Cuprins

Prefață

Înainte de prefața cărții vreau să vorbesc despre „a scrie în ziua de azi”. Cine mai are nevoie de informații din cărți în epoca platformelor și vitezei, cine mai are timp să citească atunci când ar putea să ia concluziile gândite de alții deja și, pe scurt, oare ce le motivează pe tinerele autoare să scrie?

Nu e mai ușor să plătești publicitate sau să vorbești la o emisiune TV?

Cred că a scrie este o obligație a oricărui intelectual care lucrează cu concepte – atunci când scrii nu ai doar dreptul de exprimare, dar și obligația de a fi consistent. Atunci când scrii și recitești ești și arhitect, și constructor, dar și consumator de idei, altfel nu poți depăși o pagină sau două. Într-o epocă a volumului și vorbitului, este nevoie de mai multă responsabilitate și, înainte de toate, este nevoie să vedem scrisul ca pe o lucrare personală, ca o parte din moștenirea pe care o minte sclipitoare trebuie să se asigure că o transmite și altora, că o împarte cu cititorii.

Trecând mai departe, tema cărții este provocatoare – dreptul ca disciplină este un dinozaur viu, pentru că legile sunt pentru și despre oameni și societăți. Cu fiecare carte scrisă despre legi și despre modul cum funcționăm se clădește o conștiință colectivă a ceea ce înseamnă societate, reguli, ce este acceptabil, despre bine și rău. Pe lângă interes, cartea de față este o lucrare folositoare și întărește nu doar obligația de a scrie, dar și obligația de a interpreta și provoca principiile vechi la noile realități.

Sunt legi și principii vechi de mii de ani, care încă stau la baza relațiilor noastre, și există și legi noi pentru provocări noi – cum este GDPR, consecința avântului globalizării și tehnologizării din viața fiecărui om.

Interesant pentru mine este că citatul din începutul cărții pune legislația GDPR sub semnul vechii bătălii din Lumea Nouă și Bătrânul Continent, aducând demnitatea în centrul societății, ca o valoare esențială a ființei umane. Sunt idei umaniste cărora în sfârșit le-a venit vremea. Eliberat de foame și sclavie sub diferite forme, omul de rând își caută sensul și limitele libertății.

Libertatea de a înțelege ce se întâmplă cu informațiile despre tine, libertatea de a-ți administra opțiunile personale, precum și multe altele detaliate în prezenta carte sunt de fapt o digitalizare a relațiilor omenești în care ideile sunt noile valori și cursa este despre a înțelege opțiunea

maselor. Deciziile în timp real impun reguli în timp real care să reechilibreze balanța de putere între algoritmi și oameni. Legile referitoare la protecția datelor vin să așeze lucrurile în societate și tocmai de aceea acest subiect este nu doar actual, dar mai ales relevant în viitor. Tehnologia și inteligența artificială avansează exponențial. E timpul ca oamenii să înțeleagă cine folosește informațiile, cum arată noua media, de ce personalizarea vine cu prețul viziunii și pentru cine implementăm de fapt GDPR.

Este o mare bucurie și onoare să fiu o mică parte din această lucrare care încearcă să ne aducă mai aproape legile și regulile – care ni se aplică, indiferent dacă le înțelegem sau nu. De fapt, cartea este un exercițiu de (auto)educație și tocmai de aceea vă felicit că o aveți în brațe și vă urez lectură plăcută!

Monica CADOGAN
CEO şi fondator Vivre

GDPR-UL DIN PUNCTUL DE VEDERE AL AFACERILOR (COMPANIILOR/SOCIETĂȚILOR) – IMPACTUL ECONOMIC ȘI ORGANIZAȚIONAL

„A fi european înseamnă a avea dreptul ca datele tale cu caracter personal să fie protejate de legi puternice, europene. Pentru că europenilor nu le plac dronele care zboară pe deasupra lor şi le înregistrează fiecare mişcare, nici companiile care contabilizează fiecare click pe mouse. De aceea, Parlamentul, Consiliul şi Comisia au convenit în mai anul acesta un regulament comun privind protecţia datelor cu caracter personal. Acest regulament este o lege europeană fermă aplicabilă companiilor, indiferent de locul în care îşi au sediul şi ori de câte ori prelucrează datele dumneavoastră cu caracter personal. Pentru că, în Europa, păstrarea confidenţialităţii datelor personale contează. Această chestiune ţine de demnitatea umană”.

