POLITICA DE PRELUCRARE A DATELOR CU CARACTER PERSONAL LA LICEUL TEHNOLOGIC „DOMOKOS KAZMER” din localitatea Sovata

LICEUL TEHNOLOGIC „DOMOKOS KAZMER"
SOVATA
Cod SIRUES : 1161605 , RO-545500 – SOVATA
Jud. Mureş , Str. Principală Nr.54/B.
Tel : Fax: 0265-570219
e-mail : fvass@digicomm.ro

Cuprins

Liceul Tehnologic „Domokos Kazmer" , cu sediul in Sovata, str. Principala , nr. 54/b., jud. Mures, CF 4376025; cod CAEN 8532 -Domeniu de activitate, Invatamant, prelucreaza date cu caracter personal in conformitate cu REGULAMENTUL(UE) PARLAMENTULUI EUROPEAN SI AL CONSILIULUI nr.679 din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulament general privind protectia datelor).

I. NOTIUNI

In prezenta Politica de prelucrare a datelor cu caracter personal sunt utilizate urmatoarele notiuni:

- **GDPR** - REGULAMENTUL(UE) PARLAMENTULUI EUROPEAN SI AL CONSILIULUI nr.679 din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulament general privind protectia datelor);
- **date cu caracter personal** - orice informatie referitoare la o persoana fizica identificata sau identificabila (persoana vizata). Persoana identificabila este persoana care poate fi identificata, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identitatii sale fizice, fiziologice, psihice, economice, culturale sau sociale;
- **operator** – persoana fizica sau persoana juridica de drept public sau de drept privat, inclusiv autoritatea publica, orice alta institutie ori organizatie care, în mod individual sau impreună cu altele, stabileste scopurile si mijloacele de prelucrare a datelor cu caracter personal; atunci cand scopurile si mijloacele prelucrarii sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevazute in dreptul Uniunii sau in dreptul intern;

- **ofiter de protectie a datelor(DPO)** – specialist in protectia datelor al carui rol principal este acela de a coordona si supraveghea implementarea conditiilor de conformitate GDPR, precum si ca persoana de legatura intre organizatie si autoritatea de supraveghere.
- **mijloace de protectie a informatiei care contine date cu caracter personal** - mijloace tehnice, de program si tehnico-aplicative, sisteme si complexe de sisteme ce realizeaza algoritmi de conversie criptografica a informatiei care contine date cu caracter personal, destinate sa asigure integritatea si confidentialitatea informatiei in procesul de prelucrare, depozitare si transmitere a acesteia prin canalele de comunicatii;
- **perimetru de securitate** - zona care reprezinta in sine o bariera de trecere asigurata cu mijloace de control fizic si/sau tehnic al accesului;
- **utilizator** – persoana care actioneaza sub autoritatea detinatorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informationale de date cu caracter personal;
- **sesiune de lucru** — perioada care dureaza din momentul pornirii calculatorului si aplicatiei de utilizare a resursei informationale sau din momentul pornirii resursei informationale si pana la momentul opririi acestora;
- **prelucrarea datelor cu caracter personal** – orice operatiune sau serie de operatiuni care se efectueaza asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, inregistrarea, organizarea, stocarea, pastrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvaluirea prin transmitere, diseminare sau in orice alt mod, alaturarea ori combinarea, blocarea, stergerea sau distrugerea;
- **stocare** - pastrarea pe orice fel de suport a datelor cu caracter personal;
- **sistem de evidenta a datelor cu caracter personal** - orice structura organizata de date cu caracter personal, accesibila potrivit unor criterii determinate, indiferent dacă aceasta structura este organizata in mod centralizat ori descentralizat sau este repartizata dupa criterii functionale ori geografice;
- **restrictionarea prelucrarii –** inseamna marcarea datelor cu caracter personal stocate cu scopul de a limitata prelucrarea viitoare a acestora;
- **crearea de profiluri -** inseamna orice forma de prelucrare automata a datelor cu caracter personal care consta in utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoana fizica, in special

pentru a analiza sau prevedea aspecte privind performanta la locul de munca, situatia economica, sanatatea, preferintele personale, interesele, fiabilitatea, comportamentul, locul in care se afla persoana fizica respectiva sau deplasarile acesteia;

