POLITICA PRIVIND UTILIZAREA ECHIPAMENTELOR TEHNICE

A. Scop

Versus Project adoptă prezenta politică privind utilizarea echipamentelor („**Politica**") pentru a asista societatea în asigurarea gestionării corecte a echipamentelor tehnice puse la dispoziția angajaților pentru desfășurarea activității lor, precum și a protecției datelor cu caracter personal în contextul desfășurării activităților de către angajați și a activităților de monitorizare a conformării cu cerințele legale și politicile interne. Politica include reguli privind accesul la aceste date care sunt stocate pe serverele care aparțin Versus Project, precum și pe calculatoarele, tabletele, telefoanele mobile și mașinile aparținând Versus Project, puse la dispoziția angajaților pentru realizarea atribuțiilor de serviciu („**Echipament Tehnic**"). Aceste reguli sunt menite să asigure că prelucrarea Datelor cu Caracter Personal stocate în Echipamentul Tehnic („**Date din Echipamentul Tehnic**") se face cu respectarea legislației privind protecția datelor și confidențialitatea. Dacă există orice dubii cu privire la aplicarea regulilor din prezenta Politică, orice asemenea întrebări vor fi adresate Administratorului.

B. Definiții

- „**Date cu Caracter Personal**" înseamnă informațiile care identifică o persoană fizică sau care o fac cel puțin identificabilă.
- „**Date de Trafic**" înseamnă datele prelucrate în contextul trimiterii de comunicări, excluzând conținutul acestor comunicări. Datele de Trafic includ, fără limitare, informații indicând apelurile trimise și primite, durata apelurilor, mesajele e-mail trimise și primite, frecvența apelurilor și mesajelor e-mail, precum și volumul mesajelor e-mail circulate.
- „**Date de Comunicații**" înseamnă Datele de Trafic și/sau conținutul comunicațiilor.
- „**Angajat Vizat**" - orice angajat, lucrător temporar, contractor independent sau alt colaborator al Versus Project al cărui Echipament Tehnic este accesat pe baza cestei Politici.
- **„Angajat Nominalizat"** - orice angajat, lucrător temporar, contractor independent sau alt colaborator al Versus Project care este nominalizat să acceseze mesajele e-mail ale Angajatului Absent, potrivit secțiunii D din prezentele Reguli.
- **„Fișierele Echipamentului Tehnic"** - orice fișiere, documente și orice alt tip de informații stocate în Echipamentul Tehnic. Pentru evitarea oricăror dubii, orice referiri la „angajați" în această Politică acoperă, de asemenea, lucrătorii temporari, contractorii independenți sau orice colaboratori care lucrează în Versus Project.

C. Obligațiile angajaților privind utilizarea Echipamentului Tehnic

Întregul Echipament Tehnic pus la dispoziție de către Versus Project și tot ce este generat prin intermediul acestui Echipament Tehnic (inclusiv, dar fără limitare la, corespondența din conturile de e-mail ale Versus Project) este proprietatea Versus Project. Angajații Versus Project vor respecta regulile stabilite de CPAG privind modul de utilizare al acestor echipamente. Angajații Versus Project trebuie să respecte cerințele de securitate impuse la nivelul Versus Project prin intermediul prezentei politici.

În mod particular, angajații care au acces la Datele cu Caracter Personal în desfășurarea activităților lor trebuie să respecte următoarele obligații principale:

i. să prelucreze Date cu Caracter Personal și să acceseze documente / fișiere ce conțin Date cu Caracter Personal doar dacă este necesar și numai pentru îndeplinirea atribuțiilor specifice de serviciu;
ii. să nu acceseze mai multe informații decât este strict necesar pentru îndeplinirea sarcinilor de serviciu;
iii. să utilizeze parole pentru acest acces, parole ce au minimum opt caractere și conțin cel puțin o literă mare și cel puțin o cifră sau un simbol. Parolele trebuie schimbate periodic. Angajații trebuie să își protejeze în permanență parolele și să nu le comunice la nici o persoană din cadrul Versus Project sau din afara acesteia;
iv. să nu permită accesul la computere și terminale de acces persoanelor neautorizate;
v. să blocheze ecranul computerelor și terminalelor de acces atunci când se îndepărtează de ele (de ex., când pleacă la o întâlnire, în pauza de masă, etc.);
vi. să nu lase laptopurile / echipamentele portabile / dosarele conținând Date cu Caracter Personal nesupravegheate și să nu ia acasă documente conținând Date cu Caracter Personal. În cazurile absolut excepționale documente pot fi luate acasă sub condiția de a le stoca în condiții de securitate;
vii. să nu utilizeze programe software care provin din surse externe, neverificate în prealabil de către responsabilul IT contractat de Versus Project;
viii. să utilizeze sistemele de salvare a documentelor puse la dispoziție de Versus Project pentru salvarea documentelor;
ix. să nu printeze documente sau fișiere ce conțin Date cu Caracter Personal decât atunci când este strict necesar în contextul realizării atribuțiilor de serviciu;
x. să lase biroul curat la sfârșitul programului de lucru, precum și în momentele în care lipsesc de la birou o durată mai lungă de timp (de ex., când pleacă în concediu);
xi. să nu lase documente conținând Date cu Caracter Personal pe birou sau pe stațiile de lucru când există posibilitatea accesului neautorizat;
xii. să respecte cerințele de securitate pentru protecția datelor stabilire prin politicile sau instrucțiunile Versus Project;
xiii. să participe la sesiunile de training privind cerințele în domeniul protecției datelor cu caracter personal organizate periodic de către Versus Project;
xiv. să respecte orice alte obligații stabilite de Versus Project prin proceduri interne și instrucțiuni de lucru în scopul protejării Datelor cu Caracter Personal.

