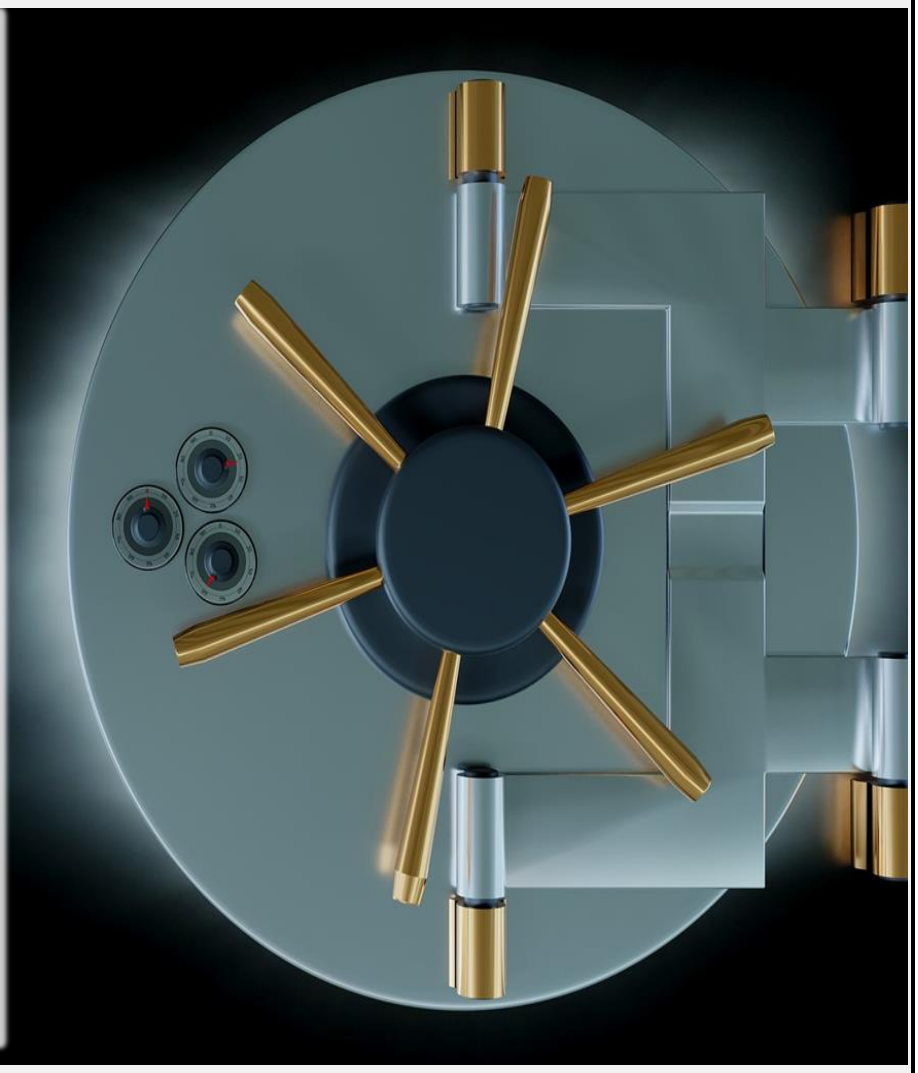
Raport privind măsurile de protecție a datelor personale

Ghid introductiv

Iulie 2019



7 recomandări privind măsurile tehnice și organizatorice esențiale pentru protecția datelor cu caracter personal conform cerințelor Regulamentului UE 679/2016.

Ghid introductiv destinat uzului intern în scop instructiv.

Trusteos SRL
București, str. Ion Nistor nr.4
Tel.: 0727 077 111
www.trusteos.org

Cuprins

De ce este importantă protecția datelor cu caracter personal?

Drepturile și libertățile fundamentale includ respectarea:

- ✓ vieții private și de familie,
- ✓ reședinței și comunicațiilor,
- ✓ libertății de gândire, de conștiință și de religie,
- ✓ libertății de exprimare și informare,
- ✓ libertății de a desfășura o activitate comercială,
- ✓ dreptului la o cale de atac eficientă și la un proces echitabil,
- ✓ diversității culturale, religioase și lingvistice.