Jean Claude Juncker

Tuturor ne place să măsurăm – fie că vorbim despre profit, cifra de afaceri, marjă sau alţi indicatori – ne place să raportăm şi să ne raportam la cifre. În cazul apariţiei GDPR-ului cei mai mulţi s-au raportat la cât business s-a pierdut din cauza apariţiei Regulamentului European, câţi bani s-au cheltuit pe consultanţi, cât timp s-a pierdut pentru a răspunde la chestionare şi câţiva s-au raportat la ce amenzi au avut de plătit.

Mai puţini s-au gândit la ce a însemnat pentru organizaţia lor implementarea unor reguli pentru a respecta GDPR-ul, schimbarea organigramei uneori chiar şi a culturii organizaţionale.

Foarte puţini oameni de afaceri s-au gândit la partea bună a lucrurilor, la securitatea sporită a datelor şi a businessului implicit care a venit o dată cu implementarea GDPR-ului.

Noi, autoarele, ne propunem să explicăm pe înţelesul neprofesioniştilor ce trebuie să întreprindă o societate pentru a se conforma prevederilor GDPR. Astfel, fie că sunteţi juristul din cadrul unei societăţi, fie că lucraţi în departamentul de Marketing sau Resurse Umane, fie că sunteţi chiar administratorul societăţii, ne dorim ca această carte să fie un punct de sprijin pentru călătoria de conformare. Deşi se spune că se poate

preciza cu exactitate momentul începerii implementării, dar niciodată nu se va şti când se va finaliza, GDPR-ul fiind un domeniu în care trebuie menţinută atenţia şi concentrarea pe toată durata de viaţă a societăţii, ne propunem ca limbajul să fie unul accesibil (să ieşim din zona de „păsărească" a specialiştilor), astfel încât să putem sprijini cât mai multe persoane dornice să înţeleagă GDPR-ul. Cartea nu se doreşte a fi una exhaustivă, dedicată specialiştilor, ci este una practică, cu multe exemple din experienţa noastră, a autoarelor – care practică avocatura de afaceri, concentrându-se inclusiv pe protecţia datelor, de mai bine de 17 ani.

După cum se ştie, datele au valoare pecuniară. Având valoare financiară, ele se comercializează pe piaţă. Fac obiectul intermedierilor şi al unui comerţ intens. Analytics, big data, market profiling, inteligenţa artificială (AI), blockchain, IoT (internet-of-things) etc. – sunt doar câteva domenii notorii şi prezente pe piaţa digitală.

Toate domeniile economiei şi finanţelor în activitatea curentă, gestionează baze masive de date (banking, asigurări, servicii medicale private, contabilitate etc.) şi îşi construiesc strategiile pe baza unor intense şi din ce în ce mai sofisticate operaţiuni de profilare şi prelucrare a datelor personale.

Datelor personale le este recunoscută valoarea comercială în mod explicit inclusiv prin Directiva privind Contractele de furnizare de conţinut digital şi de servicii digitale din 26 martie 2019 (ce va trebui transpusă în legislaţia naţională până la 01.07.2021), recunoscându-se datelor personale valoare de piaţă, prin care se achită un serviciu: „*Prezenta directivă se aplică şi atunci când comerciantul furnizează sau se angajează să furnizeze consumatorului conţinut digital sau un serviciu digital, iar consumatorul furnizează sau se angajează să furnizeze comerciantului date cu caracter personal (…)*". Monetizarea, inclusiv pe cale legislativă a valorii datelor personale, este o realitate juridică.

Dar nu doar societăţile din domeniul tehnologiei folosesc baze de date – datele cu caracter personal ale clienţilor sunt folosite de clinici, grădiniţe şi şcoli, magazine online, agenţii de turism şi recrutare etc., dar toate societăţile deţin date cu caracter personal ale angajaţilor.

