



Prezentul Act Adițional privind Procesarea Datelor se încheie de către și între:

Transics International BV/SRL, cu sediul social la Ter Waarde 91, 8900 Ieper, Belgia, nr. TVA BE 0881.300.923 RPR/RPM Gent,

(Denumită în continuare „**Transics**” sau „**Procesator**”),

și

, cu sediul social la ,
(Denumită în continuare „**Client**” sau „**Controlor**”);

Controlorul și Procesatorul sunt denumiți în continuare, în mod colectiv, „**Părțile**” și individual „**Partea**”.

Întrucât Transics îi furnizează Clientului servicii de management al flotei și alte servicii conexe („**Serviciile**”), astfel cum sunt descrise în Contractul de Prestări Servicii și/sau comenzile de lucru (în continuare, „**Contractul de Prestări Servicii**”) încheiat între Transics și Client.

Întrucât, în măsura în care prestarea Serviciilor impune schimbul și procesarea de Date Personale între Părți, respectiv Părțile doresc să stabilească termenii și condițiile în care pot primi, accesa și procesa ulterior Date Personale de la cealaltă Parte dacă, și în măsura în care, Transics procesează Date Personale în calitate de Procesator în numele Clientului în legătură cu Serviciile furnizate Clientului de către Transics în baza Contractului de Prestări Servicii.

PRIN PREZENTA, PĂRȚILE SUNT DE ACORD CU URMĂTOARELE:

1. Definiții

1. Termenii definiți în Contractul de Prestări Servicii între Procesator și Controlor vor avea același înțeles atunci când sunt folosiți în prezentul Act Adițional privind Procesarea Datelor („**Actul Adițional**”).

2. În accepțiunea prezentului Act Adițional, „**Date Personale**”, „**Categorii speciale de date**”, „**Proces / procesare**”, „**Controlor**” (sau „**Controlor de date**”), „**Procesator**” (sau „**Procesator de date**”), „**Subcontractant**”, „**Persoană vizată**” și „**Încălcarea securității datelor personale**” vor avea același înțeles cu cel enunțat în Legile aplicabile privind Protecția Datelor.

3. „**Legile privind Protecția Datelor**” înseamnă Regulamentul General privind Protecția Datelor 2016/679 („**GDPR**”) și de completare a prevederilor legislației naționale din statele membre ale SEE, Directiva UE 2002/58/CE din 12 iulie 2002 privind procesarea Datelor Personale și protejarea confidențialității în sectorul comunicațiilor electronice, astfel cum este transpusă în legile naționale ale statelor membre ale SEE, astfel cum poate fi modificată, abrogată, înlocuită sau completată la anumite intervale de timp, precum și orice alte legi sau regulamente privind protecția datelor și confidențialitatea, care se aplică Datelor Personale controlate de fiecare Parte.

2. Obiect și Durată

Prezentul Act Adițional se va aplica oricărei colectări, utilizării, partajării și procesării ulterioare de Date Personale de către Transics dacă, și în măsura în care, Transics procesează Date Personale în calitate de Procesator, în numele Clientului, în legătură cu Serviciile furnizate Clientului de către Transics în baza Contractului de Prestări Servicii.

Prezentul Act Adițional înlocuiește, fără să anuleze niciun acord anterior încheiat de Părți în aspectele acestora care se referă la procesarea Datelor Personale, inclusiv, dar fără limitare la, orice Acord privind Procesarea Datelor.

Prezentul Act Adițional este parte integrantă a Contractului de Prestări Servicii aferent. Prezentul Act Adițional va fi considerat a produce efecte începând cu data semnării și va continua să fie în vigoare și să producă efecte depline până la încetarea Contractului de Prestări Servicii.

3. Obiect

Părțile, în calitate avută de fiecare, vor procesa Datele Personale în conformitate cu Legea aplicabilă privind Protecția Datelor, Legea aplicabilă privind confidențialitatea și

comunicațiile electronice, GDPR din 25 mai 2018, și orice alt regulament aplicabil sub incidența căruia intră Controlorul și/sau Procesatorul.

