Informare legala

1. Completarea acestor documente se va face pe propria răspundere, II EUROPEANCONSULTING SRL neasumându-și în niciun fel răspunderea pentru eventualele prejudicii care pot apărea ca urmare a folosirii acestor documente, incluzând, dar fără a se limita la sancțiuni din partea autorităților sau pretenții din partea altor persoane.

2. Documentele sunt menite să fie un punct de pornire pentru crearea propriilor documente, verificate în prealabil pentru respectarea legislației incidente și a standardelor de calitate. Prin urmare, este responsabilitatea dvs. de a vă asigura că documentul respectă cerințele legale incidente. Recomandăm consultarea unui unui specialist în domeniul GDPR anterior utilizării acestui document.

3. II EUROPEANCONSULTING SRL nu face nici o declarație, promisiune sau garanție cu privire la exactitatea, exhaustivitatea sau caracterul adecvat al template-urilor, nu își asumă nicio obligație de rezultat sau diligență față de nicio persoană cu privire la template-uri și/sau conținutul acestora și exclude în mod expres și neagă răspunderea pentru orice cost, pierdere sau daunele suferite ca urmare a utilizării template-urilor sau ca așteptare ca aceste documente să satisfacă nevoile organizației dvs., incluzând, dar fără a se limita la erori, denaturări sau omisiuni din conținutul lor.

4. II EUROPEANCONSULTING SRL detine dreptul de autor asupra intregului material de continut, precum prezentari de diapozitive, imagini, manuale, proceduri, note de orientare sau informatii, continute in prezentul DOCUMENT

5. II EUROPEANCONSULTING SRL acorda cumparatorului prin prezenta o licenta neexclusiva, netransferabila, fara redeventa si revocabila, pentru reproducerea si modificarea Materialului in scopul utilizarii, dezvoltarii si implementarii unui proiect GDPR ("GDPR") in cadrul unei singure organizatii. In sensul prezentei clauze, o singura organizatie ("organizatia") este definita ca organizatie unica (care, pentru evitarea oricarei indoieli, poate opera din mai multe locatii si / sau din mai multe zone geografice si / sau jurisdictii legale) care se afla in sfera unui singur proiect GDPR documentat prin utilizarea materialului in aceasta U.A.T.

6. Aceasta licenta nu include dreptul de a utiliza materialul in mai multe companii sau proiecte GDPR si, in cazul in care o singura organizatie opereaza mai mult de un proiect GDPR, Materialul este licentiat pentru utilizare/implementare numai in unul dintre acestea

7. Neasumarea răspunderii: Conținutul prezentului material și/sau a șabloanelor, ghidurilor și a altor materiale conținute de prezentul cumul de documente, numit KIT GDPR, nu reprezintă o consultație juridică în sensul Legii nr. 51/1995.

8. Prezenta informare se completeaza cu documentul ACORD DE LICENTA PRIVIND DREPTURILE DE AUTOR

ACORD DE LICENTA PRIVIND DREPTURILE DE AUTOR

1. Acest acord de licență pentru drepturi de autor ("Contractul") este încheiat între II EUROPEANCONSULTING SRL, CIF 43755429, înregistrat la Registrul Comerțului sub nr. J33/345/2021, cu sediul social in Str. Ghiocelului nr. 16, Mun. Câmpulung Moldovenesc, județul Suceava, Romania și Dvs. (persoana sau organizația care a achiziționat produsul GDPR, care poate fi confirmată de o factură oficială originală emisă de către II EUROPEANCONSULTING SRL) și intră în vigoare de la data (conform facturii) la care ați făcut achiziția.

2. II EUROPEANCONSULTING SRL deține dreptul de autor asupra întregului material de conținut, precum prezentări de diapozitive, imagini, manuale, proceduri, note de orientare sau informații, conținute în GDPR ("Materialul") pe care l-ați cumpărat , precum și în orice actualizări sau actualizări sau orice tip care ar putea fi, din când în când, puse la dispoziția dvs., cu excepția materialelor legislative și a infograficelor care sunt furnizate și prezentate cu titlu GRATUIT..

