Anexa nr.1 la Proiectul de hotărâre nr.13/2021

ANALIZA DE RISC
ÎN DOMENIUL SECURITĂȚII ȘI PROTECȚIEI DATELOR CU CARACTER PERSONAL A PRIMĂRIEI COMUNEI CAPLENI, JUDEȚUL SATU MARE

RAPORT DE ANALIZĂ A RISCURILOR ȘI VULNERABILITĂȚILOR PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
EVALUAREA ORGANIZĂRII ŞI MANAGEMENTULUI SECURITĂȚII INTERNE				
1.	Lipsa unor documente specifice de planificare şi organizare a activităţii de securitate a informaţiei, subliniind aici lipsa unei politici de securitate formalizate printr-un document programatic, avizat de conducerea Primăriei şi în fapt, lipsa unor prevederi clare privind calitatea serviciilor pe zona securității informatice, dar și responsabilităților pe linia administrării serviciilor tehnice informatice, coroborate cu lipsa unor clauze sancţionatorii cuantificabile.	La nivelul Primăriei nu sunt elaborate documente specifice de planificare şi organizare a activităţii de securitate a informaţiei, politicii de securitate formalizate printr-un document programatic, avizat de conducerea Primăriei. Lipsa unor prevederi clare privind calitatea serviciilor pe zona securității informatice, dar și a responsabilităților pe linia administrării serviciilor tehnice informatice, coroborate cu lipsa unor clauze sancţionatorii cuantificabile.	Risc mediu privind posibilitatea apariției unor incidente de securitate și incapacitatea stabilirii unui responsabil pentru realizarea incidentului.	Impact mediu. Securitatea redusă a sistemului, posibilitatea exfiltrării/compromiterii de date fără determinarea responsabilităților de securitate. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
2.	Lipsa unei persoane încadrate în funcția de DPO (Data Protection Officer) în Primărie sau externalizarea serviciului..	Funcția nu există la momentul actual deoarece legislația abrogată, tradusă prin Legea nr. 677/2001 nu impunea această funcție în organigrama Primăriei.	Risc Major, Imposibilitatea conformării cu politica GDPR 2018, inexistența unui responsabil pe domeniu generează protecția deficitară a datelor cu caracter personal, lipsa punctului unic de contact și a coordonării unitare a domeniului în Primărie.	Impact major, Neconformare încălcare art.37 alin.1 secțiunea 4. din Politica GDPR
3.	Lipsa procedurilor pe domeniul securității informatice interne: procedură de urgentă privind apariția unui incident de securitate ce a generat compromiterea datelor cu caracter personal, procedură de sistem privind colectarea, prelucrarea, ștergerea, transferul, datelor cu caracter personal, procedură de sistem la apariția unui eveniment de securitate, procedură privind accesul la sisteme informatice și aplicații, procedura de back-up /	Nu sunt definite: - procedură de urgență privind acțiunea la apariția unui incident de securitate ce a generat compromiterea datelor cu caracter personal (GDPR); - procedură de back-up date cu caracter personal; - procedură/politica de update a produselor software utilizate; - procedură de acces și utilizare sistem informatic al Primăriei; - procedura de obținere, prelucrare,	Risc Major privind acțiunea ineficientă în situația compromiterii datelor cu caracter personal, în situația aplicării dreptului de a fi uitat sau în situația solicitării transferului de date. Risc mediu privind posibilitatea compromiterii datelor și informațiilor specifice Primăriei.	Impact major, NECONFORMARE Imposibilitatea acțiunii coordonate pentru punerea în practică a prevederilor art. 33, art. 34 și art. 35 din capitolul IV.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	disaster recovery.	stocare, utilizare, transmitere și ștergere a datelor cu caracter personal (GDPR).		
4.	Nu sunt nominalizate persoanele care îndeplinesc funcțiile de administrator de securitate și administrator de sistem.	Aceste activități sunt parțial realizate de un consilier local în a cărui fisă a postului sunt trecute unele dintre responsabilitățile administratorului de sistem și unele din responsabilitățile administratorului de rețea	Risc mediu privind apariția unui incident de securitate ca urmare a implementării partiale a politicilor de securitate a infrastructurii Primăriei.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
5.	Inexistența în cadrul Primăriei a unei persoane responsabile pe domeniul securității care să coordoneze modul de asigurare a securității datelor și informațiilor cât și organizarea și administrarea internă a securității pentru protecția datelor fapt care poate genera lipsa unui management pe acest domeniu si apariția unor breșe de securitate.	Aceste responsabilități nu sunt îndeplinite efectiv de nicio persoană din cadrul Primăriei. Nu sunt prevăzute responsabilități și sarcini privind asigurarea securității infrastructurii informatice a Primăriei și responsabilități GDPR, nici standarde de performanță privind serviciile funcționale informatice.	Risc mediu privind apariția unui incident de securitate ca urmare a implementării partiale a politicilor de securitate a infrastructurii Primăriei.	Impact mediu Securizarea neadecvată a datelor cu caracter personal, lipsa unui control al configurației sistemelor informatice. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
6.	Nu sunt implementate şi nu sunt însuşite de personalul propriu, strategiile de securitate cu privire la protecţia datelor cu caracter personal;	Primăria nu are stabilite proceduri interne pentru protecția datelor cu caracter personal.	Risc mediu privind apariția unui incident de securitate ca urmare a lipsei unor proceduri interne care să stabilească modul corect de a acționa.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