Versus Project poate monitoriza modul în care sunt utilizate Echipamentele Tehnice, cu respectarea cerințelor legale și ale prevederilor prezentei Politici. Versus Project are dreptul de a solicita angajatului în orice moment să predea Echipamentul Tehnic pus la dispoziția acestuia, cu condiția furnizării unor echipamente înlocuitoare în măsura în care acest lucru este necesar pentru ca angajatul să își desfășoare activitatea în condiții normale. Angajații nu trebuie să utilizeze Echipamentul Tehnic pentru scopuri personale. Dacă totuși un angajat folosește respectivul Echipament Tehnic în scopuri personale, regulile din prezenta Politică se vor aplica respectivei utilizări. Astfel, angajatul care folosește Echipamentul Tehnic în scop personal, își asumă posibilitatea ca Versus Project să acceseze inclusiv conținutul generat într-un asemenea

mod. În toate cazurile, Versus Project va respecta regulile de confidențialitate atunci când va constata că respectivele comunicări sunt personale și nu au legătură cu scopul urmărit de eventuala accesare.

D. Gestionarea accesului la Echipamentele Tehnice

1. Procedura de acces

Regulile din prezentul capitol se aplică în măsura în care Versus Project a primit o sesizare rezonabilă, în orice modalitate, privind posibile neconformități, precum și în alte situații în care există indicii privind o asemenea posibilă neconformitate. Persoana care face sesizarea poate să aleagă să-și lase numele sau nu. Fiecare situație este analizată de către Administratorului din cadrul CPAG. Administratorul începe analiza faptelor raportate și colectează date în privința acestora.

În măsura în care Administratorul, pe baza informațiilor colectate:

- consideră că alerta reprezintă o preocupare substanțială, conform celor explicate la secțiunea C.2. de mai jos;
- crede că există o necesitate de a continua investigația, și
- consideră că pentru o derulare eficientă a respectivei investigații, accesul la mesajele e-mail și/sau la Fișierele Echipamentului Tehnic ale Angajatului Vizat este necesar,

Administratorul trimite o solicitare către persoana desemnată de compania contractată pentru servicii profesionale de întreţinere proactivă, mentenanță şi remediere situaţii pentru echipamentele de calcul şi comunicaţie - Responsabilul de IT („**Responsabilul de Securitate**”) pentru accesarea mesajelor e-mail și/sau a Fișierelor Echipamentului Tehnic ale Angajatului Vizat. Această solicitare va cuprinde:

- instrucțiuni către Responsabilul de Securitate de accesare a mesajelor e-mail și/sau a Fișierelor Echipamentului Tehnic ale Angajatului Vizat, după caz;
- instrucțiuni către Responsabilul de Securitate cu privire la condițiile de acces;
- datele de contact ale persoanelor care derulează investigația („**Investigatori**”), către care Responsabilul de Securitate va trebui să trimită rezultatele accesării mesajelor e-mail și/sau a Fișierelor Echipamentului Tehnic.

Instrucțiunile date de Administratorul /Responsabilul de Securitate cu privire la condițiile de acces pot include, de exemplu, următoarele:

- filtrarea mesajelor e-mail pe baza unor anumite cuvinte-cheie într-un anumit interval de timp;
- verificarea dacă Angajatul Vizat a trimis sau a primit un mesaj e-mail din partea unei anumite adrese e-mail într-un anumit interval de timp;
- accesarea conținutului mesajelor e-mail ale Angajatului Vizat trimise sau primite într-un anumit interval de timp pentru a verifica o anumită informație.