Deşi se discută atât de mult de General Data Protection Regulation – (Regulamentul General privind Protecţia Datelor), se pare că doar o parte din companiile europene au implementat obligaţiile GDPR (cifrele diferă în funcţie de sursă – mai puţin de jumătate, conform IAPP (International Association of Privacy Professionals) sau două companii din trei, conform unui studiu realizat de RSM pentru European Business Awards[1].

[1] https://www.rsm.global/news/30-european-businesses-are-still-not-compliant-gdpr.

De asemenea, se discută foarte mult de cât costă implementarea normelor GDPR – conform International Association of Privacy Professionals (IAPP), cele mai bogate 500 firme au cheltuit 7.8 miliarde de dolari pe implementarea GDPR, bugetul mediu pentru fiecare firmă fiind de 16.000.000 $. Pe de altă parte, autorităţile naţionale (inclusiv Comisia Europeana) insistă pe faptul că nu ar trebui cheltuite sume foarte mari, ci doar respectate normele impuse de GDPR, pornind de la principiile enumerate în preambulul regulamentului.

Este evident că investiţia în soluţiile de securitate pentru criptarea datelor, asigurarea confidenţialităţii, detectarea posibilelor ameninţări, gestionarea răspunsurilor către persoanele vizate şi mai ales pregătirea permanentă a angajaţilor presupune costuri, existând soluţii scumpe şi soluţii ieftine, procese acoperitoare şi dosare cumpărate „de-a gata" fără a fi implementate.

În ciuda costurilor, majoritatea companiilor au considerat că implementarea GDPR nu a dăunat dezvoltării lor – 65% dintre respondenţi au considerat că GDPR a avut un impact pozitiv asupra afacerii lor şi doar 15% au considerat că GDPR a avut un impact negativ asupra activităţii lor.[2]

La împlinirea unui an de la aplicarea GDPR, Comisia Europeană a publicat un raport conform căruia 67% dintre europeni au auzit de GDPR, în timp ce 57% dintre aceştia ştiu de existenţa unei autorităţi publice în fiecare ţară care se ocupă de protejarea drepturilor lor în ceea ce priveşte datele cu caracter personal şi către care pot trimite plângeri pentru încălcarea acestor drepturi.[3]

Chiar şi în momentul pandemiei – o perioadă dificilă pentru toate statele lumii, în Europa nu s-a oprit discuţia despre GDPR şi despre importanţa datelor cu caracter personal – fie că vorbim despre date de sănătate (temperatură), fie că vorbim despre numele persoanelor infectate sau despre localizarea lor exactă. De asemenea, societăţile au trebuit să îşi completeze politicile privind prelucrarea datelor cu caracter personal pentru cazurile în care angajaţii aveau anumite boli cronice care ar fi presupus o precauţie suplimentară.

Ce este GDPR?

GDPR reprezintă Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor

[2] GDPR Complience Status TrustArc https://info.trustarc.com/Web-Resource-2018-07-12-GDPR-ResearchReport_TYP.html.

[3] https://ec.europa.eu/info/sites/info/files/infographic-gdpr_în_numbers.pdf.

fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).[4] GDRP a fost publicat în Jurnalul Oficial al Uniunii Europene L119/4 mai 2016, a intrat în vigoare la 25 mai 2016 şi este aplicabil din 25 mai 2018 la nivelul întregii Uniuni Europene.

GDPR nu reprezintă o noutate absolută, fiind de fapt doar o adaptare a Directivei 95/46/CE la modificările tehnologice şi cerinţele sporite privind securitatea datelor cu caracter personal.

Se vorbeşte de schimbări extraordinare, unii numesc o revoluţie în domeniul protecţiei datelor – noi vrem doar să punctăm noutăţile din domeniul protecţiei datelor cu caracter personal, subliniind faptul că GDPR:

- sporeşte drepturile individuale ale persoanelor vizate de colectarea şi prelucrarea datelor cu caracter personal;
- lărgeşte spectrul categoriilor de date cu caracter personal;
- impune noi obligaţii operatorilor de date cu caracter personal, precum şi persoanelor împuternicite de aceştia, obligaţii care cu un impact tehnic şi organizaţional;
- stabileşte amenzi semnificative în caz de neconformitate;
- impune în unele cazuri numirea unui DPO (Data Protection Officer – Responsabil de date cu caracter personal), persoană care trebuie să se asigure de aplicarea coerentă a dispoziţiilor legale pentru a da eficienţă acestora faţă de persoanele vizate.