Protecția datelor cu caracter personal este vitală pentru asigurarea unui climat de încredere, care să permită progresul economic și social în condiții de securitate și justiție, transparență și libertate de circulație.

Accesul fraudulos la datele cu caracter personal amenință în mod direct drepturile și libertățile fundamentale, îngrădind libertatea de gândire și exprimare, limitând accesul la un proces echitabil, restricționând libertatea de a desfășura o activitate comercială.

Valoarea datelor cu caracter personal este suficient de atrăgătoare pentru infractorii cibernetici. Astfel, aceștia dedică resurse considerabile și timp pentru găsirea și exploatarea unor vulnerabilități care să le confere acces neautorizat la informații pe care le pot transforma în bani, fie prin vânzarea lor, fie prin obținerea unor recompense pentru deblocarea lor.

Evoluţiile tehnologice rapide şi globalizarea au generat noi provocări pentru protecţia datelor cu caracter personal. Amploarea colectării şi a schimbului de date cu caracter personal a crescut în mod semnificativ.

Tehnologia permite atât societăţilor private, cât şi autorităţilor publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităţilor lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informaţii cu caracter personal. Tehnologia a transformat deopotrivă economia şi viaţa socială.

Ce este de făcut?

Protecția datelor cu caracter personal este necesară la nivelul fiecărei activități de prelucrare, *din momentul conceperii și în mod implicit*, conform cerințelor Regulamentului UE 679/2016 (cunoscut ca „GDPR" sau „RGPD").

Acest raport are scopul de a vă pune la dispoziție informații esențiale, menite să vă ajute să vă continuați activitatea într-un climat de încredere, cu o siguranță îmbunătățită pentru angajați, clienți, colaboratori, asociați și alți parteneri.

Veți economisi timp prețios, concentrându-vă asupra afacerii dumneavoastră, fără să fie nevoie să căutați și să sortați tot felul de soluții improvizate și riscante. Punând în practică recomandările acestui raport, veți beneficia de un grad sporit de protecție a datelor cu caracter personal pe care le prelucrați.

Acordați atenția cuvenită fiecărei recomandări din acest raport. Veți putea reveni la concluzii ori de câte ori veți avea nevoie. Ar fi cel mai bine să începeți imediat aplicarea acestora, întrucât realitatea se schimbă rapid.

De regulă, recomandările urmăresc trei direcții:

- incidentele cibernetice;
- solicitările și reclamațiile;
- controalele autorităților.

Această abordare are la bază studierea perioadei de aplicare a reglementărilor GDPR începând cu 25 mai 2018, data intrării lor în vigoare. De asemenea, au fost luate în considerare și informații anterioare acestei date, din perspectiva unor decizii definitive ale instanțelor interne și internaționale în privința protecției datelor cu caracter personal.

Recomandările au caracter informativ. Răspunderea revine fiecărui cititor pentru aplicarea lor corectă. De cele mai multe ori, este necesară personalizarea soluțiilor de la caz la caz, în funcție de contextul și specificul fiecărei situații.

Măsuri tehnice și organizatorice esențiale

Vă recomandăm să aplicați aceste recomandări fără întârziere. Mai târziu, veți avea nevoie de informații noi, actualizate. Amânarea utilizării acestora poate crește riscul apariției unor situații neplăcute. Costurile lipsei de pregătire pot fi copleșitoare.

Aceste recomandări au la bază experiența și testele efectuate de asociații profesionale și autorități specializate în securitate cibernetică, din mai multe țări. De asemenea, unele dintre concluzii au fost cuprinse în rapoarte complexe de audit, pentru care beneficiarii au plătit onorarii consistente.