Tip de date

Controlorul a precizat că următoarele categorii de date vor fi colectate, procesate și utilizate de către Procesator în baza prezentului Act Adițional:

Datele Personale prezentate, stocate, trimise sau primite de către Client sau utilizatorii săi finali prin intermediul Soluției de Management al Flotei, care pot include:

- Numele, funcția, numărul permisului de conducere, calificarea, datele de intrare / ieșire din serviciu, data expirării certificatului medical
- Adresele profesionale, comerciale sau de serviciu
- Data / anul / data nașterii
- Date privind telecomunicațiile (de exemplu: conexiune, locație, utilizare și date cu privire la trafic)
- Număr de telefon, număr de telefon mobil
- Adresă de e-mail
- Date tahograf (ore de condus, repaus, lucru)
- Mesaje
- Adrese IP
- Date eco
- Date de planificare și control
- Date de localizare exactă (poziții GPS)
- Plăcuța de înmatriculare camion și remorcă
- Date de diagnosticare aferente dispozitivului și serviciului
- Fotografia
- Sexul
- Rolul (șofer / vizitator / dispecer / administrator)
- Limba utilizată de șofer
- Cardul tahografic: ID
- Cardul tahografic: Țara de emisie
- Activități (circulație, staționare, odihnă etc.)
- Alarmer
- Data ultimei citiri a tahografului
- Performanța / tendință ECO: Ralanti, Turație mare, Supravitează, Rulare liberă, Frânare puternică, Viteză de croazieră, consum mediu de combustibil
- Integrarea datelor TrackKing pentru remorcă (Thermo King): temperatura zonelor, starea ușii, presiunea în anvelope, alarme
- Datele FMS (sisteme de management flotă) ale vehiculului / Date privind utilizarea vehiculului, precum: distanța parcursă, momentul din zi, durata condusului, viteza vehiculului, turația motorului, sarcina motorului, temperatura motorului, manevre de frânare / virare / accelerare, durata deplasării și distanța, tensiunea bateriei
- Datele de utilizare ale trailerului, precum: distanța parcursă, ora, durata călătoriei, viteza trailerului, încărcătura trailerului, frânarea (EBS) / distanța, sistemul de măsurare presiune în pneuri, sistemul electronic de monitorizare a randamentului de frânare, sistemul de navigație prin satelit
- Înregistrare video (activarea trebuie efectuată de client)

Categorii de Persoane vizate

Controlorul a definit următoarele categorii de Persoane vizate ale căror Date Personale, astfel cum sunt definite mai sus, vor fi colectate, procesate și utilizate de către Procesator în baza prezentului Acord privind Procesarea Datelor:

- angajații Clientului;
- contractanții Clientului;
- personalul clienților, furnizorilor și subcontractanților Clientului;
- orice altă persoană care transmite date prin intermediul Soluției de Management al Flotei, inclusiv persoanele care colaborează și comunică cu utilizatorii finali ai Clientului.

Păstrarea datelor

Procesatorul nu va păstra Datele Personale într-o formă care permite identificarea Persoanelor vizate mai mult timp decât este necesar în scopurile pentru care prelucrează Datele

Personale prin intermediul FMS a Transics, dacă nu se impune sau permite altceva în baza Legilor privind Protecția Datelor sau a altor regulamente aplicabile. Clientul solicită în mod expres Transics să stabilească perioada de păstrare la 1 an, pentru a garanta disponibilitatea tuturor datelor Clientului, în orice moment. După această perioadă, Transics are opțiunea de a șterge aceste Date cu caracter personal sau de a le face inaccesibile. Înainte de expirarea acestei perioade, Clientul trebuie să exporte toate datele necesare prin intermediul instrumentelor Transics. Transics nu are obligația de a șterge copiile Datelor cu caracter personal, care sunt păstrate în copii de rezervă realizate automat generate de Transics și care vor fi păstrate pe perioada maximă pentru asigurarea continuității, dar vor fi șterse în termen de 14 luni de la data creării. Aceste copii de rezervă realizate automat vor continua să fie supuse prezentului Act adițional de prelucrare a datelor și Acordului până când sunt distruse. Fără a aduce atingere dreptului Controlorului prevăzut la articolul 4.i de mai jos, Transics are dreptul să anonimizeze Datele Personale colectate, generate și/sau stocate în cadrul furnizării Serviciilor și să utilizeze ulterior datele astfel anonimizate în scopuri statistice, analitice, comerciale și de referință.