Regulamentul este inclus în categoria documentelor care formează Cadrul european în domeniul securităţii cibernetice alături de alte trei documente (Convenţia privind criminalitatea informatică, Directiva privind măsurile pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice şi Strategia de securitate cibernetică a Uniunii Europene).

Acest regulament a influenţat şi alte legislaţii naţionale, fiind un model pentru Brazilia, Japonia, China, Rusia şi California. În Statele Unite, California a fost primul stat cu o mai bună protecţie a datelor pentru cetăţenii săi. În ceea ce priveşte forma şi conţinutul, acest Act de confidenţialitate a consumatorilor din California (CCPA)[5] este în mod clar comparabil cu GDPR european. De asemenea, în aprilie 2016, Republica Turcia a publicat Legea privind protecţia datelor cu caracter personal w.

„Data protection by design” și „data protection by default”.

[4] http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679.

[5] The California Consumer Privacy Act (CCPA) a intrat în vigoare pe 01.01.2020.

nr. 6698, în Monitorul Oficial. La cererea reprezentanţilor afacerilor turce, termenul pentru această înregistrare a fost amânat pentru 30.06.2020 când autoritatea turcă va putea începe amendarea celor care nu s-au conformat.

Cerut cu insistenţă de asociaţiile de consumatori, scopul a fost acela de a proteja persoanele fizice, mai ales în contextul în care marile corporaţii au folosit şi o parte din ele încă folosesc datele personale în moduri greu de înţeles pentru persoanele obişnuite, precum şi pentru a determina companiile să acorde o atenţie mai mare protecţiei datelor.

„Unul dintre principalele scopuri ale Regulamentului general privind protecţia datelor este de a da mai multă putere oamenilor şi de a le oferi mai mult control asupra uneia dintre cele mai valoroase resurse din economia modernă – datele lor. Putem atinge acest obiectiv numai dacă şi când oamenii devin pe deplin conştienţi de drepturile lor şi de consecinţele deciziilor lor.

Începem deja să vedem efectele pozitive ale noilor reguli. Cetăţenii au devenit mai conştienţi de importanţa protecţiei datelor şi a drepturilor lor. Şi acum îşi exercită aceste drepturi, aşa cum realizează autorităţile naţionale de protecţie a datelor în activitatea lor de zi cu zi. Au primit până acum peste 95.000 de reclamaţii din partea cetăţenilor.” (Declaraţie comună a Vice-Preşedintelui Timmermans, Vice-Preşedintelui Ansip, Comisarului European Jourová and Gabriel, cu ocazia Zilei Internaţionale a Datelor cu caracter personal, 25.01.2019)

Ce sunt datele cu caracter personal?

„Datele cu caracter personal” au fost definite în cadrul Regulamentului ca fiind „orice informaţii privind o persoană fizică identificată sau identificabilă („persoană vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;”

Foarte important de reţinut este faptul că datele personale nu se limitează la elemente uşor de înţeles precum CNP-ul, adresă, nume, adresa de email etc., ci aria este mult mai extinsă în noul regulament, cuprinzând şi informaţii legate de localizarea prin GPS, adrese IP, asigurări, date părinţi şi copii, date biometrice, datele referitoare la preferinţele de cumpărare, religie, sex, etnie sau locul de muncă.

Exemple de date care nu sunt considerate a fi date cu caracter personal:

- CUI-ul/CIF-ul unei societăţi;
- O adresă de e-mail care are formatul info@numecompanie.com, secretariat@numecompanie.ro, vanzari@numecompanie.eu;
- Sediul unei societăţi;
- Datele anonimizate;
- Numărul de telefon al unei societăţi publicat pe pagina sa web.

Normele GDPR se aplică numai datelor cu caracter personal privind persoanele fizice şi nu reglementează datele referitoare la societăţi sau la alte entităţi juridice.