7.	Nu sunt precizate clar în contractele cu Companiile de prestări servicii informatice responsabilitatile în domeniul managementului securității interne privind dezvoltarea, mentenanța și hosting-ul pentru site-ul web, precum și pentru dezvoltarea aplicațiilor de management al bazelor de date sau în procedurile interne, prin care Primăria își rezervă drepturile de exercitare a controlului privind implementarea măsurilor de	Contractele pe care Primăria le are cu furnizorii de servicii IT și cu furnizorii aplicațiilor folosite de Primărie nu conțin clauze clare pentru stabilirea responsabilităților în ceea ce privește sercuritatea aplicațiilor și în ceea ce privește compatibilitatea plicațiilor folosite cu regulile GDPR.	Risc mediu privind procesarea datelor cu caracter personal într-o manieră neconformă cu reglementările GDPR.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	securitate informatică prin controale inopinate, inspecții și evaluări tehnice, pe baza unui raport QoS			
8.	Lipsa clauzelor contractuale clare prin care sa se reglementeze: modul de asigurare a serviciilor informatice, persoanele din cadrul Companiilor de prestări servicii informatice care au acces la infrastructura de reţea a Primăriei, precum şi responsabilitățile privind asigurarea securităţii cibernetice pentru aplicațile utilizate de Primărie	Contractele pe care Primăria le are cu furnizorii de servicii IT și cu furnizorii aplicațiilor folosite de Primărie nu conțin clauze clare prin care să se stabilească persoanele din cadrul companiilor care au acces la datele cu caracter personal prelucrate de Primărie.	Risc mediu privind procesarea datelor cu caracter personal într-o manieră neconformă cu reglementările GDPR.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
9.	Existența unei imagini incomplete a infrastructurii informatice deținute de Primărie și lipsa documentelor de lucru pe domeniul securității cibernetice interne (documentație sistem informatic, liste utilizatori și drepturi de acces în sistemul informatic, inventar echipamente tehnice, proceduri de back-up/disaster recovery etc.).	Primăria nu are elaborată și aprobată o documentație scrisă clară din care să rezulte arhitectura rețelei, liste utilizatori și drepturi de acces în sistemul informatic, inventar echipamente tehnice, proceduri de back-up/disaster recovery etc.	Risc mediu datorat lipsei imaginii de ansamblu a arhitecturii de rețea, bine documentate.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
10.	Jurnalele stațiilor de lucru și ale unor elemente componente ale sistemului informatic se rescriu periodic automat, fără a se face salvare și copii de siguranță ale acestora	La nivelul Primăriei nu există un management clar al jurnalelor stațiilor de lucru (logurilor de sistem).	Risc scăzut datorat incapacității administratorului de sistem de a determina când au avut loc incidente de sistem. Doar că nu toate incidentele de sistem sunt datorate unor tentative de a accesa neautorizat date cu caracter personal.	Impact mediu, poate duce la incapacitatea Primăriei de a determina cauza incidentului de securitate care a dus la scurgerea de informații confidențiale. Imposibilitatea acțiunii coordonate pentru punerea în practică a prevederilor art. 33, art. 34 și art. 35 din capitolul IV.
11.	Managementul securității se rezumată la managementul utilizatorilor și drepturilor de acces, simpla funcționare a sistemelor	La nivelul Primăriei nu sunt luate în calcul scenarii de penetrare a rețelei și documentate posibilele vulnerabilități și masurile necesare remedierii acestora.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	informatice și având un grad ridicat de formalism.			Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
12.	Neaplicarea unitară a unor politici de securitate pe stațiile de lucru.	La nivelul Primăriei fiecare stație de lucru are propriile setări de siguranță și propria politică pentru Update-uri influențată de abilitățile utilizatorului.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
13.	Accesarea de către personalul Primăriei a sistemelor informatice, printr-un cont de utilizator cu drepturi de administrator local.	Conturile de utilizator pe care angajații Primăriei le folosesc pentru folosirea stațiilor de lucru ale Primăriei sunt conturi cu drepturi de administrator local.	Risc ridicat datorat posibilității compromiterii securității cibernetice a rețelei Primăriei și accesarea neautorizată la datele cu caracter personal procesate în cadrul Primăriei.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
14.	Primăria nu deține procedură de procesare specifică pe linia securității datelor și nici proceduri standard de acces și utilizare a sistemelor informatice de către utilizatori, funcționând în acest sens pe baza cunoștințelor fiecărui utilizator și pe baza unei pregătiri minimale inițiale, la angajare.	Primăria nu deține procedură de procesare specifică pe linia securității datelor și nici proceduri standard de acces și utilizare a sistemelor informatice de către utilizatori, funcționând în acest sens pe baza cunoștințelor fiecărui utilizator și pe baza unei pregătiri minimale inițiale, la angajare.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
15.	Activitățile de control de securitate și de audit intern ar trebui să aibă o periodicitate cel puţin anuală, dar nu au fost executate până în prezent.	La nivelul sistemului informatic al Primăriei nu au fost realizate până în prezent audituri de control al securității.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
16.	Prevenţia evenimentelor nedorinte nu este o preocupare principală în cadrul politicii de securitate, iar măsurile de securitate sunt în marea	La nivelul sistemului informatic al Primăriei nu au fost realizate până în prezent audituri de control al securității.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	lor majoritate de tip reactiv la situaţiile apărute.			Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