Investigatorii către care Responsabilul de Securitate trimite informațiile potrivit acestei secțiuni au responsabilitatea păstrării confidențialității și aplicării regulilor privind protecția datelor. E posibil ca acești Investigatori să fie angajați ai Versus Project sau experți terți și/sau companii de consultanță juridică care derulează astfel de investigații potrivit instrucțiunilor date de Versus Project și bazate de aranjamentele contractuale dintre ei și Versus Project.

Administratorul poate da instrucțiuni către Responsabilul de Securitate de accesare a mesajelor e-mail și/sau a Fișierelor Echipamentului Tehnic ale Angajatului Vizat și în următoarele situații:

- în cazuri de preocupare substanțială, așa cum se detaliază în secțiunea C.2. de mai jos, și
- când acest lucru este necesar potrivit legislației aplicabile cu respectarea condițiilor și a limitelor prescrise de respectiva legislație.

2. Motive de acces

Accesul la mesajele e-mail și/sau la Fișierele Echipamentului Tehnic ale Angajatului Vizat este permis doar dacă există o **preocupare substanțială**, așa cum aceasta este determinată de către Administratorul.

Respectiva „preocupare substanțială" este determinată de Administratorul de la caz la caz, dar trebuie să se încadreze în limitele drepturilor și obligațiilor prevăzute de Codul Muncii și legislația de muncă, inclusiv în următoarele cazuri:

- încălcări posibile sau concretizate ale legislației de către Angajatul Vizat;
- încălcări posibile sau concretizate ale regulilor interne ale Versus Project și/sau ale altor reguli aplicabile de către Angajatul Vizat;
- funcționarea defectuoasă a Echipamentului Tehnic;
- riscuri de securitate, inclusiv atacuri cibernetice;
- solicitări de informații primite de la autorități publice, în limita competențelor legale ale acestora.

3. Notificarea angajatului

Versus Project informează toți angajații cu privire la modul în care Datele lor cu Caracter Personal sunt prelucrate la semnarea contractului de muncă, inclusiv cu privire la prelucrarea Datelor cu Caracter Personal în contextul acestei Politici.

Angajatul Vizat ale cărui date din Echipamentul Tehnic urmează a fi accesate trebuie să fie notificat cu privire la accesarea intenționată. Respectiva notificare va face trimitere la informația minimă cerută de regulile aplicabile de protecția datelor comunicată anterior Angajatului și va include precizarea că Angajatul Vizat poate adresa orice întrebări sau obiecțiuni către Administrator.

4. Verificarea datelor

De fiecare dată când este posibil, accesul la datele de pe Echipamentul Tehnic trebuie limitat la analiza Datelor de Trafic. Accesarea conținutului este permisă doar atunci când este improbabil ca Datele de Trafic să ofere clarificările necesare sau să rezolve preocuparea substanțială care a dat naștere nevoii de acces.

Se va încerca să se limiteze dezvăluirea comunicărilor și documentelor, de exemplu prin pre-selectarea conținutului care poate fi de interes dintr-o revizuire inițială a numelor de fișiere.

Accesul va fi restricționat doar pentru perioada de timp necesară pentru a atinge scopul accesării.

Realizarea accesului către și analiza Datelor din Echipamentul Tehnic de către Responsabilul de Securitate și, respectiv, de către Investigatori se vor face de un personal restricționat la minimul absolut.

5. Păstrarea datelor

Rapoarte derivând din investigații, inclusiv Datele din Echipamentul Tehnic colectate, vor fi distribuite pe baza principiului necesității, marcate drept „Confidențial" și păstrate în concordanță cu politicile interne ale Versus Project și cu cerințele legale. Datele stocate trebuie să beneficieze de o găzduire sigură.

În cazul unei investigații care duce la confirmarea unei asemenea preocupări substanțiale, Datele din Echipamentul Tehnic colectate în acest context vor fi păstrate atât timp cât este necesar în vederea atingerii scopurilor avute în vedere de investigație, precum și ulterior dacă este necesar pentru alte scopuri sau potrivit legislației și regulilor interne aplicabile, așa cum se menționează mai sus.

E. Reguli specifice

Atunci când un angajat este absent (inclusiv în perioada călătoriilor de serviciu, concediului anual, concediului medical sau în perioada oricărui alt tip de concediu) sau părăsește Versus Project („**Angajat Absent**"), un manager al Versus Project aflat pe o poziție de management superioară față de cea în care se găsește Angajatul Absent (sau se găsea, în situația foștilor angajați) în cadrul Versus Project („**Solicitant**") poate solicita accesul către mesajele de e-mail ale Angajatului Absent pentru o perioadă limitată de timp. Solicitarea este trimisă către Responsabilul de Securitate și Administrator. Responsabilul de resurse umane este cel care aprobă solicitarea de acces. Perioada limitată de acces nu va depăși, de regulă, trei (3) luni.