- **pseudonimizare** – inseamna prelucrarea datelor cu caracter personal intr-un asemenea mod incat acestea sa nu mai poata fi atribuie unei anume persoane vizate fara a se utiliza informatii suplimentare, cu conditia ca aceste informatii suplimentare sa fie stocate separat si sa faca obiectul unor masuri de natura tehnica si organizatorica care sa asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
- **persoana imputernicita de operator –** persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care prelucreaza datele cu caracter personal in numele operatorului;
- **destinatar –** persoana fizica sau juridica, autoritatea publica, agentia sau alt organism carora le sunt divulgate datele cu caracter personal, indiferent daca este sau nu o parte terta. Cu toate acestea, autoritatile publice carora li se pot comunica date cu caracter personal in cadrul unei anumite anchete in conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de catre autoritatile publice respective respecta normele aplicabile in materie de protectie a datelor, in conformitate cu scopurile prelucrarii;
- **parte terta –** persoana fizica sau juridica, autoritate publica, agentie sau organism altul decat persoana vizaata, operatorul, persoana imputernicita de operator si persoane care, sub directa autoritate a operatorului sau a persoanei imputernicite de operator, sunt autorizate sa prelucreze date cu caracter personal;
- **consimtamant al persoanei vizate –** inseamna orice manifestare de vointa libera, specifica, informata si lipsita de ambiguitate a persoanei vizate prin care aceasta accepta, printr-o declaratie sau printr-o actiune fara echivoc, ca datele cu caracter personal care o privesc sa fie prelucrate;
- **incalcarea securitatii datelor cu caracter personal –** inseamna o incalcare a securitatii care duce, in mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizata a datelor cu caracter personal transmise, stocate sau prelucrate intr-un alt mod, sau la accesul neautorizat la acestea;
- **date genetice –** inseamna datele cu caracter personal referitoare la caracteristicile genetice mostenite sau dobandite ale unei persoane fizice, care ofera

informatii unice privind fiziologia sau sanatatea persoanei respective si care rezulta in special in urma unei analize a unei mostre de material biologic recoltate de la persoana in cauza;

- **date biometrice –** date cu caracter personal care rezulta in urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirma identificarea unica a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;
- **date privind sanatatea –** date cu caracter personal legate de sanatatea fizica sau mentala a unei persoane fizice, inclusiv prestarea de servicii de asistenta medicala, care dezvaluie informatii despre starea de sanatate a acesteia;
- **autoritate de supraveghere –** inseamna o autoritate publica independenta instituita de un stat membru.

II. SCOPUL

2.1. Scopul acestei politici este de a stabili masurile necesare si responsabilitatile utilizatorilor **Liceul Tehnologic „Domokos Kazmer",** pentru indeplinirea obligatiilor referitoare la protejarea datelor cu caracter personal, in vederea utilizarii datelor personale, apartinand salariatilor, elevilor, prescolarilor,parintilor **Liceul Tehnologic „Domokos Kazmer",**

2.2. Colectarea si prelucrarea informatiei in vederea completarii contractelor de munca si transmiterea acestor date in Registrul General de Evidenta a Salariatilor – REVISAL -, completarii si transmiterii declaratiilor aferente activitatilor de salarizare catre ANAF, AJOFM si ITM, Inspectoratului Scolar Judetean,MEN, CJRAE si alte institutii pentru temei legal.

2.3. Colectarea si prelucrarea datelor apartinand salariatilor, elevilor, prescolarilor,parintilor

2.4. Colectarea si prelucrarea datelor apartinand salariatilor, elevilor, prescolarilor,parintilor nu vor fi utilizate pentru servicii de marketing si nu va fi destinata tertilor pentru alte scopuri decat cele prevazute la pct. 2.2. si 2.3.

III. CATEGORII DE DATE CU CARACTER PERSONAL PE CARE LICEUL TEHNOLOGIC „DOMOKOS KAZMER' LE PRELUCREAZA

3.1. In cadrul sistemului de evidenta a datelor cu caracter personal apartinand ***salariatilor*** sunt prelucrate urmatoarele:
de exemplu