17.	Nerespectarea regimului de management a parolelor conturilor de utilizatori din cadrul sistemului informatic al Primăriei.	La nivelul sistemului informatic al Primăriei nu existe configurate parole pentru conturile de utilizatori ale angajaților Primăriei	Risc ridicat datorat posibilității compromiterii securității cibernetice a rețelei Primăriei și accesarea neautorizată la datele cu caracter personal procesate în cadrul Primăriei.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
18.	Obligativitatea angajaților Primăriei de a salva date cu caracter personal pe suport fizic – CD și de transmitere a acestor informații autorităților statului.	Date cu caracter personal procesate de Primărie sunt transferate, pe suport fizic – CD, către autoritățile statului.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
	SECURITATEA INFRASTRUCTURII ȘI SISTEMELOR DE TEHNOLOGIE A INFORMAȚIEI (IT)			
1.	Lipsa unui sistem de detecție și protecție împotriva intruziunilor (IDS/IPS) implementat la nivelul întregii rețele ca protecție de perimetru și ca soluție complementară de securitate, care să protejeze mediul de rețea, și să poată fi utilizată pentru eficientizarea managementului de securitate.	Lipsa unui sistem de detecție și protecție împotriva intruziunilor (IDS/IPS) implementat la nivelul întregii rețele ca protecție de perimetru și ca soluție complementară de securitate, care să protejeze mediul de rețea, și să poată fi utilizată pentru eficientizarea managementului de securitate.	Risc ridicat datorat posibilității compromiterii securității cibernetice a rețelei Primăriei și accesarea neautorizată la datele cu caracter personal procesate în cadrul Primăriei.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
2.	Lipsa unei soluții de tip SIEM (securitatea informațiilor și managementul evenimentelor) dimensionate corespunzător numărului de stații pentru colectarea	Log-urile de securitate (fișierele jurnal) la nivel de utilizator nu sunt salvate/stocate într-o zonă de memorie separată, cu acces limitat și nu sunt analizate de către responsabilul cu	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la incapacitatea Primăriei de a determina cauza incidentului de securitate care a dus la scurgerea de informații

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	și monitorizarea automată și activă a logurilor de securitate și accesului la date cu caracter personal, ca soluție integratoare de securitate. La momentul evaluarii, log-urile de securitate (fișierele jurnal) la nivel de utilizator nu sunt salvate/stocate într-o zonă de memorie separată, cu acces limitat și nu sunt analizate de către responsabilul cu securitatea, deoarece în sistem nu există o politică de management a log-urilor de securitate aplicată tehnic. De asemenea, procesele de modificare/ștergere/corectare a datelor cu caracter personal nu pot fi documentate cu exactitate în timp.	securitatea, deoarece în sistem nu există o politică de management a log-urilor de securitate aplicată tehnic. De asemenea, procesele de modificare/ștergere/corectare a datelor cu caracter personal nu pot fi documentate cu exactitate în timp.		confidențiale. Imposibilitatea acțiunii coordonate pentru punerea în practică a prevederilor art. 33, art. 34 și art. 35 din capitolul IV.
3.	Neimplementarea unitară a unei soluții profesionale anti-spam, anti-malware, anti-ransomware.	Stațiile de lucru din rețeaua interna a Primăriei au instalate ca soluție anti-malware Malwarebites home și instalarea update-urilor nu este unitară	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
4.	Stocarea datelor cu caracter personal în toate bazele de date interne în clar, fără instrumente de criptare și pseudoninimizare și fără posibilitatea de a păstra o evidență electronică completă a activităților de prelucrare/modificare/ștergere prin monitorizare activă și salvare de log-uri ale utilizatorilor.	Datele cu caracter perssonal sunt salvate în clar în baza de date și baza de date este stocata într-o zona de memorie nesecurizată – necriptată.	Risc scăzut datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact scăzut, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
5.	Neexecutarea periodică a testelor pentru securitatea infrastructurii informatice a Primăriei și nerealizarea sistematică a update-uri	Nu există stabilite politici pentru update-uri automate sau stabilite reguli de instalare a update-urilor. Nu există politici pentru scanarea periodică pentru	Risc scăzut pentru scanarea vurnerabilităților sistemului informatic al Primăriei. Risc ridicat pentru lipsa update-urilor	Impact scăzut, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	urile software și patch-urile de securitate.	vurnrabilități.	regulate a sistemului informatic al Primăriei.	Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
6.	Lipsa controlului porturilor de tip USB și a mediilor de stocare externe, prin politici de securitate manuale instalate pe stațiile client sau printr-un sistem automat.	Stațiile de lucru din rețeaua interna a Primăriei permit conectarea prin porturile USB a memoriilor stick si HDD-urilor externe.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
7.	Lipsa controlului sistemelor de tipărire prin produse software de jurnalizare.	Nu există nici o posibilitate la nivelul sistemului informatic al Primărie de a stabili cine, ce și unde a scos la imprimantă.	Risc scăzut, nu afectează securitatea sistemului informatic dar poate afecta securitatea accesului la datele cu caracter personal procesate în cadrul sistemului informatic al Primăriei.	Impact mediu, poate duce la incapacitatea Primăriei de a determina cauza incidentului de securitate care a dus la scurgerea de informații confidențiale. Imposibilitatea acțiunii coordonate pentru punerea în practică a prevederilor art. 33, art. 34 și art. 35 din capitolul IV.
