod corespunzător atunci când sunt transmise copii ale Documentelor Electronice prin alte mijloace de comunicare electronice.

6.4. Distrugerea Documentelor Electronice

Imediat ce nu mai sunt necesare, orice copii copii fizice sau electronice ale Documentelor Electronice (altele decât copiile de siguranță din arhiva Societății) vor fi distruse de persoana care le-a utilizat. Pentru evitarea oricărui dubiu, această obligație nu se aplică oricăror Documente Electronice care potrivit legii trebuie păstrate pentru o anumită perioadă de timp. Aceste Documente Electronice, imediat ce nu mai sunt necesare, vor fi predate persoanei responsabile cu arhivarea documentelor, pentru a fi arhivate.

Documentele Electronice din arhiva Societății (copiile de siguranță) pot fi distruse/ șterse numai de persoane autorizate din cadrul Societății, respectiv de coordonatorii departamentelor constituite conform unor criterii de ierarhie a membrilor sau de către oricare membru al departamentelor ce nu sunt constituite conform unor criterii de ierarhie, conform atribuțiilor deținute. La distrugerea originalelor Documentelor Electronice sau a copiilor acestora din arhiva Societății va fi încheiat un proces-verbal. Persoanele responsabile se vor asigura că odată cu distrugerea oricăror Documente Electronice din arhivă sunt distruse și copiile de siguranță ale acestora, astfel încât limitările legate de stocare să fie respectate.

6.5. Copiile de siguranță ale Documentelor Electronice

Prevederile din Capitolul 5 din această Politică (*Cerințe specifice privind securitatea datelor cu caracter personal stocate pe suporturi fizice*) privind copiile de siguranță ale Documentelor Fizice se aplică în mod corespunzător și Documentelor Electronice.

6.6. Reguli speciale privind transmiterea e-mail-urilor

Cu toții folosim e-mail-ul pentru a ne realiza sarcinile în cadrul Societății. În marea majoritate a cazurilor, e-mail-urile conțin date cu caracter personal. Chiar adresa de e-mail, atunci când se referă la o persoană identificată sau identificabilă, constituie o dată cu caracter personal.

De fiecare dată, gândiți-vă dacă nu există mijloace mai adecvate de prelucrare a datelor decât e-mail-ul. De exemplu, dacă există un sistem dedicat în care persoanele vizate trebuie să introducă date cu caracter personal, nu transmiteți aceste date/ nu solicitați transmiterea acestor date prin e-mail.

Nu folosiți adresa de e-mail de serviciu pentru scopuri personale. Dacă primiți mesaje personale pe această adresă, delimitați-le clar de comunicările profesionale (foldere separate) pentru perioada pentru care vă sunt strict necesare, iar ulterior aceste e-mailuri se vor șterge definitiv. Odată ce încetați raporturile cu Societatea, ștergeți în mod definitiv toate e-mail-urile personale din căsuța dumneavoastră (atât din Inbox cât și din folderul dedicat păstrării temporare a e-mail-urilor șterse (*e.g. Recycle Bin, Deleted Items)*.

Organizați e-mail-urile în funcție de subiect (eg, per proiect, per domeniu – HR, IT etc.).

Ștergeți periodic e-mail-urile din căsuța dumneavoastră atunci când nu mai aveți nevoie de ele, pentru a respecta principiul obligatoriu al limitărilor legate de stocare.

Schimbați periodic parola și nu o divulgați nimănui.

7. MONITORIZAREA ACTIVITĂȚII ȘI A CORESPONDENȚEI

În efectuarea activităților de monitorizare a sistemelor informatice și a aplicațiilor informatice utilizate de către angajați / colaboratori / contractori, în scopuri de asigurarea a securității și integrității datelor precum și de prevenire a oricăror potențiale incidente de securitate, personalul desemnat în acest sens al Societății poate dobândi acces la conținutul creat și stocat de un angajat / colaborator / contractor, inclusiv în ceea ce privește corespondențe și informații personale, destinate uzului personal al acestuia. Un astfel de acces este justificat pentru rațiuni de securitate. Pentru a minimiza intruziunea, angajații / colaboratorii și contractorii sunt obligați să nu dețină corespondențe personale și/sau informații personale pe stațiile de lucru, dincolo de acele corespondențe și informații ce sunt păstrate strict conform prevederilor acestei Politici.

8. AUTORIZARE ȘI DISEMINARE

Aprobarea și autorizare acestei Politici au fost realizate conform mențiunilor redate în cadrul Secțiunii 1 din această Politică. Revizuirea Politicii se realizează anual sau ori de câte ori este nevoie.

Această Politică generală privind securitatea informatiilor a fost adoptată la nivelul FORT S.A.

De către: Delia-Alina Necuma

În calitate de: Director General

Actualizată în data de: 01.06.2026

Aplicabilă în această versiune din data de: 01.06.2026