4. Obligațiile Procesatorului

Atunci când Transics (acționând în calitate de Procesator) procesează Date Personale în numele Clientului (acționând în calitate de Controlor de date), acesta:

- a. Va procesa sau va solicita procesarea Datelor Personale în conformitate cu Legile privind Protecția Datelor aplicabile acestuia în calitate de Procesator de date.
 - b. Va procesa – și se va asigura că orice persoană care acționează sub autoritatea sa procesează – Date Personale în numele Controlorului și în conformitate cu instrucțiunile documentate ale acestuia, cu excepția cazului în care i se impune să facă acest lucru de legislația Uniunii sau a statului membru al UE sub incidența căreia se află Procesatorul. Într-un astfel de caz, Procesatorul va informa Controlorul cu privire la acea cerință legală înainte de procesare, exceptând cazul în care legislația interzice această informare din motive importante de interes public. Prezentul Act adițional reprezintă instrucțiunile documentate transmise de Operatorul de date Persoanei împuternicite de operator. La solicitarea Controlorului, Procesatorul va și corecta, rectifică sau bloca Datele Personale și se va asigura că doar personalul instruit corespunzător are acces la Datele Personale.
 - c. Ținând cont de natura procesării și de informațiile de care dispune Procesatorul, îi va asista pe Controlor în asigurarea respectării obligațiilor care îi revin în conformitate cu Legislația aplicabilă privind Protecția Datelor, inclusiv cu efectuarea oricăror evaluări necesare privind impactul asupra vieții private.
 - d. Va pune în aplicare măsuri tehnice și organizatorice adecvate, în conformitate cu Legislația aplicabilă privind Protecția Datelor, pentru a proteja Datele Personale împotriva distrugerii accidentale sau ilicite sau a pierderii accidentale, modificării, accesului neautorizat, divulgării sau transferului, utilizării abuzive și împotriva oricăror alte forme ilegale de procesare, precum și cel puțin următoarele măsuri de securitate:
 - i. Pseudonimizarea și criptarea Datelor Personale;
 - ii. Capacitatea de a asigura, în mod continuu, confidențialitatea, integritatea, disponibilitatea și reziliența sistemelor și serviciilor de procesare;
 - iii. Capacitatea de a restabili disponibilitatea și accesul în timp util la Datele Personale în cazul unui incident fizic sau tehnic;
 - iv. Un proces de testare, măsurare și evaluare periodică a eficacității măsurilor tehnice și organizatorice pentru asigurarea securității procesării.
- În conformitate cu Anexa 1, Procesatorul documentează implementarea măsurilor tehnice și organizatorice.
- e. Va pune la dispoziția Controlorului toate informațiile necesare pentru a demonstra conformitatea cu obligațiile Procesatorului de a respecta Legislația



aplicabilă privind Protecția Datelor și de a permite și de a contribui la audituri, inclusiv inspecții, efectuate de Controlor sau de un alt auditor mandatat de către Controlor. Dreptul la audit al Controlorului va fi condiționat de transmiterea unei notificări în scris Procesatorului, cu cel puțin patru (4) săptămâni în prealabil, privind orice astfel de audit.