- *nume si prenume;*
- *codul numeric personal;*
- *seria si nr CI si data eliberarii si emitentul, valabilitate CI;*
- *adresa de domiciliu, anul si locul nasterii;*
- *datele privind locul de munca si functia ocupata;*
- *adresa de corespondenta , numar de telefon si adresa de e-mail;*
- *marimea salariului brut si alte premii, sporuri, stimulente suplimente;*
- *calificare, diplome de studii, competente dobandite,stare civila*
- *numele, prenumele, CNP persoanelor care se afla la intretinerea persoanei respective(membrii familiei, alte rude si persoane, dupa caz);*
- *datele referitoare la starea de sanatate, date din certificatele de concediu medical acordate necesare pentru calcularea indemnizatiei corespunzatoare;*
- *cont bancar IBAN pentru virarea salariului,*
- *cont bancar IBAN pentru virarea burselor,*
- *marimea concreta a drepturilor salariale calculate, taxele si impozitele aferente, inclusiv contributiile de asigurari sociale obligatorii, si alte sume datorate in virtutea legii sau contractului individual de munca;*

3.2. In vederea deservirii salariatilor, elevilor, prescolarilor,parintilor sunt prelucrate urmatoarele tipuri de date cu caracter personal:

- *nume si prenume, CNP, serie si nr. CI,domiciliu,locul nasterii, emitent CI/BI, data emiterii, valabilitate CI/BI, anul si locul nasterii, stare civila;*
- *adresa de domiciliu, numar de telefon, adresa de e-mail;*
- *date venituri, salariale calculate, taxele si impozitele aferente, inclusiv contributiile de asigurari sociale obligatorii, si alte sume datorate in virtutea legii sau contractului individual de munca;*
- *calificative, note, date despre parinti*

IV. LOCATIA SI DESCRIEREA SISTEMULUI DE EVIDENTA

4.1. Datele cu caracter personal continute in sistemul de evidenta al salariatilor in cadrul **Liceul Tehnologic „Domokos Kazmer"**se prelucreaza/stocheaza:

- pe suport hartie;
- in format electronic;

4.2 Datele cu caracter personal continute in sistemul de evidenta al elevilor, prescolarilor,parintilor, salariatilor in cadrul **Liceul Tehnologic „Domokos Kazmer"**se prelucreaza/stocheaza in programul SIIIR -Sistemul Informatic Integrat al invatamantului din Romania:

4.3. Mentenanta programului de evidenta este efectuat de catre **Liceul Tehnologic „Domokos Kazmer"**, programul SIIIR este actualizat de catre Inspectoratul Scolar Judetean Mures si Siveco.

4.4. Mentenanta programului de salarizare este efectuat de catre **Liceul Tehnologic „Domokos Kazmer"**, programul Revisal este actualizat de catre Inspectia Muncii.

4.5 Mentenanta programului de salarizare este efectuat de catre **Liceul Tehnologic „Domokos Kazmer"**, programul Edusal este actualizat de catre Inspectoratul Scolar Judetean Mures si Siveco.

Prelucrarea informatiilor in sistemul de evidenta contabila (state de salarii) si cele de personal, pe suport hartie este structurata dupa criteriul „dosare-bibliorafturi", fiind pastrate in dulapuri, care sunt amplasate la sediul Mentenanta programului de salarizare este efectuat de catre **Liceul Tehnologic „Domokos Kazmer".**

4.6 Stocarea datelor cu caracter personal mentionate la punctele 3.1. si 3.2. se va putea face in fise, registre, scrisori, adeverinte, etc pe suport de hartie si informatizat pe serverele aflate la sediul si punctele de lucru ale Liceului Tehnologic „Domokos Kazmer" , mentionate in preambulul prezentelor politici.

V. DURATA DE STOCARE A DATELOR CU CARACTER PERSONAL

5.1. Prelucrarea datelor cu caracter personal ale salariatilor se efectueaza pe perioada valabilitatii activitatii lor(din momentul semnarii contractului de munca pana la finalizarea efectuarii actiunilor prevazute de actele legislative in cazul incetarii raportului de munca).

5.2. Prelucrarea datelor cu caracter personal apartinand prescolarilor, elevilor, parintilor, salariatilor se face pe perioada aflarii acestora pe listele de evidenta/ contractele individuale de munca ,contractele civile de furnizare servicii,contractele educationale, alte evidente iar stocarea acestor date va fi cea prevazuta de dispozitiile legale, ulterior acestor perioade fiind declasate si distruse.

5.3. La expirarea termenelor mentionate la punctul 5.1., datele din sistemele folosite pentru salarizare sunt pastrate in forma arhivata, pe perioada stabilita de Nomenclatorul general stabilit si aprobat.

5.4. La expirarea termenelor prevazute de lege pentru pastrarea datelor apartinand prescolarilor, elevilor, parintilor, salariatilor , acestea vor fi sterse, iar documentele pe suport hartie aferente acestora vor fi distruse.