3. Utilizarea in orice mod a oricarei parti a Materialelor constituie acceptarea termenilor prezentului Contract.

4. Aceasta licenta nu include dreptul de a utiliza materialul in mai multe companii sau proiecte GDPR si, in cazul in care o singura organizatie opereaza mai mult de un proiect GDPR, Materialul este licentiat pentru utilizare/implementare numai in unul dintre acestea.

5. Prezentul se completeaza cu Acordul de licenta privind drepturile de autor atasat prezentului.

POLITICI INTERNE

GDPR

ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ”

POLITICA INTERNA
Audit Intern

conform cu

Regulamentul UE 2016/679 al Parlamentului European

ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ”

Cuprins

I. SCOP

Scopul acestei politici este definirea unui proces de testare si evaluarea periodica a eficientei masurilor tehnice si organizatorice pentru **asigurarea securitatii procesarii datelor** in cadrul unitatii de invatamant **ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ”**.

II. DESCRIEREA PE SCURT A POLITICII

Prin aceasta politica se stabilesc masurile necesare si responsabilitatile angajatilor care trebuie respectate pentru a realiza periodic auditul intern. Aceasta procedura se aplica tuturor activitatilor de prelucrare a datelor cu caracter personal.

III. DOMENIUL DE APLICARE

Domeniul de aplicare al acestei politici include toti angajatii care au un punct de lucru desemnat sau un birou alocat in cadrul punctelor de luru ale unitatii de invatamant **ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ”**.

IV. AUTORIZAREA POLITICII

Respectarea acestei politici este autorizata de managementul unitatii de invatamant **ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ”**, iar monitorizarea functionalitatii ei se face de catre Seful/Responsabilul de Departament si DPO - Responsabilul cu protectia datelor din punct de vedere al protectiei datelor cu caracter personal.

V. RESPONSABILITATEA

Toti angajatii, angajatii si entitatile care lucreaza in numele unitatii de invatamant **ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ”** fac obiectul acestei politici.

VI. PUNEREA IN APLICARE

Orice angajat care a constatat ca a incalcat aceasta politica poate face obiectul unor masuri disciplinare, inclusiv pana la incetarea contractului de munca.

VII. GARANTII

Unitatea de invatamant ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ” garanteaza ca drepturile de confidentialitate ale angajatilor, furnizorilor, partenerilor si clientilor ului vor fi respectate ca parte a acestei politici.

VIII. DOCUMENTELE NECESARE POLITICII

Acest document se completeaza cu

- Politica generala de lucru cu date cu caracter personal
- Regulament de ordine interioara
- Eventualele Documente, Formulare, Cereri incluse in prezenta politica;
- Procedurile incluse in prezenta politica

Acest document se completeaza cu intreg setul de politici/proceduri aprobat de conducerea unitatii de invatamant **ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ”** si aflat in vigoare.

IX. LEGISLATIE DE REFERINTA

Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si libera circulatie a acestor date si de abrogare a Directivei 95/46 / CE);

Legea nr. 190 din 18 iulie 2018 privind masuri de punere in aplicare a Regulamentului (UE) 2016/679 al Parlamentului European si al Consiliului 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 .

Legea nr. 129 din 15 iunie 2018 pentru modificarea si completarea Legii nr. 102/2005 privind infiintarea, organizarea si functionarea Autoritatii Nationale de Supraveghere a Prelucrarii Datelor cu Caracter Personal, precum si pentru abrogarea Legii nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date;

Legea nr. 102 din 3 mai 2005 privind infiintarea, organizarea si functionarea Autoritatii Nationale de Supraveghere a Prelucrarii Datelor cu Caracter Personal, cu modificarile si completarile ulterioare;

Ordinul Avocatului Poporului nr. 52 din 18/04/2002 privind aprobarea Cerintelor minime de securitate a prelucrarilor de date cu caracter personal;

Decizia ANSPDCP nr. 90 din 18/07/2006 privind stabilirea cazurilor in care nu este necesara notificarea prelucrarii unor date cu caracter personal;

Decizia ANSPDCP nr. 100 din 23/11/2007 privind stabilirea cazurilor in care nu este necesara notificarea prelucrarii unor date cu caracter personal;

Decizia nr. 174 din 8 Ocrombrie 2018 privind efectuarea DPIA emisă de ANSPDCP ce reglementeaza situatiile cand trebuie efectuata o Evaluare de Impact DPIA asupra Datelor cu Caracter Personal procesate in conformitatea cu GDPR.