8.	Utilizarea de către angajații primăriei a conturilor de acces cu drepturi de administrator local și fără parolă.	Angajații Primăriei pot accesa stațiile de lucru din sistemul informatic al Primăriei fără a specifica o parola și conturile folosite au drepturi de administrator local.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
9.	Lipsa unei politici privind managementul parolelor de acces la sistemele informatice și la aplicațiile specializate în care se procesează date cu caracter personal.	Nu exista parole de acces configurate pe stațiile din sistemul informati al Primăriei.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
10.	Accesul la rețeaua LAN a Primăriei se face automat în momentul în care calculatorul este conectat la rețea.	Accesul la rețeaua LAN a Primăriei se face automat în momentul în care calculatorul este conectat la rețea.	Risc scăzut, datorită separării rețelei LAN în zona protejată unde sunt procesate datele cu caracter personal	Impact scăzut, poate duce la accesarea neautoriaztă a datelor cu caracter personal

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
			și zona neprotejată care permite doar accesul la INTERNET.	procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
11.	Accesul la rețeaua WLAN a Primăriei se face folosind parola specifică.	Accesul la rețeaua WLAN a Primăriei se face folosind parola specifică.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
12.	Existența unei singure rețele de WIFI la care se pot conecta atât angajații primăriei în interes de sericiu cât și vizitatorii.	Există o singură rețea de WIFI la care se pot conecta atât angajații primăriei în interes de sericiu cât și vizitatorii.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
13.	Inexistența unui firewall hardware dedicat pentru sistemul informatic al Primăriei, care să protejeze sistemul informatic al Primăriei împotriva accesului neautorizat la date din exterior.	Nu există nici un firewall hardware configurat pentru protejarea reţelei informatice a Primăriei.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
14.	Inexistența unui controler de domeniu și a unui server de Active Directory (AD) care să gestioneze unitar conturile de utilizatori ale angajaţilor Primăriei, să permită aplicarea unei politici uniforme de securitate și să ofere facilități centralizate de management al accesului angajaților la resursele informatice ale Primăriei.	Nu există nici un server de AD configurat pentru getiunea unitară a conturilor de utilizator ale reţelei Primăriei.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
15.	Folosirea sericiilor externe de FTP (WeTransfer).	Angajații Primăriei folosesc serviciile de FTP oferite de **https://wetransfer.com/** sau altor furnizori din această categorie.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
			personal procesate de Primărie.	procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR dar și art. 33, art. 34 și art. 35 din capitolul IV
16.	Lipsa unor politici de tip white list sau black list pe ruterul central pentru a împiedica accesul la resursele de internet care compromit securitatea datelor și a rețelei de calculatoare a Primăriei.	La nivelul sistemului informatic al Primăriei nu exista stabilite reguli de filtrare al accesului la resursele Internet, angajații Primăriei pot accesa orice site doresc.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie și de compromitere a securității sistemului informatic al Primăriei.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR dar și art. 33, art. 34 și art. 35 din capitolul IV.
17.	Inexistența unei soluții profesionale de back-up.	Nu există o soluție de back-up pentru datele personale procesate de Primărie.	Risc mediu datorat de imposibilitatea angajaților Primăriei de a recupera datele cu caracter personal sterse accidental sau cu bună voință.	Impact mic, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
18.	Folosirea pe stațiile de lucru ale Primăriei, de către angajați, atât a conturilor de email personale cât și a celor de serviciu.	Folosirea pe stațiile de lucru ale Primăriei, de către angajați, atât a conturilor de email personale cât și a celor de serviciu.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
19.	Lipsa criptării unităților de memorie pentru stațiile de lucru pe care sunt procesate date cu caracter personal.	Datele cu caracter personal procesate de Primărie sunt salvate într-un format necriptat pe stațiile de lucru.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact ridicat, nerespectarea principiului de „privacy by default and privacy by design”.
20.	Folosire de către angajații Primăriei a telefoanelor cu tehnologia de dual sim pentru a avea și numărul personal și numărul de serviciu în același telefon.	Angajații Primăriei folosesc telefoane dual sim pentru a avea în acelasi echipament atât cartela SIM personală cât și cartela SIM primită de la Primărie.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
				Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
21.	Stocarea locală, în memoria telefonului a datelor cu caracter personal procesate.	Angajații Primăriei salvează datele cu caracter personal procesate de în memoria internă a primăriei.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
22.	Lipsa unor modalități de sercurizare a accesului la datele din telefoanele angajaților Primăriei.	Lipsa unor modalități de sercurizare a accesului la datele din telefoanele angajaților Primăriei.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
23.	Lipsa unei politici centralizate pentru activarea ștergerii de la distanță a telefoanelor pierdute / furate.	La nivelul Primăriei nu există stabilită o procedură aprobată de Primărie pentru stergerea conținutului unui telefon în cazul în care acesta este pierdut sau furat.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
24.	Lipsa unei politici interne pentru gestionarea unităților optice	Stațiile de lucru din cadrul rețele informatice a Primăriei dispun de unități optice pe care angajații le pot folosi pentru a salva informațiile din stațiile de lucru pe CD/DVD.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
25.	Lipsa unei politici interne privind modul cum sunt stocate datele cu caracter personal de către angajați pe telefoanele de serviciu sau cele personale care conțin și cartela SIM de serviciu.	Fiecare angajat al Primărie folosește telefonul mobil pe care procesează date cu caracter personal după cum consideră de cuviință.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
				capitolul II, politica GDPR.
26.	Lipsa unei politici interne pentru securizarea leptopurilor pentru a preveni accesul neautorizat la datele salvate pe unitatea de stocare internă.	Primăria nu are stabilite politici și proceduri pentru securizarea datelor cu caracter personal salvate pe unitățile de stocare internă	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
27.	Conturile de email pe care Primăria le utilizează nu folosesc versiunile securizate ale protocoalelor de comunicare.	Serverul de email al Primăriei nu folosește protocoalele securizate de comunicare.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
EVALUARE ȘI PREGĂTIRE PERSONAL				
MANAGEMENT JURIDIC AL CONTRACTELOR, IN VEDEREA CONFORMARII CU POLITICA GDPR				

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR

ANALIZA ELEMENTELOR DE NECONFORMITATE ÎN RAPORT CU REGULAMENTUL UE NR.679/2016 PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL ȘI SOLUȚII DE OPTIMIZARE

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
ORGANIZAREA ȘI MANAGEMENTUL SECURITĂȚII INTERNE			
1.	Lipsa unor documente specifice de planificare şi organizare a activităţii de securitate a informaţiei, subliniind aici lipsa unei politici de securitate formalizate printr-un document programatic, avizat de conducerea Primăriei şi în fapt, lipsa unor prevederi clare privind calitatea serviciilor pe zona securității informatice, dar și responsabilităților pe linia administrării serviciilor tehnice informatice, coroborate cu lipsa unor clauze sancţionatorii cuantificabile.	- Crearea documentației specifice pentru politicile de securitate implementate. - Stabilirea responsabilului cu securitatea infrastructurii IT a Primăriei și stabilirea unor responsabilități clare pentru persoana numită. - Stabilirea modalităților clare de sancționare a persoanei numite resonsabil cu securitatea infrastructurii IT pentru neîndeplinirea sarcinilor.	