Cine își mai desfășoară astăzi afacerile la întâmplare? Fără o minimă pregătire, șansele de eșec vor fi mai mari decât cele de succes. Cei mai mulți întreprinzători răspund atât pentru ei înșiși, cât și pentru cei din jur, care depind de ei:

- ✓ Familie,
- ✓ Angajați,
- ✓ Clienți,
- ✓ Furnizori,
- ✓ Etc.

Aceste relații rămân valabile și în privința protecției datelor cu caracter personal, care li se aplică și familiilor angajaților, clienților, furnizorilor și celorlalte persoane ale căror date le prelucrați.

Recomandarea #1: informați și instruiți

Indiferent de domeniul de activitate pe care l-ați ales, într-o formă sau alta, la un moment dat operațiunile dumneavoastră necesită interacțiunea cu alte persoane. Prelucrarea datelor cu caracter personal ale acestora va solicita anumite măsuri de precauție. Cum procedați?

În primul rând, vă informați și vă asigurați că toți oamenii din firma dumneavoastră primesc informații despre obligațiile legate de prelucrarea datelor cu caracter personal, conform reglementărilor.

Instruirea include prezentarea informațiilor într-un mod sistematic, care verifică înțelegerea și asimilarea cunoștințelor, în scopul punerii lor în practică. Pentru unele

persoane, instruirea va include modificarea unor obișnuințe, renunțarea la anumite obiceiuri.

De exemplu, deseori se culeg și stochează informații fără măsuri de protecție, adică fără o parolă de acces, fără asigurarea unor măsuri de protecție fizică. Sau, când se utilizează o parolă, aceasta este foarte simplă, de genul *1234* sau *aaaa*.

În alte situații, aceeași parolă este folosită pentru acces la informații diferite, atât online cât și pentru documente electronice stocate pe propriile sisteme informatice. Uneori, parola este comunicată altor persoane sau scrisă într-un loc unde poate vedea oricine.

Este necesar să-i instruiți pe oameni în privința riscurilor cibernetice, care pot fi concretizate prin atacuri vizând accesul neautorizat la date sau prin pierderi provocate de neglijență sau lipsă de informare.

De exemplu, accesarea unor fișiere anexate la mesaje de email poate avea consecințe neplăcute și poate genera costuri greu de suportat. Instruirea poate preveni multe astfel de situații, dacă oamenii știu să sesizeze mesajele suspecte și să evite acțiunile riscante.

Recomandarea #2: protejați-vă sistemele informatice

Desfășurarea unei activități economice este aproape imposibilă fără sisteme informatice. Este necesară utilizarea unor măsuri tehnice de protecție, pornind de la actualizarea imediată a sistemelor de operare și instalarea unui elementar program *antivirus*, care poate fi obținut chiar și gratuit, până la implementarea unor politici de utilizare a acestor sisteme.

Unele lucruri se pot face cu un minim de abilități tehnice, de utilizatori obișnuiți. Soluțiile mai complexe solicită susținerea unor experți, care să neutralizeze cât mai multe vulnerabilități și să prevină majoritatea riscurilor importante.

De cele mai multe ori, chiar și atunci când aveți nevoie de soluții care poartă costuri ridicate, gândiți-vă că incidentele costă de zeci de ori mai mult. Un singur incident vă poate bloca activitatea mai multe zile, poate atrage sancțiuni ale autorităților și reacții negative de la clienți și alți parteneri.

De exemplu, numai în 2018, oficiali și funcționari ai Marii Britanii au pierdut mai mult de 500 de sisteme informatice! Toate acestea au fost considerate incidente. Efectele negative au fost mai reduse, atunci când datele aflate pe aceste sisteme erau protejate prin criptare.

Așadar, vă recomandăm să dezactivați setările predefinite ale sistemelor și să le personalizați. De asemenea, alocați parole unice fiecărui utilizator care prelucrează date personale, definind un nivel de acces limitat, în funcție de nevoi. Criptați datele.

Administrați utilizatorii sistemelor informatice, monitorizați activitatea acestora, pentru a detecta mai ușor activitățile neobișnuite sau suspecte. Interveniți și corectați imediat, atunci când este necesară remedierea unor erori.