- f. În ceea ce privește punctul (e) de mai sus, va notifica imediat Controlorul dacă este de părere că o instrucțiune primită de la Controlor încalcă Legile privind Protecția Datelor.
- g. Având în vedere natura procesării și informațiile de care dispune, va asista Controlorul cu măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației Controlorului de a furniza informații cu privire la colectarea, procesarea sau utilizarea Datelor Personale unei Persoane vizate și va răspunde solicitărilor de exercitare a drepturilor Persoanei vizate. Orice solicitare din partea unei Persoane vizate, adresată direct Procesatorului, trebuie să fie direcționată către Controlor.
- h. Fără întârzieri nejustificate, va informa Controlorul despre încălcarea securității Datelor Personale care afectează Datele Personale procesate de către Procesator și, ținând cont de natura procesării și de informațiile pe care le are la dispoziție, îl va asista pe Controlor, în măsura în care este posibil, să își îndeplinească obligațiile, dacă va surveni o încălcare a securității Datelor Personale.
- i. La alegerea Controlorului, va șterge sau va returna Controlorului toate Datele Personale după terminarea furnizării serviciilor legate de procesare și va șterge copiile existente, cu excepția cazului în care legislația Uniunii sau a statelor membre impune stocarea Datelor Personale. Dacă, după 3 luni de la încetarea Serviciilor, nu au fost trimise opțiuni sau instrucțiuni, Transics nu va mai permite accesul la Datele cu caracter personal sau le va șterge. Clientul va trebui să exporte datele necesare prin intermediul instrumentelor Transics în termen de 3 luni de la încetarea Serviciilor.
- j. Se va asigura că persoanele (de exemplu: angajații) autorizate să proceseze Datele Personale s-au angajat să păstreze confidențialitatea sau se află sub incidența unei obligații legale adecvate de confidențialitate.
- k. Fără a aduce atingere obligației Controlorului prevăzută la articolul 6.4 de mai jos, va păstra o evidență a tuturor categoriilor de activități de procesare efectuate în numele Controlorului în conformitate cu GDPR.

Procesatorul are dreptul să solicite remunerație pentru asistența oferită Controlorului, care depășește ceea ce este impus de Legile privind Protecția Datelor și de prezentul Act Adițional privind Protecția Datelor.

5. Subcontractarea procesării

- Prin intermediul prezentului Act Adițional, Controlorul oferă Procesatorului o autorizație scrisă generală în vederea angajării unui alt procesator pentru procesarea totală sau parțială în baza prezentului Act Adițional.
- Se convine că orice Subcontractant enumerat în Anexa 2 este autorizat în mod expres.
- Procesatorul va informa Controlorul cu privire la orice modificări intenționate în ceea ce privește adăugarea sau înlocuirea altor procesatori, oferind astfel Controlorului posibilitatea de a se opune unor astfel de modificări. În cazul în care Controlorul are motive substanțiale și legitime de a se opune Subcontractantului specific și notifică în scris Procesatorului aceste obiectii în cel mai scurt timp posibil după primirea notificării Procesatorului privind un astfel de Subcontractant.
- În cazul în care, cu aprobarea generală a Controlorului, așa cum se prevede mai sus, Transics face orice aranjament sau are în vedere solicitarea ca orice Date Personale deținute în temeiul acestui Act Adițional să fie transferate și procesate de un Subcontractant, se vor aplica următoarele condiții:
 - Transics va face acest lucru numai printr-un acord scris

cu Subcontractantul care impune Subcontractantului aceleași obligații impuse Procesatorului în baza prezentului Act Adițional, în special obligația de a implementa măsuri tehnice și organizatorice adecvate, astfel încât procesarea să îndeplinească cerințele relevante în conformitate cu Legile aplicabile privind Protecția Datelor.

- b) În cazul în care orice Date Personale sunt sau vor fi transferate în afara SEE într-o țară care nu prezintă un nivel adecvat de protecție a datelor, Clauzele contractuale standard ale UE pentru Procesatori vor fi încheiate între Subcontractant și Controlor (după caz, cu Transics care acționează în numele Controlorului) sau vor fi puse în aplicare orice alte mecanisme adecvate de transfer al datelor în conformitate cu Legile aplicabile privind Protecția Datelor; iar Clientul autorizează în mod expres Transics să încheie, în numele Clientului, Clauze contractuale standard cu Subcontractanții enumerați în Anexele relevante.
- c) În cazul în care Subcontractantul nu își îndeplinește obligațiile de protecție a datelor în baza unui astfel de acord scris, Procesatorul va rămâne pe deplin răspunzător față de Controlor pentru îndeplinirea obligațiilor Subcontractantului, sub rezerva limitelor de răspundere convenite în prezentul Act Adițional.