2.	Lipsa unei persoane încadrate în funcția de DPO (Data Protection Officer) în Primărie sau externalizarea serviciului..	- Numirea unui DPO din cadrul Primăriei; - Stabilirea clară a responsabilităților și obiectivelor de performanță; - Instruirea și pregătirea continuă a acestuia.	
3.	Lipsa responsabilităților în domeniul managementului și administrării securității sistemului informatic intern și a infrastructurii informatice ale Primăriei precizate clar în procedurile interne și stabilite prin fișa postului pentru o persoană din cadrul Primăriei.	Numirea și responsabilizarea clară a unei persoane privind administrarea de securitate a Primăriei prin: - Precizarea clară a administrării de sistem, a administrării de securitate și a protecției resurselor informaționale; - Precizarea clară a calității serviciilor oferite și a responsabilităților. Persoana numită administrator de sistem nu poate îndeplini în același timp și funcția de administrator de securitate și mai ales pe cea de DPO, datorită incompatibilității descrise în Regulamentul European al protecției datelor cu caracter personal.	
4.	Nu sunt nominalizate persoanele care îndeplinesc funcțiile de administrator de securitate și administrator de sistem.	- Numirea unei persoane cu competențe specifice pe poziția de administrator de securitate; - Instruirea și pregătirea continuă a acestuia; - Numirea unei persoane cu cumpetențe specifice pe poziția de administrator de sistem;	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
		- Instruirea și pregătirea continuă a acestuia;	
5.	Inexistența în cadrul Primăriei a unei persoane responsabile pe domeniul securității care să coordoneze modul de asigurare a securității datelor și informațiilor cât și organizarea și administrarea internă a securității pentru protecția datelor fapt care poate genera lipsa unui management pe acest domeniu si apariția unor breșe de securitate.	- Numirea unei persoane cu competențe specifice pe poziția de coordonator al implementării și gestionării sercurității informatice; - Instruirea și pregătirea continuă a acestuia;	
6.	Nu sunt implementate şi nu sunt însuşite de personalul propriu, strategiile de securitate cu privire la protecţia datelor cu caracter personal;	- Elaborarea strategiilor de securitate specifice primăriei, conform raportului de evaluare; - Instruirea personalului intern al Primăriei cu privire la mudul în care aceste strategii de securitate se aplică pentru fiecare departament în parte; - Adaptarea continuă a strategiilor de securitate conform ultimelor descoperii în domeniul;	
7.	Nu sunt precizate clar în contractele cu Companiile de prestări servicii informatice responsabilitățile în domeniul managementului securității interne privind dezvoltarea, mentenanța și hosting-ul pentru site-ul web, precum și pentru dezvoltarea aplicațiilor de management al bazelor de date sau în procedurile interne, prin care Primăria își rezervă drepturile de exercitare a controlului privind implementarea măsurilor de securitate informatică prin controale inopinate, inspecții și evaluări tehnice, pe baza unui raport QoS.	- Includerea unor clauze contractuale clare privind managementu securității interne prin anexe pentru contractele pe care Primăria le are sau urmează să le încheie cu Companiile de prestări servicii informatice.	
8.	Lipsa clauzelor contractuale clare prin care sa se reglementeze: modul de asigurare a serviciilor informatice, persoanele din cadrul Companiilor de prestări servicii informatice care au acces la infrastructura de reţea a Primăriei, precum şi responsabilitățile privind asigurarea securităţii cibernetice pentru aplicațile utilizate de Primărie	- Includerea unor clauze contractuale clare privind reglementarea modului de asigurare a serviciilor informatice, prin anexe, pentru contractele pe care Primăria le are sau urmează să le încheie cu Companiile de prestări servicii informatice; - Includerea unor clauze contractuale clare ce fac referire explicită la persoanele din cadrul Companiilor de prestări servicii informatice care au acces la infrastructura de rețea a Primăriei, prin anexe, pentru contractele pe care Primăria le are sau urmează să le încheie cu Companiile de prestări servicii informatice;	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
		- Stabilirea unor clauze contractuale clare, prin anexe la contract, ce stabilesc responsabilitățile privind asigurarea securității cibernetice pentru aplicațile utilizate de Primărie.	
9.	Existența unei imagini incomplete a infrastructurii informatice deținute de Primărie și lipsa documentelor de lucru pe domeniul securității cibernetice interne (documentație sistem informatic, liste utilizatori și drepturi de acces în sistemul informatic, inventar echipamente tehnice, proceduri de back-up/disaster recovery etc.).	- Realizarea unui audit intern sau extern din care să rezulte imaginea completă a infrastructurii informatice a Primăriei și a vulnerabilităților existente; - Realizarea unui audit intern sau extern care să descrie în mod clar, concret și explicit lista utilizatorilor existenți în sistemul informatic și enumurarea drepturilor de acces pe care fiecare dintre acestia le au; - Inventarierea detaliată a echipamentelor tehnice existente în Primărie; - Stabilirea procedurilor de back-up pentru sistemul informatic al Primăriei; - Stabilirea procedurilor disaster recovery pentru sistemul informatic al Primăriei;	
10.	Jurnalele stațiilor de lucru și ale unor elemente componente ale sistemului informatic se rescriu periodic automat, fără a se face salvare și copii de siguranță ale acestora.	- Realizarea unei proceduri interne privind managementul logurilor de sistem pentru sistemul informatic al primăriei.	