Decizia nr. 161 din 9 octombrie 2018 privind procedura de efectuare a investigațiilor de către ANSPDCP conform cu a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) și a legii nr.

190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679.

X. TERMENI SI DEFINITII

ANSPDCP - Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal;

Codul numeric personal (CNP) - un numar semnificativ care individualizeaza in mod unic o persoana fizica, constituind un instrument de verificare a starii civile a acesteia si de identificare in anumite sisteme informatice de catre persoanele autorizate;

Date cu caracter personal - orice informatii referitoare la o persoana fizica identificata sau identificabila; o persoana identificabila este acea persoana care poate fi identificata, direct sau indirect, in mod particular prin referire la un numar de identificare ori la unul sau la mai multi factori specifici identitatii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

Date cu caracter personal cu functie de identificare de aplicabilitate generala (date cu caracter special) - numere prin care se identifica o persoana fizica in anumite sisteme de evidenta si care au aplicabilitate generala, cum ar fi: codul numeric personal, seria si numarul actului de identitate, numarul pasaportului, al permisului de conducere, numarul de asigurare sociala sau de sanatate;

Date anonime - date care, datorita originii sau modalitatii specifice de prelucrare, nu pot fi asociate cu o persoana identificata sau identificabila

Operator/Controlor - orice persoana fizica sau juridica, de drept privat ori de drept public, inclusiv autoritatile publice, institutiile si structurile teritoriale ale acestora, care stabileste scopul si mijloacele de prelucrare a datelor cu caracter personal; daca scopul si mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau in baza unui act normativ, operator este persoana fizica sau juridica, de drept public ori de drept privat, care este desemnata ca operator prin acel act normativ sau in baza acelui act normativ;

Procesator/Procesor/Colector/Prelucrator/Persoana imputernicita de catre operator - o persoana fizica sau juridica, de drept privat ori de drept public, inclusiv autoritatile publice, institutiile si structurile teritoriale ale acestora, care prelucreaza date cu caracter personal pe seama operatorului;

DPO - Persoana responsabila de protectia datelor cu caracter personal – persoana responsabila de functionarea corespunzatoare a sistemului complex de protectie a informatiei care contine date cu caracter personal, precum si de elaborarea, implementarea si monitorizarea respectarii prevederilor politicii de securitate a detinatorului de date cu caracter personal;

Prelucrarea datelor cu caracter personal - orice operatiune sau set de operatiuni care se efectueaza asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, inregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvaluirea catre terti prin transmitere, diseminare sau in orice alt mod, alaturarea ori combinarea, blocarea, stergerea sau distrugerea;

Utilizator - orice persoana care actioneaza sub autoritatea operatorului, a persoanei imputernicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.
Statie de lucru – Calculator sau Laptopt care este atribuita unui angajat pentru desfasurarea activitatii.
GDPR - Regulamentul General pentru Protectia Datelor cu caracter personal nr. 679/2016
DSAR Data Subject Access Rights – Drepturile de acces ale persoanei vizate

XI. DETALIERE POLITICA

1. Scopul auditului intern

(1) Scopul auditului intern este de a determina daca procedurile, controalele, procesele si aranjamentele pentru activitatile de prelucrare a datelor cu caracter personal sunt conforme cu reglementarile aplicabile si cu documentatia interna a organizatiei, daca acestea sunt efectiv implementate si mentinute si daca indeplinesc cerintele si obiectivele stabilite ale politicii.

2. Planificarea auditului intern

(1) Unul sau mai multe audituri interne ar trebui efectuate in decurs de un an, asigurand acoperirea cumulata a tuturor activitatilor de prelucrare a datelor cu caracter personal.

(2) Auditurile interne sunt planificate pe baza evaluarii riscurilor, precum si a rezultatelor auditurilor anterioare.

(3) REPLEGAL ..... defineste programul anual de audit (adica datele la care vor fi efectuate unul sau o serie de audituri).

3. Numirea auditorilor interni

(1) REPLEGAL ..... desemneaza auditorii interni.

(2) Un auditor intern poate fi un angajat din companie sau o persoana din afara organizatiei.