Atenţie! Cu toate acestea, informaţiile legate de societăţi alcătuite dintr-o singură persoană pot constitui date cu caracter personal dacă permit identificarea unei persoane fizice (numele societăţii este Vasile Ion SRL cu sediul la domiciliul domnului Vasile Ion, număr de telefon: numărul de telefon al domnului Vasile Ion).

Atenţie! Normele se aplică, de asemenea, tuturor datelor cu caracter personal referitoare la persoane fizice în cadrul unei activităţi profesionale, cum ar fi angajaţii unei societăţi, precum adresele de e-mail de afaceri ca prenume.nume@societate.ro sau numerele de telefon ale angajaţilor.

În cazul în care este necesar a fi prelucrate date cu caracter personal, acestea ar trebui să fie **adecvate, relevante şi limitate la ceea ce este necesar în scopul respectiv („reducerea la minimum a datelor”).** În calitate de operator, societatea trebuie să evalueze ce volum de date este necesar şi de a se asigura că nu se colectează date irelevante.

Exemplu: În cazul unei societăţi care oferă persoanelor fizice servicii de închiriere a autoturismelor, se vor colecta şi prelucra următoarele date: nume, adresa şi numărul cardului de debit/credit al clienţilor şi, poate, informaţii privind o eventuală dizabilitate de care suferă persoana în cauză (aşadar, date privind sănătatea), dar nu şi de originea rasială/sexul clienţilor.

Cui i se aplică GDPR? Este important unde are sediul o societate pentru a vedea dacă se aplică GDPR?

GDPR se aplică în cazul:

- unei societăţi care prelucrează date cu caracter personal la sediul sau la sediul unei sucursale din UE sau
- unei societăţi care are sediul în afara UE şi oferă bunuri/servicii (contra cost sau gratuit) unor cetăţeni ai unor ţări membre UE sau monitorizează comportamentul unor persoane fizice din UE.

Exemplu când se aplică GDPR: O societate de recrutare cu activitate online şi sediu în afara UE. Aceasta vizează în principal studenţii din UE. Ea oferă consultanţă gratuită cu privire la mai multe slujbe din SUA, iar studenţii au nevoie de un nume de utilizator şi o parolă pentru a accesa materialele online.

Exemplu când nu se aplică GDPR: O societate care este un portal de vânzare şi închiriere de bunuri imobile dintr-o ţară din afara UE. Societatea are sediul în afara UE şi oferă servicii unor persoane din afara UE. Clienţii pot utiliza aceste servicii când călătoresc în alte ţări, inclusiv pe teritoriul UE. Atât timp cât serviciile prestate de societate nu se adresează în mod specific persoanelor fizice din UE, societatea nu face obiectul normelor GDPR.

Nu este relevantă dimensiunea companiei – GDPR-ul se aplică şi societăţilor mari şi societăţilor mici sau mijlocii (IMM) care prelucrează date conform descrierii de mai sus. Activităţile care prezintă riscuri ridicate pentru drepturile şi libertăţile persoanelor fizice, indiferent dacă sunt desfăşurate de către un IMM sau de către o corporaţie, atrag aplicarea unor norme suplimentare, mai dure. Cu toate acestea, unele obligaţii prevăzute de GDPR nu li se aplică tuturor IMM-urilor.

De exemplu, societăţile cu mai puţin de 250 de angajaţi nu au obligaţia să păstreze evidenţe ale activităţilor lor de prelucrare decât dacă prelucrarea datelor cu caracter personal este o activitate regulată, reprezintă o ameninţare la adresa drepturilor şi a libertăţilor persoanelor fizice sau se referă la date sensibile ori la cazier judiciare.

Tot astfel, IMM-urile au obligaţia de a numi un responsabil cu protecţia datelor numai dacă prelucrarea reprezintă activitatea lor principală şi dacă aceasta implică anumite ameninţări la adresa drepturilor şi a libertăţilor persoanelor fizice (cum ar fi monitorizarea persoanelor fizice sau prelucrarea unor date sensibile ori a unor cazier judiciare), în special pentru că se desfăşoară la scară largă.