VI. DREPTURILE PERSOANELOR VIZATE

6.1. **Liceul Tehnologic „Domokos Kazmer",** in calitate de operator de date cu caracter personal, garanteaza respectarea drepturilor privind protectia datelor cu caracter personal ce le revin angajatilor si pacientilor.

6.2. In conformitate cu principiile de protectie ale datelor cu caracter personal, persoanele vizate beneficiaza de drepturi care sunt mentionate in notele de informare (anexa la prezentul document) pe care societatea le ofera persoanelor vizate.

6 .3. Conform Regulamentului Parlamentului European si al Consiliului nr.679/2016, persoanele vizate beneficiaza de urmatoarele drepturi:

- **dreptul la informare si acces** – persoanele vizate pot solicita informatii privind activitatile de prelucrare a datelor personale si au dreptul de a obtine o confirmare din partea noastra ca prelucram sau nu aceste date, iar daca da, sa ofere acces la aceste date precum si informatii despre cum sunt prelucrate;

- **dreptul la rectificare** – persoana vizata are dreptul de a obtine de la noi, fara intarzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc.Tinandu-se seama de scopurile in care au fost prelucrate datele, persoana vizata are dreptul de a obtine completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaratii suplimentare;
- **dreptul la stergerea datelor(dreptul de a fi uitat)** – persoana vizata are dreptul de a obtine din partea operatorului stergerea datelor cu caracter personal care o privesc, fara intarzieri nejustificate;

- **dreptul la restrictionarea prelucrarii** – persoana vizata are dreptul de a obtine din partea noastra restrictionarea prelucrarii datelor in urmatoarele cazuri: persoana vizata contesta exactitatea datelor, pentru o perioada care ne permite sa verificam exactitatea datelor; prelucrarea este ilegala, iar persoana vizata se opune stergerii datelor cu caracter personal, solicitand in schimb restrictionarea utilizarii

lor; operatorul nu mai are nevoie de datele cu caracter personal in scopul prelucrarii, dar persoana vizata i se solicita pentru constatarea, exercitarea sau apararea unui drept in instanta;

- **dreptul la portabilitatea datelor** – persoana vizata are dreptul de a primi datele cu caracter personal care o privesc si pe care le-a furnizat operatorului intr-un format structurat, utilizat in mod curent si care poate fi citit automat si are dreptul de a transmite aceste date altui operator, fara obstacole din partea operatorului caruia i-au fost furnizate datele cu caracter personal;

- **dreptul la opozitie –** in orice moment, persoana vizata are dreptul de a se opune, din motive legate de situatia particulara in care se afla, prelucrarii datelor cu caracter personal care o privesc, inclusiv crearii de profiluri pe baza respectivelor dispozitii. Operatorul nu mai prelucreaza datele cu caracter personal, cu exceptia cazului in care operatorul demonstreaza ca are motive legitime si imperioase care justifica prelucrarea si care prevaleaza asupra intereselor, drepturilor si libertatilor persoanei vizate sau ca scopul este constatarea, exercitarea sau apararea unui drept in instanta;

- **dreptul de a fi notificat** in caz de incalcari privid securitatea datelor, de catre operator;

- **dreptul persoanei vizate de a depune o petitie/plangere la autoritatea de supraveghere.**

- **dreptul persoanei vizate de a se adresa justitiei.**

6.4. Toate persoanele implicate in activitatea de administrare si/sau prelucrare a informatiilor din sistemele de evidenta vor respecta procedura de acces la datele cu caracter personal.

VII. MASURI DE PROTECTIE ALE DATELOR CU CARACTER PERSONAL PRELUCRATE IN SISTEMELE DE EVIDENTA

7.1. Masurile generale de administrare a securitatii informationale:
7.1.1. La terminarea sesiunilor de lucru, computerele si imprimantele se deconecteaza de la reteaua electrica.
7.1.2. Operatorul asigura securitatea punctelor de primire si expediere a corespondentei, precum si securitatea contra accesului neautorizat la aparatele de copiere.
7.1.3. Accesul fizic la mijloacele de reprezentare a informatiei preluate din sistemele de evidenta ale prescolarilor/elevilor/salariatilor/parintilor/ , este blocat impotriva vizualizarii de catre persoane neautorizate.