(3) Criteriile de numire a auditorilor interni sunt:

- cunoasterea controalelor din Anexa A ISO / IEC 27001
- cunoasterea Regulamentului UE 679/2017 - GDPR
- familiarizarea cu tehnicile de audit al sistemului de management
- cunoasterea modului in care functioneaza tehnologiile informatiei si comunicatiilor in masura in care acesta cunoaste scopul sistemelor individuale, precum si impactul asupra proceselor de securitate si / sau asupra continuitatii activitatii

(4) Auditorii interni trebuie selectati astfel incat sa se asigure obiectivitatea si impartialitatea, adica evitarea conflictului de interese, deoarece auditorilor nu li se permite sa-si controleze propria activitate.

(5) Se recomanda ca auditorii interni sa finalizeze un curs pentru auditori interni conform ISO / IEC 27001.

4. Efectuarea auditurilor interne individuale

(1) Daca un audit este efectuat de o echipa formata din mai multi auditori, persoana responsabila de audit este cea identificata ca lider al echipei de audit.

(2) Urmatoarele trebuie sa fie luate in considerare, testate, evaluate si comparate cu situatia din cadrul Societatii in timpul unui audit intern:

- cerintele politicilor, procedurilor si planurilor proprii de securitate ale organizatiei
- rezultatele auditurilor interne sau externe anterioare
- rezultatele evaluarii riscurilor, punerea in aplicare a controalelor, evaluarea impactului privind protectia datelor, etc.
- controalele aplicabile din Anexa A la standardul ISO 27001 enumerate in lista de verificare a auditului intern

(3) Urmatoarele trebuie sa fie documentate ca rezultate ale auditului intern:

- Auditorul intern trebuie sa tina cont de toate constatarile din lista de verificare a auditului intern
- Daca se constata neconformitati, auditorul intern trebuie sa le notifice DPO Responsabilului pentru protectia datelor in forma scrisa sau prin e-mail

5. Procedura de lucru

(1) Pentru mentinerea gradului de securitate si conformitate se initiaza un audit intern, anual sau in urmatoarele situatii**:**

a. efectuarea evaluarii initiale;
b. derularea programului de audit;
c. la solicitarea conducerii, pentru a obtine date suplimentare necesare analizei efectuate de management;
d. in cazul unor modificari ale structurii organizatorice;
e. pentru pregatirea in vederea unui audit extern cerut si efectuat de un client sau de un organism de certificare;
f. in cazul in care se constata probleme anumite procese

(2) Directorul Departamentului IT elaboreaza in luna ianuarie a fiecarui an un "Programul de Audit Intern". Auditarea se va face pe departamente.

(3) Directorul Departamentului IT numeste auditorii, avand in vedere:

a. independenta acestora fata de procesul auditat;
b. experienta si instruirea necesara pentru auditarea procesului respectiv.

(4) Coordonatorul Echipei de Audit instiinteaza Reponsabilul/Proprietarul de Proces care urmeaza sa fie auditat, cel putin cu 1 saptamana inainte de audit, sau chiar in ziua auditului, daca e vorba de un audit neprogramat.

(5) La data stabilita de comun acord intre proprietarul de proces si Coordonatorul Echipei de Audit, se va desfasura o reuniune de deschidere a auditului, al carei obiectiv este de a prezenta scopul auditului si stabilirea unui mod de lucru comun.

(6) Incepe auditul propriu-zis prin examinarea de catre auditori a procesului avut in vedere si stabilirea daca documentele aplicabile si implementarea sistemului calitatii in zona auditata sunt corecte si complete (Chestionar de Audit, Standarde, Proceduri).

(7) Toate observatiile/neconformitatile evidentiate sunt clar si precis documentate pe baza de dovezi obiective. Dovezile se obtin prin:

a. discutii;

b. examinarea documentelor;
c. observarea activitatior si situatiilor.

(8) Auditorii inregistreaza toate neconformitatile, observatiile si oportunitatile de imbunatatile pe "**Raportul de audit intern**"

(9) Proprietarul de proces stabileste masurile de tratare a neconformitatilor si actiunile corective/preventive adecvate, pe care le poate discuta cu echipa de audit, urmind sa le inscrie pe "**Raportul de Actiune Corectiva /Preventiva**"

(10) "**Raportul de Audit Intern**" este semnat de echipa de audit si de proprietarul de proces auditat, o copie ramine la proprietarul de proces, iar originalul este retinut de Coordonatorul Echipei de Audit. In cel mult 2 zile de la auditul intern, o copie a "Raportului de Audit Intern" (822-01-02) este trimisa de Coordonatorul Echipei de Audit la RMI.