11.	Managementul securității se rezumată la managementul utilizatorilor și drepturilor de acces, simpla funcționare a sistemelor informatice și având un grad ridicat de formalism.	- Realizarea periodica a unor teste de penetrare a sistemului informatic al Primăriei și a unui plan de măsuri pentru îmbunătățirea securității sistemului informatic;	
12.	Neaplicarea unitară a unor politici de securitate pe stațiile de lucru.	- Implementarea la nivelul serverului de AD a politiciilor de update automat al sistemului de operare de pe stațiile de de lucru ale Primăriei; - Implementarea unei soluții de antivirus centralizată la nivel de server	
13.	Accesarea de către personalul Primăriei a sistemelor informatice, printr-un cont de utilizator cu drepturi de administrator local.	- Eliminarea dreptului de administrator local pentru conturile de utilizator folosite de angajații Primăriei.	
14.	Primăria nu deține procedură de procesare specifică pe linia securității datelor și nici proceduri standard de acces și utilizare a sistemelor informatice de către utilizatori, funcționând în acest sens pe baza cunoștințelor fiecărui utilizator și pe baza unei pregătiri minimale inițiale, la	- Dezvoltarea unei proceduri interne specifice securității datelor în cadrul sistemului informatic propriu; - Adaptarea continuă a procedurilor interne specifice securitații conform ultimelor descoperii în domeniul; - Instruirea periodică a angajaților Primăriei referitor la modul de	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
	angajare.	aplicare al acestor proceduri în cadrul departamentului din care angajatul face parte.	
15.	Activitățile de control de securitate și de audit intern ar trebui să aibă o periodicitate cel puţin anuală, dar nu au fost executate până în prezent.	- Realizarea a cel putin un audit intern de sercuritate pe an;	
16.	Prevenţia evenimentelor nedorinte nu este o preocupare principală în cadrul politicii de securitate, iar măsurile de securitate sunt în marea lor majoritate de tip reactiv la situaţiile apărute.	- Auditarea periodică a securității sistemului informatic propriu.	
17.	Nerespectarea regimului de management a parolelor conturilor de utilizatori din cadrul sistemului informatic al Primăriei.	- Configurarea conturilor de utilizator ale angajaților Primăriei să solicite parolă pentru autentificarea în sistemul informatic; - Parola să fie exprire, cel mult, odată la 3 luni; - Puterea parolei să fie cel puțin mediu și un minim de 9 caractere.	
18.	Obligativitatea angajaților Primăriei de a salva date cu caracter personal pe suport fizic – CD și de transmitere a acestor informații autorităților statului.	- Realizarea unei proceduri interne prin care să se stabilească nominal persoanele responsabile cu salvarea datelor cu caracter personal pe suport fizic – CD, modul de lucru și responsabilitățile pe care aceștia le au;	
	SECURITATEA INFRASTRUCTURII ȘI SISTEMELOR DE TEHNOLOGIE A INFORMAȚIEI		
1.	Lipsa unui sistem de detecție și protecție împotriva intruziunilor (IDS/IPS) implementat la nivelul întregii rețele ca protecție de perimetru și ca soluție complementară de securitate, care să protejeze mediul de rețea, și să poată fi utilizată pentru eficientizarea managementului de securitate.	- Implementarea la nivelul întregii rețele a unui sistem împotriva intruziunilor (IDS/IPS)	
2.	Lipsa unei soluții de tip SIEM (securitatea informațiilor și managementul evenimentelor) dimensionate corespunzător numărului de stații pentru colectarea și monitorizarea automată și activă a logurilor de securitate și accesului la date cu caracter personal, ca soluție integratoare de securitate. La momentul evaluarii, log-urile de securitate (fișierele jurnal) la nivel de utilizator nu sunt salvate/stocate într-o zonă de memorie separată, cu	- Implementarea unei soluții SIEM pentru monitorizarea activității din rețea. - Crearea pe server a unei zone de memorie dedicată păstrării logurilor echipementelor din infrastructura IT a Primăriei; - Analiza regulată a logurilor stocate. - Securizarea accesului la zona de memorie de pe server unde sunt stocate logurile de sistem și	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
	acces limitat și nu sunt analizate de către responsabilul cu securitatea, deoarece în sistem nu există o politică de management a log-urilor de securitate aplicată tehnic. De asemenea, procesele de modificare/ștergere/corectare a datelor cu caracter personal nu pot fi documentate cu exactitate în timp.	permiterea accesului pentru administratorul de sistem și DPO;	
3.	Neimplementarea unitară a unei soluții profesionale anti-spam, anti-malware, anti-ransomware.	- Implementarea la nivel de server a unei soluții profesionale antivirus, antispam, antimalware, antiransomware care să monitorizeze activitatea întregii rețele.	
4.	Stocarea datelor cu caracter personal în toate bazele de date interne în clar, fără instrumente de criptare și pseudoninimizare și fără posibilitatea de a păstra o evidență electronică completă a activităților de prelucrare/modificare/ștergere prin monitorizare activă și salvare de log-uri ale utilizatorilor.	- Acolo unde este cazul implementarea unor modalități de criptare, pseudonimizare a datelor stocare în baza de date; - Criptarea zone de memorie de pe server unde bazele de date sunt stocate, pentru cazul în care nu se pot salva într-o manieră criptată datele în baza de date.	
5.	Neexecutarea periodică a testelor pentru securitatea infrastructurii informatice a Primăriei și nerealizarea sistematică a update-urile software și patch-urile de securitate.	- Realizarea testelor de sercuritate a infrastructurii informatice a Primăriei, cel puțin o dată pe an; - Configurarea politicilor de update automat la nivel de server.	