Pentru a fi la curent cu prevederile legale în materie de protecţie a datelor cu caracter personal, recomandăm operatorilor de date

consultarea permanentă a paginii web a Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal pe următoarea adresă: http://www.dataprotection.ro/. La secţiunea de legislaţie se pot observa trei subcapitole şi anume Legislaţie internă, Legislaţie UE şi Decizii A.N.S.P.D.C.P.

Norme GDPR obligatorii pentru toate societăţile

GDPR a stabilit o serie de principii pe care toţi operatorii de date cu caracter personal ar trebui să le urmeze, textul de lege fiind scris la nivel de recomandare, urmând ca DPO-ul să ajute la interpretarea adecvată a fiecărui principiu în scopul de a se asigura de respectarea acestora în acord cu obiectul de activitate al operatorului.

Aceste principii ghidează raţionamentul DPO-ului în găsirea de soluţii operaţionale care să ajute la buna desfăşurare a prelucrării, cu respectarea drepturilor persoanelor vizate. Cu alte cuvinte, principiile sunt liniile generale de avut în vedere la începutul oricărui tip de prelucrare.

Tipul şi cantitatea de date cu caracter personal pe care societatea are dreptul să le prelucreze depind de motivul pentru care sunt prelucrate (temeiul juridic în cauză) şi de scopul în care sunt prelucrate. Societatea/organizaţia trebuie să respecte mai multe norme-cheie, inclusiv următoarele:

- datele cu caracter personal trebuie prelucrate într-un mod legal şi transparent, garantând echitatea în ceea ce priveşte persoanele fizice ale căror date cu caracter personal sunt prelucrate („legalitate, echitate şi transparenţă”);
- trebuie să existe scopuri specifice ale prelucrării datelor şi societatea trebuie să informeze persoanele fizice în legătură cu scopurile respective atunci când le colectează date cu caracter personal. Societatea nu poate colecta pur şi simplu date cu caracter personal în scopuri nedefinite;
- societatea trebuie să colecteze şi să prelucreze numai acele date cu caracter personal care sunt necesare pentru îndeplinirea scopului respectiv („reducerea la minimum a datelor”);
- societatea trebuie să se asigure că datele cu caracter personal sunt exacte şi actualizate, având în vedere scopurile pentru care sunt prelucrate, şi să fie corectate în caz contrar („exactitate”);
- societatea nu are dreptul să utilizeze datele cu caracter personal în alte scopuri care nu sunt compatibile cu scopul iniţial;
- societatea trebuie să se asigure că datele cu caracter personal nu sunt stocate mai mult timp decât este necesar pentru scopurile în care au fost colectate („limitări legate de stocare”);

- societatea trebuie să prevadă garanţii tehnice şi organizaţionale adecvate care să asigure securitatea datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnologice adecvate („integritate şi confidenţialitate”).

Exemplul 1: Un magazin online trebuie să le explice clienţilor săi într-un limbaj clar şi simplu politica sa de confidenţialitate, de ce are nevoie de datele colectate, cum le va utiliza şi cât timp intenţionează să le păstreze.

Exemplul 2: O societate care organizează un târg în cadrul căruia vizitatorii se înregistrează trebuie să comunice exact către cine şi care dintre date vor ajunge la societăţile care sunt expozante în cadrul respectivului târg.

Ce înseamnă „prelucrare a datelor”?

Prelucrarea datelor înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

„Restricţionarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora fie în vederea criptării sau anonimizării, fie atunci când o persoană ale cărei date au fost prelucrate a solicitat acest lucru, fie în vederea ştergerii acestora atunci când se împlineşte termenul pe care societatea s-a angajat să îl respecte pentru păstrarea datelor.

Scopul prelucrării datelor. Pot fi prelucrate datele în orice scop?

Nu, scopul în care sunt prelucrate datele cu caracter personal trebuie cunoscut, iar persoanele fizice ale căror date sunt prelucrate trebuie informate. Nu se poate menţiona pur şi simplu că se vor colecta şi prelucra date cu caracter personal. Acesta este principiul „limitărilor legate de scop”. Astfel, atât în mediul online (în cadrul politicii de confidenţialitate cât şi în