6. Obligațiile Controlorului

- Controlorul stabilește scopurile și mijloacele de procesare a Datelor Personale prin intermediul FMS a Transics.
- Controlorul garantează că:
 - Procesatorul obține permisiunea să folosească Datele Personale în scopul procesării în modul stabilit în Actul Adițional privind Procesarea Datelor.
 - Datele Personale au fost colectate și procesate în mod legal în conformitate cu Legile privind Protecția Datelor.
 - Respectarea Legilor aplicabile privind Protecția Datelor este garantată atunci când Controlorul transferă Date Personale către Procesator pentru a respecta prezentul Act Adițional privind Procesarea Datelor și când oferă instrucțiuni Procesatorului privind procesarea Datelor Personale.
- Controlorul trebuie să se asigure că datele sunt procesate într-o manieră care asigură o securitate adecvată, inclusiv protecție împotriva procesării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, utilizând măsuri tehnice sau organizatorice adecvate.
- Controlorul va ține o evidență a activităților de procesare aflate sub responsabilitatea sa, în conformitate cu GDPR în care FMS a Transics ar trebui să fie acoperită.

7. Cesiune

Procesatorul nu își va cesiona obligațiile în baza prezentului Act Adițional privind Procesarea Datelor fără consimțământul scris prealabil al Controlorului, cu excepția cesiunii către o filială sau o societate afiliată, care face parte din grupul ZF, caz în care nu este necesar consimțământul prealabil în scris al Controlorului. În cazul în care Procesatorul cesionează prezentul Act Adițional privind Procesarea Datelor cu consimțământul Controlorului, el va face acest lucru numai prin intermediul unui acord scris cu cesionarul, care impune cesionarului aceleași obligații care îi sunt impuse Procesatorului în baza prezentului Act Adițional de procesare a datelor.

8. Răspundere

Răspunderea Părților respective una față de cealaltă pentru încălcarea prezentului Act Adițional și obligația de despăgubire pe care o au una față de cealaltă pentru revendicările făcute de terți împotriva unei Părți din cauza unei încălcări contractuale sau necontractuale a prezentului Act Adițional sau a Legilor privind protecția datelor de către cealaltă Parte, vor fi reglementate de termenii de răspundere și de despăgubire prevăzuți în Contractul de Prestări Servicii încheiat între Transics și Client cu privire la Serviciile relevante.

9. Legislația aplicabilă și jurisdicția

Prezentul Act Adițional privind guvernarea datelor intră sub incidența legislației care reglementează Contractul relevant de Prestări Servicii (cu excepția situației în care această alegere a legislației nu ar fi valabilă conform legislației aplicabile a țării în care este înființat Controlorul relevant, caz în care legislația

aleasă va fi cea din țara în care este înființat Controlorul relevant).

Jurisdicția competentă pentru orice litigii contractuale sau necontractuale care decurg din sau în legătură cu prezentul Act Adițional este aceeași cu cea convenită în Contractul relevant de Prestări Servicii. Cu toate acestea, acest paragraf nu afectează niciuna dintre obligațiile respective ale Părților în temeiul Legilor aplicabile privind Protecția Datelor.

CONVENIT de către Părți prin intermediul reprezentanților lor autorizați în mod legal, la data la care ambele Părți au semnat prezentul Act Adițional privind prelucrarea datelor.

Pentru și în numele:

Transics

Num: Michael Serisé
Funcția: Șef unitate DCS

Client

Num: _____
Funcția: _____
Data: _____



Anexa 1: Măsurile tehnice și operaționale

Prezenta Anexă se adresează clienților și partenerilor de afaceri și definește măsurile tehnice și organizatorice pentru protejarea Datelor Personale împotriva accesului neautorizat, corupției și pierderii, în conformitate cu Legile privind Protecția Datelor.