(11) **Auditatul are autoritatea de a initia si efectua toate actiunile corective/preventive** necesare pentru a elimina neconformitatile trecute in "Raportul de Audit Intern". Auditul este considerat finalizat numai dupa verificarea implementarii si inchiderea actiunilor corective/preventive, conform procedurii interne "Actiuni Corective/Preventive".

(12) **La data stabilita pentru verificarea implementarii** actiunilor corective, auditorii interni efectueaza un audit de eficacitate.

6. Actiuni corective eficace

DA	Coordonatorul Echipei de Audit si auditatul incheie "Raportul de Actiune Corectiva/Preventiva" o copie ramine la auditat, iar originalul este trimis la RMI. "Rapoartele de Audit Intern" sunt utilizate ca si date de intrare la sedintele de analiza a procesului de audit.
NU	Auditatul stabileste noi actiuni corective/preventive de implementat, iar impreuna cu Coordonatorul Echipei de Audit stabileste data unui nou audit de eficacitate "Raport de Audit".

7. Gestionarea inregistrarilor

Toate activitatile legate de derularea acestei proceduri vor fi inregistrate in documente specifice dupa cum urmeaza:

Denumire document	Locul stocarii	Persoana Care are acces	Controale pentru protectia inregistrarii	Termen de pastrare
Programul de Audit Intern	Serverul local de date si/sau reteaua locala a Companiei si in backupurile periodice	Top management Directorul IT Persoana desemnata DPO Auditor intern	Numai persoanele autorizate pot accesa fisierul cu drepturi precise de editare definite; istoricul schimbarilor trebuie mentinut.	5 ani
Raportul de audit intern	Serverul local de date si/sau reteaua locala a Companiei si in backupurile periodice	Top management Directorul IT Persoana desemnata DPO Auditor intern	Numai persoanele autorizate pot accesa fisierul cu drepturi precise de editare definite; istoricul schimbarilor trebuie mentinut.	5 ani

Raportul de Actiune Corectiva /Preventiva	Serverul local de date si/sau reteaua locala a Companiei si in backupurile periodice	Top management Directorul IT Persoana desemnata DPO Auditor intern	Numai persoanele autorizate pot accesa fisierul cu drepturi precise de editare definite; istoricul schimbarilor trebuie mentinut.	5 ani
Lista de verificare a auditului intern (formular, completat in timpul auditului intern)	Serverul local de date si/sau reteaua locala a Companiei si in backupurile periodice	Auditor Intern Persoana desemnata DPO	Listele de verificare sunt stocate doar in format de citire fara drept de editare, de preferat PDF	5 ani
Notificari din partea auditului intern catre responsabilul cu protectia datelor	Serverul local de date si/sau reteaua locala a Companiei si in backupurile periodice	Auditor Intern	Numai auditorul intern si responsabilul cu protectia datelor pot avea acces la aceste documente	5 ani

XII. DISPOZITII FINALE

(1) Conducerea unitatii de invatamant ȘCOALA GIMNAZIALĂ „BOGDAN VODĂ” este responsabila pentru respectarea si aplicarea prevederilor prezentului document.

(2) Marcarea documentelor. Toata informatia care se intentioneaza a fi dezvaluita, si care contine date cu caracter personal, urmeaza a fi marcata prin includerea numarului de inregistrare din Registrul de evidenta al controlor-operatorului de date cu caracter personal.

(3) Responsabilitatea pentru asigurarea securitatii datelor cu caracter personal precum si a informatiilor cu accesibilitate limitata

Versiune	Autor	Data	Aprobata de catre	Descrierea modificarii
1.0	Leșinschi Iustinian-Andrei	14 Februarie 2024		Prima versiune

Aprobata de:
Nume si prenume _____
Functie _____
Data _____
Semnatura _____

Intocmita de:
Nume si prenume Leșinschi Iustinian-Andrei
Functie DPO
Data 14.02.2024
Semnatura