7.2. Masurile de protectie ale datelor cu caracter personal, prelucrate in sistemele de evidenta ale prescolarilor/elevilor/salariatilor/parintilor/, se infaptuiesc tinand cont de necesitatea asigurarii confidentialitatii si integritatii acestora, prin protectie in forma manuala, electronica si externa.

7.3 Accesul la sistemele de evidenta ale prescolarilor/elevilor/salariatilor/ parintilor/ este restrictionat, fiind permis doar persoanelor care au autorizatia necesara si doar in timpul orelor de program. Accesul in perimetrul sistemului de evidenta este posibil doar cu codul de acces.

7.4. Perimetrul de securitate se considera perimetrul locul in care este amplasat sistemul de evidenta al prescolarilor/elevilor/salariatilor/parintilor/, fiind integru din punct de vedere fizic (echipament de alarma, echipament de supraveghere video, sistem de alarma, contract cu firma de securitate.)

7.5. Computerele sunt amplasate in locuri cu acces limitat pentru persoane straine.

7.6. Usile si ferestrele sunt incuiate in cazul in care in incapere lipsesc angajatii autorizati de administrarea sistemului.Spatiul de depozitare in arhiva unitatii sub cheie cu acces limitat al personalului angajat.

7.7. Securitatea antiincendiara a sistemelor de evidenta ale prescolarilor/elevilor/salariatilor/parintilor/: locatia unde sunt amplasate sistemele de evidenta ale prescolarilor/elevilor/salariatilor/parintilor/este dotat cu sistem de alarmare si stingere, instinctoare, etc si corespunde cerintelor si normelor antiincendiare in vigoare.

VIII. IDENTIFICAREA SI AUTENTIFICAREA UTILIZATORILOR SISTEMULUI DE EVIDENTA

8.1. Toti utilizatorii au un identificator personal (ID-ul utilizatorului), care nu trebuie sa contina semnalmentele nivelului de accesibilitate al utilizatorului.

8.2. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. Utilizarea parolelor in procesul asigurarii securitatii informational: pe langa cerintele de pastrare a confidentialitatii parolelor, este interzisa inscrierea acestora pe suport de hartie. La momentul introducerii, parolele nu se reflecta in clar pe monitor.

8.3. Se efectueaza modificarea parolelor de fiecare data cand sunt depistati indicii unei eventuale compromiteri a sistemului sau parolei.

8.4. In scopul depistarii si evitarii cazurilor de acordare ale drepturilor de acces neautorizat, se revizuieste cu regularitate, si dupa oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidenta contabila, etc.

8.5. Folosirea tehnologiilor fara fir, echipamentelor portative si mobile se autorizeaza de catre persoanele responsabile.

8.6. Se impun limite in privinta persoanelor care au dreptul:
a) sa vizualizeze informatiile stocate in sistemele de evidenta;
b) sa copieze, sa descarce, sa stearga sau sa modifice orice informatie stocata.

8.7. Toti angajatii cu drepturi de acces beneficiaza de o instruire initiala in domeniul protectiei datelor cu caracter personal.

8.8. Orice activitate de dezvaluire a datelor cu caracter personal catre terti este documentata si supusa unei analize riguroase in prealabil privind scopul si temeiul legal a intentiilor de dezvaluire a unui anumit volum de date cu caracter personal.

8.9. Orice incalcare a securitatii in ceea ce priveste sistemele de evidenta ale salariatilor si clientilor este supusa documentarii, iar persoana responsabila de realizarea politicii de securitate este informata in legatura cu acest lucru cat de urgent posibil.

8.10. Inainte de acordarea accesului in sistem, utilizatorii sunt informati despre faptul ca folosirea sistemelor de evidenta ale persoanelor vizate, este controlata si ca folosirea neautorizata a acestora este sanctionata in conformitate cu legislatia in vigoare.

8.11. Alti operatori secundari si destinatari ai datelor cu caracter personal ale persoanelor vizate sunt : ANAF, ITM, AJOFM,MEN, Inspectorat Scolar, Inspectorat de Politie etc.... alte autoritati ale statului si colaboratori.

8.12. Utilizatori/operatori date : angajatii unitatii, colaboratori, imputernicit sistem informatic,etc.

IX. ASIGURAREA INTEGRITATII INFORMATIILOR DIN SISTEMUL DE EVIDENTA

9.1. Se asigura identificarea, protocolarea si inlaturarea deficientelor de soft-uri destinate prelucrarii informatiilor din sistemele de evidenta ale persoanelor vizate, inclusiv instalarea corectarilor si pachetelor de reinnoire a acestora, protectia contra infiltrarii programelor daunatoare in soft-uri, masuri care asigura posibilitatea reinnoirii automate si la timp a mijloacelor de asigurare a protectiei contra programelor daunatoare si signaturilor de virus.