Acest document oferă detalii suplimentare cu privire la măsurile tehnice și organizatorice implementate de către Procesator în scopul protecției datelor.

SECURITATEA CENTRULUI DE DATE & REȚELE

Centrul de date utilizat de către Transics este un centru de date de nivel 3:

- **SLA pentru disponibilitatea energiei electrice – 100%**
- **SLA pentru temperatură**
Țintă: Menținerea temperaturii în camera calculatoarelor la o temperatură sursă de 18 grade C până la 27 grade C în mod continuu, sub rezerva unei temperaturi exterioare mai mici de 40 grade C și în conformitate cu Orientările ASHRAE.
- **SLA pentru umiditate**
Țintă: Menținerea umidității camerei calculatoarelor între 40% și 60%
- **Unitate**
Soluții de înaltă densitate disponibile
24 x 7 x 365 funcționare a construcției
planșeu supraînălțat de 800 mm cu 3,5 metri până la partea inferioară a plafonului fals
Stație de livrare acoperită, prevăzută cu platformă de nivel și magazine securizate
Sarcină planșeu 12KN pe metru pătrat
- **Energie electrică**
Puncte de alimentare dublă
N+1 generatoare
2N UPS
- **Securitate**
Securitate la amplasament 24 x 7
Citițoare de card și biometrie
Barieră de oprire cu trapă
Gard de împrejurire a perimetrului de 3 m
CCTV intern și extern – 90 de zile de înregistrare
- **Conformitate / Certificări**
Centru de date certificat pentru nivelul 3 de către Uptime Institute
Conform ISO27001, PCIDSS, certificat BREEAM
Standardele și Orientările ASHRAE pentru Centre de date
- **Răcire**
Soluție adiatică indirectă cu aer exterior
Nu este necesară răcire mecanică convențională
Absență apă în spațiul alb al centrului de date

INCINTELE TRANSICS

1. Controlul accesului (clădire / birouri / centru de date)

Procesatorul a implementat, dar fără a se limita la, următoarele măsuri pentru a împiedica accesul neautorizat la sistemele de procesare a datelor în care sunt procesate Datele Personale:

- Angajații au un card personal/o cheie pentru acces în clădire.
- Persoanele neautorizate vor fi împiedicate să obțină acces fizic în incintele, clădirile sau camerele în care se găsesc sisteme de procesare a datelor, care procesează și/sau utilizează Date Personale.

2. Controlul accesului (sisteme)

Procesatorul a implementat, dar fără a se limita la, următoarele măsuri pentru a împiedica utilizarea sistemelor de procesare a datelor de către persoane neautorizate:

- Sistemele informatice la nivelul întregii întreprinderi sunt monitorizate continuu 24x7, 365 zile / an de către echipa IT a Transics.
- Angajații au fiecare un terminal individual cu identificare personală și parolă.
- Există o temporizare automată a terminalului utilizatorului atunci când acesta este inactiv. Sunt necesare identificarea și parola pentru redeschidere.
- Dezactivarea automată a ID-ului de utilizator atunci când parola este introdusă greșit de mai multe ori, fișier de înregistrare a evenimentelor (monitorizarea tentativelor de efracție).
- Toți angajații se află sub incidența unor acorduri de nedivulgare și confidențialitate. Orice acces la date fără caracter public este oferit strict în funcție de necesitatea de cunoaștere și monitorizat. Există un proces de educare continuă a utilizatorilor privind importanța securității datelor în activitatea profesională.
- Accesul la sistemele de producție se face prin intermediul autentificării multi-factor.
- Transics are acces conform domeniului funcțional de responsabilitate, și anume echipa de cercetare și dezvoltare, echipa de găzduire, echipa biroului de asistență ... Accesul este bazat pe funcție și include revizuirii regulate ale membrilor grupului.