Recomandarea #3: folosiți regulamente, proceduri, politici

Activitățile se desfășoară mai eficient, atunci când există un cadru și o distribuție cunoscută a rolurilor. Regulamentul de ordine interioară este necesar. De asemenea, este utilă aplicarea unor proceduri clare și ușor de urmat.

De exemplu, atunci când cineva primește un email suspect, va urma procedura de anunțare a persoanei responsabile cu securitatea informatică în firma dumneavoastră. Va urma instrucțiunile acestei persoane și va putea contribui la prevenirea unui incident.

Politicile pot stabili în ce modalitate este permis accesul diferențiat pe nivele de securitate pentru utilizatorii sistemelor informatice. De asemenea, veți putea urmări deazctivarea permisiunilor a căror necesitate a expirat și veți putea face modificările necesare, atunci când doriți să limitați anumite drepturi de acces sau să le extindeți.

Echipamentele pe care le utilizați în mod curent au nevoie de anumite configurații și de mentenanță. Normele interne, pe care le stabiliți dumneavoastră, vor prevedea și modalitatea în care aceste echipamente vor fi gestionate.

De asemenea, tot în aceste reguli, proceduri și politici se vor regăsi detaliile privind rolurile și responsabilitățile, inclusiv ierarhice. Totodată, vă recomandăm să precizați canalele de comunicare și perioadele de timp pentru situațiile uzuale.

De exemplu, concediile se solicită în scris, iar *cererile* se depun la responsabilul cu resursele umane cu cel puțin 30 zile înainte de prima zi de concediu solicitată. *Mesajele email* considerate suspecte se anunță imediat responsabilului cu securitatea informatică, prin cel mai eficient mijloc posibil – personal, dacă este prezent în locație, telefonic sau SMS, dacă se află într-o locație diferită.

Un alte exemplu se referă la politica privind dispozitivele personale, conectate la sistemele informatice ale firmei. În principiu, dacă este permisă conectarea unor

dispozitive personale la sistemele informatice ale firmei, atunci acest lucru se va face numai în anumite condiții stricte de securitate, pentru a vă proteja.

Aceste reguli, proceduri și politici vor avea nevoie de actualizări periodice, pentru a răspunde nevoilor. Evoluția continuă solicită adaptarea permanentă a capacității de administrare a informațiilor noi, cu o viteză amețitoare.

Aceste reguli, proceduri și politici vă înlesnesc operațiunile curente și vă îmbunătățesc flexibilitatea afacerii. Veți face față mult mai bine cererilor de la clienți, depășindu-le așteptările și oferindu-le satisfacții, fidelizându-i.

În cadrul acestor regulamente, proceduri și politici, va fi nevoie să faceți referire la anumite documente specifice, utilizate în cadrul firmei. Vă recomandăm să le standardizați, folosindu-le în mod uniform și adecvat cu cerințele reglementărilor. Desemnați persoane responsabile cu aplicarea și monitorizarea acestora.

Recomandarea #4: Actualizați-vă formularele interne și externe

Cu siguranță, activitățile obișnuite ale firmei dumneavoastră includ completarea și transmiterea unor formulare și documente tipizate. Fie că le-ați generat intern, cum ar fi diverse *cereri* și *fișe*, fie că au un format specific reglementărilor contabile sau de altă natură, acestea au intrat în rutină.

Pentru multe firme, apariția GDPR a semănat confuzie în privința documentelor. Unii au modificat toate documentele existente și au adăugat altele noi, create după propria interpretare a cerințelor regulamentului. Alții au cumpărat, pur și simplu, machete pe care le-au introdus în activitățile lor. Cum este cel mai bine?

De exemplu, indiferent de domeniul de activitate, foarte multe firme folosesc un formular tipizat de *acord.* Îl solicită semnat de clienți, de angajați, de orice persoană care interacționează cu firma. Oare, așa trebuie?