9.2. Se utilizeaza tehnologii si mijloace de constatare a intrarilor ilegale, ce permit monitorizarea evenimentelor si constatarea atacurilor, inclusiv asigura identificarea tentativelor folosirii neautorizate a informatiilor din sistemele de evidenta ale persoanelor vizate.

9.3. Se asigura testarea functionarii corecte a componentelor de securitate a sistemelor de evidenta ale persoanelor vizate (automat - la pornirea sistemului, si dupa caz - la solicitarea persoanei responsabile de politica de securitate a prelucrarii datelor cu caracter personal).

9.4. Copiile de siguranta: reiesind din volumul prelucrarilor efectuate, individual, se stabileste de catre operator intervalul de timp in care se executa copiile de siguranta ale informatiilor din sistemele de evidenta ale persoanelor vizate si soft-urilor folosite pentru prelucrarile automatizate ale acestora. Copiile de siguranta se testeaza in scopul verificarii sigurantei purtatorilor de informatii si integritatii informatiei indicate. Procedurile de restabilire a copiilor de siguranta se actualizeaza si se testeaza cu regularitate, in scopul asigurarii eficacitatii acestora.

9.5. Se asigura protectia documentelor pe suport hartie privind sistemele de evidenta ale salariatilor prin arhivarea si pastrarea acestora in dulapuri securizate cu lacat aflate la sediul Liceului Tehnologic „Domokos Kazmer",din localitatea Sovata.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR DE EVIDENTA

10.1.In cazul in care are loc o incalcare a securitatii datelor cu caracter personal, **Liceul Tehnologic „Domokos Kazmer"** notifica acest lucru catre ANSPDCP – Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal, fara intarzieri nejustificate, in termen de 72 de ore de la data la care a luat cunostinta de aceasta, cu exceptia cazului in care este susceptibila sa genereze un risc pentru drepturile si libertatile persoanelor fizice. In cazul in care notificarea nu are loc in termen de 72 de ore, aceasta trebuie insotita de o explicatie motivata.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preintampinarea dezvoltarii, inlaturarea lor si restabilirea securitatii. Se monitorizeaza si documenteaza, in mod permanent, incidentele de securitate in sistemele de evidenta.

10.3. Operatorul pastreaza documente referitoare la toate cazurile de incalcare a securitatii datelor cu caracter personal, a efectelor acesteia si a masurilor de remediere intreprinse. Aceasta documentatie permite autoritatii de supraveghere sa verifice conformitatea incidentului.

10.4. In cazul in care incalcarea securitatii datelor cu caracter personal este susceptibila sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice, operatorul informeaza persoana vizata fara intarzieri nejustificate cu privire la aceasta incalcare.

10.5. Informarea persoanei vizate mentinata la punctul 10.4. nu este necesare in cazul in care este indeplinita una din urmatoarele situatii:

- operatorul a implementat masuri de protectie tehnice si organizatorice adecvate, iar aceste masuri au fost aplicate in cazul datelor cu caracter personal afectate de incalcarea securitatii datelor cu caracter personal, in special masuri prin

care se asigura ca datele cu caracter personal devin neinteligibile oricarei persoane care nu este autorizata sa le acceseze, cum ar fi criptarea;

- operatorul a luat masuri ulterioare prin care se asigura ca riscul ridicat pentru drepturile si libertatile persoanelor vizate mentionat la punctul 10.4. nu mai este susceptibil sa se materializeze;
- ar necesita un efort disproportionat. In aceasta situatie, se efectueaza in loc de informare publica sau se ia o masura similara prin care persoanele vizate sunt informate intr-un mod la fel de eficace.

XI. DISPOZITII FINALE

11.1. Prezentele politici sunt aprobate de catre conducerea Liceului Tehnologic „Domokos Kazmer" insa revizuite la necesitate.

11.2. Prezentele politici se completeaza cu prevederile legislatiei in vigoare.

11.3. Politicile sunt aduse la cunostinta salariatilor de catre reprezentantul legal al Liceului Tehnologic „Domokos Kazmer"

Data

Liceul Tehnologic ‚Domokos Kazmer"

25.05.2018

Director
Vass Ferencz