3. Controlul accesului (date)

Procesatorul a implementat, dar fără a se limita la, următoarele măsuri pentru a se asigura că utilizatorii autorizați ai unui sistem de procesare a datelor pot accesa numai datele pentru care sunt autorizați și pentru a împiedica citirea Datelor Personale cât timp datele sunt în utilizare, în mișcare sau în repaus fără autorizație:

- Conexiunile clientului sunt realizate prin autentificare multi-factor.
- Portal central de conectare cu acces securizat la aplicațiile clientului, bazat pe principiul „autentificare unică”, ce poate fi combinat cu autentificarea „cu doi factori”.

4. Controlul transferului

Procesatorul a implementat, dar fără a se limita la, următoarele măsuri pentru a se asigura că Datele Personale nu pot fi citite, copiate sau modificate în timpul transmiterii electronice sau în timpul transportului sau stocării pe disc. În plus, pentru a controla și a stabili către ce organisme este permis transferul Datelor Personale furnizate de echipamentele de comunicații de date:

- Toate interacțiunile clienților pe Internet se fac prin conexiuni securizate SSL- / TLS
- Toate conexiunile la baza de date sunt criptate
- Copiile de siguranță și datele în repaus sunt criptate

5. Controlul intrării

Procesatorul a implementat, dar fără a se limita la, următoarele măsuri pentru a se asigura că este posibil să se garanteze, să se controleze ulterior și să se stabilească dacă și de către cine au fost introduse, modificate sau eliminate Datele Personale de pe sistemele de procesare a datelor:

- o politică de autorizare pentru introducerea datelor în memorie, precum și pentru citirea, modificarea și ștergerea datelor stocate;
- autentificarea personalului autorizat;
- măsuri de protecție pentru introducerea datelor în memorie, precum și pentru citirea, modificarea și ștergerea datelor stocate;
- utilizarea codurilor de utilizator (parole);
- urmarea unei politici conform căreia toți angajații Transics, care au acces la Datele Personale procesate pentru Client, își vor reseta parolele minim o dată într-o perioadă de 90 de zile;
- asigurarea faptului că intrările în unitățile de procesare a datelor (camerele care conțin hardware pentru calculatoare și echipamentele aferente) pot fi încuiate;

- deconectarea automată a ID-urilor de utilizator care nu au fost folosite pentru o perioadă substanțială de timp.

6. Controlul comenzilor

Procesatorul a implementat, dar fără a se limita la, următoarele măsuri pentru a se asigura că Datele Personale care sunt procesate la cererea proprietarului datelor de către un procesator de date vor fi procesate numai conform instrucțiunilor date de proprietarul datelor:

Proprietarul datelor are în orice moment dreptul să controleze executarea corectă a tuturor lucrărilor comandate de el. Transics va furniza Clientului informații adecvate privind lucrările realizate.

7. Controlul disponibilității

Procesatorul a implementat, dar fără a se limita la, următoarele măsuri pentru a se asigura că Datele Personale sunt protejate împotriva distrugerii sau pierderii accidentale:

Vezi secțiunea „Centru de date”.

8. Procesarea separată

Procesatorul a implementat, dar fără a se limita la, următoarele măsuri pentru a se asigura că datele colectate în scopuri diferite pot fi procesate separat:

- Accesul la date este separat prin securitatea aplicațiilor pentru utilizatorii corespunzători;
- Există medii separate pentru DEV, QA și PRODUȚIE;
- Mediul real și de testare sunt separate.

9. Responsabil cu protecția datelor

Procesatorul a desemnat un Responsabil cu protecția datelor (Data Protection Officer - DPO) în conformitate cu GDPR. Această persoană va asigura conformitatea cu GDPR și alte Legi privind Protecția Datelor. Vă rugăm să adresați orice întrebări DPO prin intermediul privacy.cvcscds@zf.com.

Anexa 2: Lista subcontractanților procesării

O imagine de ansamblu a listei actuale de Subprocesoare utilizate de Transics poate fi găsită prin următorul link:

<https://www.zf.com/legal/subprocessors>