6.	Lipsa controlului porturilor de tip USB și a mediilor de stocare externe, prin politici de securitate manuale instalate pe stațiile client sau printr-un sistem automat.	- Configurarea sistemului informatic al Primăriei pentru a permite doar citirea de pe porturile USB și doar acolo unde este necesar pentru buna desfășurare a activității departamentului permiterea scrierii pe porturile USB; - Realizarea unor proceduri interne prin care se stabileste cine are dreptul de a scrie pe porturile USB ale statiei de lucru și cadrul organizațional în care să își desfășoare activitatea.	
7.	Lipsa controlului sistemelor de tipărire prin produse software de jurnalizare.	- Instalarea unei soluții software pentru monitorizarea activității de tipărire.	
8.	Utilizarea de către angajații primăriei a conturilor de acces cu drepturi de administrator local și fără parolă.	- Conturile de acces ale angajatilor la infrastructura informatica a Primăriei să se realizeze prin conturi de utilizator normal, fără drepturi de administrator local și care să necesite autentificare prin parolă. Puterea parolei să fie cel puțin mediu și lungimea de 8 caractere.	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
9.	Lipsa unei politici privind managementul parolelor de acces la sistemele informatice și la aplicațiile specializate în care se procesează date cu caracter personal.	- Configurarea conturilor de utilizator conform cu punctul 8; - Configurarea valabilității parolei nu mai lungă de 90 zile (3 luni).	
10.	Accesul la rețeaua LAN a Primăriei se face automat în momentul în care calculatorul este conectat la rețea.	- Filtrarea accesului la rețeaua LAN a Primăriei pe baza adresei MAC a echipamentului conectat.	
11.	Accesul la rețeaua WLAN a Primăriei se face folosind parola specifică.	- Separarea rețelei WLAN a Primăriei în două rețele separate, una pentru vizitatori care oferă doar accesul la resursele Internet, la care se poate conecta pe baza de parolă și o a doua rețea pentru angajații Primăriei care să permită accesul la infrastructura informatică a Primăriei. SSID-ul acestei a doua rețea să nu fie vizibil și accesul la aceasta să se facă pe bază adresei MAC a echipamentului conectat.	
12.	Existența unei singure rețele de WIFI la care se pot conecta atât angajații primăriei în interes de sericiu cât și vizitatorii.	- Conform punctului 11 din prezentul raport.	
13.	Inexistența unui firewall hardware dedicat pentru sistemul informatic al Primăriei, care să protejeze sistemul informatic al Primăriei împotriva accesului neautorizat la date din exterior	- Achizitionarea şi configurarea unui firewall hardware dedicat pentru protejarea reţelei interne a Primăriei de atacurile din exterior.	
14	Inexistența unui controler de domeniu și a unui server de Active Directory (AD) care să gestioneze unitar conturile de utilizatori ale angajaţilor Primăriei, să permită aplicarea unei politici uniforme de securitate și să ofere facilități centralizate de management al accesului angajaților la resursele informatice ale Primăriei.	- Configurarea unui calculator cu functie de AD şi gestionarea utilizatorilor şi drepturilor de acces la reţeaua informatică a Primăriei centralizat din serverul de AD. Dacă este necesar achizitionarea unui calculator nou care să deservească acestui scop.	
15.	Folosirea sericiilor externe de FTP (WeTransfer).	- Configurarea unui server intern de FTP, folosind protocoalele secure pe care Primăria să îl folosească pentru a transmite fișiere de dimensiuni mari către Terți sau pe care angajații Primăriei să îl folosească pentru a transmite intern fișiere;	
16.	Lipsa unor politici de tip white list sau black list pe ruterul central pentru a împiedica accesul la resursele de internet care compromit securitatea datelor și a rețelei de calculatoare a Primăriei.	- Restricționarea accesului la resursele de Internet, pe principiul nevoii de a cunoaște, pentru angajații Primăriei folosind fie politicile de tip White List fie politicile de Black List.	
17.	Inexistența unei soluții profesionale de back-up.	- Configurarea unei soluții profesionale de back-up.	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
18.	Folosirea pe stațiile de lucru ale Primăriei, de către angajați, atât a conturilor de email personale cât și a celor de serviciu.	- Introducerea în cadrul politicilor de limitare a accesului la resursele de Internet a adreselor pentru serverele de email altele decât cel al Primăriei dar și la Rețelele de socializare și Web WhatsUp.	
19.	Lipsa criptării unităților de memorie pentru stațiile de lucru pe care sunt procesate date cu caracter personal.	- Criptarea unităților de memorie a stațiilor de lucru pe care sunt procesate date cu caracter personal.	
20.	Folosire de către angajații Primăriei a telefoanelor cu tehnologia de dual sim pentru a avea și numărul personal și numărul de serviciu în același telefon.	- Securizarea accesului la telefon prin activarea unui mecanism de autentificare: recunoaștere facială, amprentă, parola sau simbol în funcție de modelul telefonului; - Activarea pe telefon a serviciilor de formatare la distanță și găsire telefon; - Configurarea unui client pentru o soluție software centralizată care să permită stergerea datelor de pe telefon de la distanță; - Realizarea unor proceduri înterne de lucru cu telefoanele mobile și de comunicare a deposedării.	
21.	Stocarea locală, în memoria telefonului a datelor cu caracter personal procesate.	- Salvarea datelor în soluția de cloud oferită de producătorul telefonului; - Folosirea telefonului doar ca terminal de acces la datele stocate în cloud;	
22.	Lipsa unor modalități de sercurizare a accesului la datele din telefoanele angajaților Primăriei.	- Securizarea telefoanelor modile conform punctelor 17 și 18 din prezentul raport.	
23.	Lipsa unei politici centralizate pentru activarea ștergerii de la distanță a telefoanelor pierdute / furate.	- Securizarea telefoanelor modile conform punctului 17 din prezentul raport; - Dezvoltarea unor proceduri interne prin care să se detalieze modul de prin care sunt sterse telefoanele mobile de la distanță.	