Consimțământul este, pe de o parte, doar unul dintre temeiurile legale pentru prelucrarea datelor personale. Pe de altă parte, există ghiduri complexe privind utilizarea consimțământului, emise de autorități.

Pentru a fi valabil, este necesar ca acest *acord* să îndeplinească o serie de condiții. Așadar, răspunsul este complex. Depinde de situație. În toate cazurile, însă, este necesar să *informați* persoanele ale căror date urmează să fie prelucrate. Le veți comunica mai multe lucruri, începând cu datele de identificare ale firmei, până la

drepturile persoanelor vizate și modalitatea de exercitare, scopul și durata prelucrării și alte informații obligatorii.

Așadar, vă recomandăm ca toate documentele care se utilizează în activități de prelucrare a datelor cu caracter personal să includă această *informare* privind datele de identificare, drepturile persoanelor, temeiul prelucrării, scopul prelucrării, durata, etc.

Din punct de vedere al documentelor pe care le utilizați în prezent, vă recomandăm să le studiați, pentru a decide pe care le veți modifica, pe care le veți înlocui și pe care le veți păstra. De exemplu, fișele de inventar pot rămâne la fel. O serie de documente vor include elementele obligatorii prevăzute de reglementările aplicabile.

Acordați atenție sporită documentelor care includ date personale ale angajaților și persoanelor cu care interacționează firma dumneavoastră. De asemenea, registrele și bazele de date vor avea nevoie de măsuri speciale pentru conformarea cu GDPR. Stocați-le în dulapuri închise, în camere cu acces controlat.

Circuitele acestor documente vor avea nevoie de atenție specială, de asemenea. Copierea lor, stocarea lor, distrugerea lor și orice operațiuni de transfer sau altă formă de prelucrare se vor supune cerințelor privind protecția datelor cu caracter personal.

Recomandarea #5: creați copii de rezervă

Oricâte măsuri de precauție își ia cineva, este nevoie să se pregătească și pentru a putea reacționa, atunci când un incident apare, totuși. Capacitatea de restaurare a unei stări anterioare incidentului este foarte importantă. De asemenea, este și o obligație legală. Majoritatea sistemelor informatice au posibilitatea de a reconstitui starea la un moment anterior apariției unui incident. Vă recomandăm să activați această opțiune.

Copiile de rezervă constituite periodic vor fi gestionate în funcție de importanța lor. Vă recomandăm să le păstrați în condiții de siguranță, izolându-le de celelalte medii de lucru și de stocare, fără acces public, în formă criptată.

Crearea copiilor poate genera o problemă de spațiu de stocare. Din acest motiv, recomandăm identificarea informațiilor critice și începeți cu protejarea acestora. Puneți în balanță costurile și luați măsuri proporționale cu nevoile, fără a copleși bugetul de care dispuneți. Ideal ar fi să reușiți să clasificați riscurile și să le evitați pe cele mai periculoase, atât ca gravitate, cât și ca probabilitate de apariție.

Recomandarea #6: comunicați eficient

Comunicarea este vitală, inclusiv pentru îmbunătățirea securității cibernetice. Pe lângă informațiile care circulă în interiorul firmei dumneavoastră, vă recomandăm să acordați atenție și comunicării constructive cu partenerii dumneavoastră – furnizori, clienți, etc. și cu publicul larg.

Stabilirea unor relații solide va contribui la creșterea vitezei de reacție în cazul apariției unor amenințări cibernetice. Alte beneficii pot veni din aprecierea pe care o veți primi pentru seriozitatea cu care tratați securitatea tranzacțiilor pe care le derulați și, implicit, pentru preocuparea dumneavoastră de a proteja siguranța clienților.

Totodată, veți identifica noi oportunități și veți dobândi acces la resurse suplimentare, pentru a face față cerințelor operaționale. Veți putea crea un plan de acțiune și veți putea lua parte la planurile de acțiune ale partenerilor și colaboratorilor, în condiții optime, minimizând eventualele pierderi generate de incidente.

Prin comunicare eficientă, puteți împărtăși din experiențele dumneavoastră, puteți adresa întrebări și primi răspunsuri din comunitatea la care luați parte, puteți contribui cu soluțiile pe care le-ați identificat și testat, ajutându-i pe alții.

Recomandarea #7: testați, verificați, controlați

Toate recomandările anterioare au un grad ridicat de importanță. Ar mai fi și alte recomandări de aplicat. Esențial este să începeți cu acestea, cel puțin. Veți turna o fundație solidă pentru afacerea dumneavoastră. Consolidarea edificiului depinde de trăinicia fundației. Astfel, poate că recomandarea cea mai importantă este aceasta.

Testați, verificați și controlați nivelul de aplicare corespunzătoare a cerințelor GDPR în firma dumneavoastră.

Un set de *formulare conforme* vă apără de incidente, în lipsa unui antivirus? Dacă aveți și antivirus, și formulare, este suficient pentru a răspunde solicitărilor și reclamațiilor de la persoanele ale căror date cu caracter personal le prelucrați? Dacă stabiliți reguli, ce siguranță aveți că ele se aplică întocmai?

Verificați dacă se respectă regulile, procedurile și politicile. Revizuiți-le periodic. Unele teste pot fi făcute automat. Altele au nevoie de intervenție specializată, cum ar fi *evaluările de impact* (DPIA). Timpul erodează, oamenii pot să uite reguli și să neglijeze proceduri, sub presiunea timpului sau în virtutea unor obișnuințe.

Controalele au menirea să funcționeze asemeni unor macazuri sau borne de referință cu capacitate de activare a unor alerte. Cum depistați o problemă? Cum sesizați un incident? Cum clasificați, abordați și reduceți riscurile cele mai importante, în ordinea gravității și a probabilității de apariție?

O privire obiectivă și independentă vă poate fi de folos. Un audit are menirea să constate și să evalueze starea de fapt. Concluziile raportului de audit vor fi însoțite de recomandări pentru implementarea unor măsuri tehnice și organizatorice vizând îmbunătățirea situației dumneavoastră.

-//-

Concluzii

Sperăm că aceste recomandări vă vor fi de real folos. Dacă veți aprecia inițiativa noastră și o considerați benefică, vă rugăm să transmiteți acest raport și altor persoane, care credeți că au nevoie de astfel de recomandări.

Ne va face plăcere să vă ajutăm și mai mult, printr-un **audit inițial**, de evaluare a situației actuale a firmei dumneavoastră. Astfel, vom putea elabora un raport mai detaliat, ținând cont de particularitățile specifice activităților pe care le desfășurați.

Participarea la proiecte complexe de audit și implementare GDPR ne permite să furnizăm servicii de calitate, spre satisfacția celor mai exigenți clienți. Garanția noastră este asigurată de certificările multiple pe care le deținem ca profesioniști și de mesajele de mulțumire ale clienților noștri.

Cu siguranță, veți beneficia de mult mai multe recomandări din partea noastră, privind măsurile tehnice și organizatorice necesare pentru a implementa cu succes cerințele GDPR în firma dumneavoastră!

Vă invităm să ne contactați la 0727 077 111 sau info@trusteos.org.

Cu cele mai bune urări,

Radu Chirvase
Manager General
Trusteos SRL

Anexă bibliografică selectivă

Recomandările prezentate au la bază resurse diverse, pe care le puteți consulta, în măsura timpului de care dispuneți. Am extras și vă punem la dispoziție mai jos o listă cu cele mai importante surse de informare utilizate în acest ghid introductiv:

1. https://cert.ro
2. https://dpo-net.ro
3. https://www.ncsc.gov.uk
4. https://iapp.org
5. https://edpb.europa.eu
6. https://ico.org.uk
7. https://gbhackers.com
8. https://healthitsecurity.com
9. https://thehackernews.com
10. https://threatpost.com
11. https://www.infosecurity-magazine.com
12. https://www.bleepingcomputer.com
13. https://securityaffairs.co
14. https://blog.malwarebytes.com
15. https://iaonline.theiia.org