24.	Lipsa unei politici interne pentru gestionarea unităților optice.	- Configurarea sistemului informatic al Primăriei pentru a permite doar citirea datelor de pe unitățile optice și doar acolo unde este necesar pentru buna desfășurare a activității departamentului permiterea scrierii datelor folosind unitățile optice; - Realizarea unor proceduri interne prin care se stabileste cine are dreptul de a scrie date folosind unitățile optice și cadrul organizațional în care să	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
		își desfășoare activitatea.	
25.	Lipsa unei politici interne privind modul cum sunt stocate datele cu caracter personal de către angajați pe telefoanele de serviciu sau cele personale care conțin și cartela SIM de serviciu.	- Realizarea unor politici interne privind modul de stocare al datelor pe telefoanele mobile ale angajaților astfel încât aceștia să le poată folosi într-un mod sigur și securizat.	
26.	Lipsa unei politici interne pentru securizarea leptopurilor pentru a preveni accesul neautorizat la datele salvate pe unitatea de stocare internă.	- Realizarea unor politici interne privind modalitățile de securizare a leptopurilor.	
27.	Conturile de email pe care Primăria le utilizează nu folosesc versiunile securizate ale protocoalelor de comunicare.	- Cofigurarea serverului de email al Primăriei să folosească versiunile securizate ale protocoalelor de comunicare; - Configurarea clienților de email pentru a se conecta la serverul de email folosint protocoalele securizate;	
	EVALUARE ȘI PREGĂTIRE PERSONAL		
28.	Posibilitatea conectării la bazele de date cu caracter personal și la sistemele informatice ale Primăriei utilizând credențialele altui utilizator sau parole implicite salvate in cache-ul sistemelor/ aplicațiilor.	Interzicerea conectării cu credențialele altor utilizatorilor interni, prin intermediul unei proceduri interne.	30.04.2020
29.	Stocarea datelor cu caracter personal în format nestructurat, pe stațiile de lucru, deși Primăria deține bazele de date structurate în cadrul aplicațiilor de sistem de dezvoltate de companiile informatice.	Interzicerea prin procedură internă a salvării de date cu caracter personal în alte locuri decât bazele de date structurate operaționale la nivelul serverelor Primăriei concomitent cu respectarea principiului minimalității.	30.04.2020
30.	Utilizarea resurselor informatice aparținând Primăriei pentru interese personale, în timpul serviciului (acces la rețele de socializare, activități de chat electronic, vizualizare/descărcare, acces video-contet, conturi de torent, copiere date personale de pe medii USB).	Reglementarea acestei practici prin procedură internă, concomitent cu implementarea soluțiilor de tip ACCES cu TOKEN și a implementării unor profile de securitate organizaționale diferite.	Martie 2020/ Ianuarie 2021
31.	Angajații pot conecta telefoane mobile, device-uri externe și medii de stocare personale la sistemele informatice de la birou.	Interzicerea/limitarea acestei practici. Managementul porturilor USB.	30.04.2020
32.	Necunoașterea prevederilor noii politici GDPR, referitoare la definirea, colectarea, procesarea, stocarea și ștergerea datelor cu caracter personal.	Realizarea unui curs de instruire specializat cu toți operatorii fie în format WEB BINAR fie pe categorii de personal pentru cunoașterea noilor prevederi GDPR.	30.06.2020

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
33.	Nu există și nu pot fi aplicate proceduri standard de colectare, procesare, stocare, ștergere și transmitere a datelor cu caracter personal prelucrate de Primărie.	Conștientizarea persoanelor autorizate de către operator prin prevederea responsabilităților respectării noilor proceduri, la nivelul fișelor postului.	
34.	Lipsa instruirii personalului pentru cunoașterea prevederilor politicii GDPR referitoare la colectarea, stocarea și procesarea datelor cu caracter personal.	Aplicarea prevederilor de la punctele 31 și 32, precizate mai sus.	30.06.2020
35.	Utilizarea resurselor informatice aparținând Primăriei pentru interese personale, în timpul serviciului (acces la rețele de socializare, activități de chat electronic, vizualizare/descărcare, acces video-contet, conturi de torent, copiere date personale de pe medii USB).	Reglementarea acestei practici prin procedură internă, concomitent cu implementarea soluțiilor de tip ACCES cu TOKEN și a implementării unor profile de securitate organizaționale diferite.	Martie 2020/ Ianuarie 2021
MANAGEMENT JURIDIC AL CONTRACTELOR, IN VEDEREA CONFORMARII CU POLITICA GDPR			
36.	Lipsa clauzelor contractuale ce stabilesc obligația de protecție a datelor cu caracter personal și răspunderea pentru incidentele de securitate apărute.	Completarea contractelor cu clauze specifice GDPR, în vederea conformării cu politica GDPR și evitarea angajării răspunderii pentru faptele terților.	Odată cu prelungirea, prin act adițional a contractelor ajunse la termen sau prin completarea celor în vigoare și care se prelungesc automat, dar nu mai târziu de luna Aprilie 2020.
37.	Nu există clauze care să stabilească obligația de protecție a datelor cu caracter personal și nici consimțământul potențialului angajat pentru prelucrarea acestora.	Includerea în contracte a unui paragraf specific prin care acesta să-și exprime consimțământul privind prelucrarea datelor cu caracter personal și posibilitatea retragerii acestui acord.	Aprilie 2020 și apoi permanent.

Constantin Bonea
Specialist protecția datelor cu caracter personal
Manager Securitatea Informației

Inițiator
Megyeri Tamás-Róbert
Primarul comunei Căpleni

Marian Duminică
Specialist protecția datelor cu caracter personal
Specialist informatician

Avizat
Csizmar Erika
Secretar general