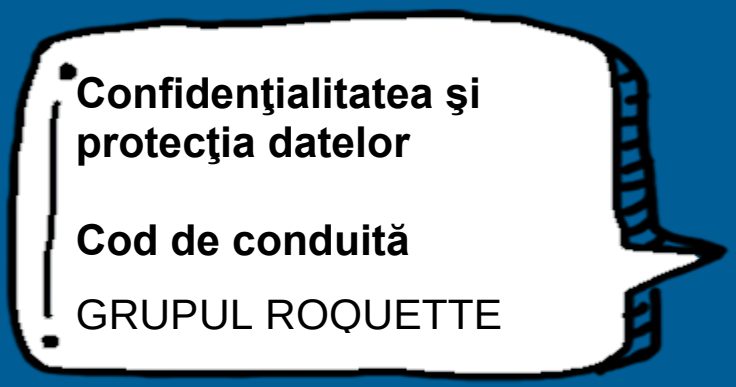
PUBLIC

ROQUETTE
*Offering the best of nature™*

Privacy & Data Protection

# CUM NE ANGAJĂM ZILNIC PENTRU CONFIDENȚIALITATE ȘI PROTECȚIA DATELOR



# Legal și conformitate

## Principalele provocări de conformitate la Roquette

Sub conducerea conducerii generale, domeniul de aplicare a conformității și managementul acesteia la Roquette reprezintă o parte cheie a departamentului „Legal & conformitate” al Grupului și este cunoscut sub denumirea de Biroul de conformitate.

Biroul de conformitate deține Codul de conduită Roquette, actualizarea și implementarea acestuia.

De asemenea, acoperă următoarele trei domenii principale:

- Securitate financiară,
- Etică profesională și
- Confidenţialitatea şi protecţia datelor

Prin urmare, a fost creat se dezvoltă un Program de conformitate pentru a ne asigura că activitatea noastră este ireproșabilă din punct de vedere juridic și financiar.

## Care este scopul conformității?

Scopul conformității este de a insufla **valori etice** și de a implementa măsuri în conformitate cu **cerințele legale**, **standardele** și **bunele practici.**

Programul nostru facilitează implementarea procedurilor care asigură respectarea regulilor aplicabile la Roquette.

Cele patru valori ale noastre – **autenticitatea, excelenţa, orientarea spre viitor, bunăstarea** – constituie o bază solidă pentru acțiunile noastre de **zi cu zi**.

### Strategia noastră de protecţie a datelor este centrată pe oameni și afaceri

Principiile privind confidențialitatea și protecția datelor fac parte din standardele stabilite în Codul nostru de conduită.

Etica este văzută din ce în ce mai mult ca fiind o valoare cheie a Grupului - iar etica datelor este o parte cheie a acesteia.

# Editat

Principiile confidențialității și protecției datelor fac parte din standardele stabilite în Codul nostru de conduită.

Toți angajații, precum și terții cu care Roquette are relații, au dreptul la confidențialitate. Din acest motiv, Roquette se angajează să le protejeze datele cu caracter personal.

Datele cu caracter personal sunt informații care permit identificarea directă sau indirectă a unei persoane fizice (nume, data nașterii, număr de asigurare socială, fotografie, adresă de e-mail, ID-uri de computer etc.).

*Protecția datelor cu caracter personal este un drept fundamental, care asigură respectarea vieții private*

Protecția datelor cu caracter personal garantează fiecărei persoane dreptul de a controla colectarea, procesarea, utilizarea și distribuirea acestor date.

Datele cu caracter personal trebuie utilizate într-o manieră echitabilă pentru un scop specific, explicit şi legitim şi păstrate doar pentru perioada necesară pentru a efectua procesarea.

În Europa procesarea datelor cu caracter personal a fost definită de Regulamentul general privind protecția datelor (GDPR), care a intrat în vigoare la 25 mai 2018.

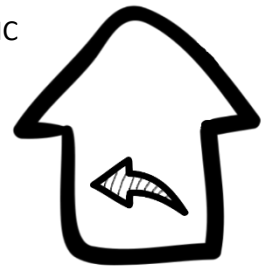
Deoarece legislaţia privind confidenţialitatea şi datele cu caracter personal variază de la o ţară la alta şi deoarece Roquette are prezenţă la nivel internaţional, Grupul a adoptat o Politică de grup privind protecţia datelor cu caracter personal. Această politică se aplică tuturor angajaților Grupului, la nivel mondial.

Acest Ghid explică buna conduită pe care trebuie să o adoptăm în activitățile noastre zilnice pentru a respecta principiile de protecție a datelor cu caracter personal și cerințele politicii noastre.

**Jennifer GODIN**, responsabilă cu protecția datelor

Déléguée à la protection des données

PUBLIC



# Cuprins


Legal și conformitate 3
Redactat de responsabilul cu protecția datelor 4

Scop 6
Descriere 7
Responsabilități 8
Formularea de întrebări sau de preocupări 9
Conformitatea cu legile şi reglementările 10
Principii de protecție a datelor 12
Risc pentru viața privată 14
Riscuri în caz de neconformare 16

**Standardele noastre în relaţiile cu subiecții de date** > **pag. 19**

- Cultura confidențialității 20
- Procesarea datelor cu caracter personal 22
- Drepturile subiecților de date 24
- Politica de confidențialitate 26
- Minimizarea datelor 28
- Securitatea datelor 30
- Clasificarea datelor cu caracter personal 32
- Păstrarea datelor 34

**Standardele noastre în relațiile noastre cu Afiliații și Subcontractanții** > pag. 37

- Calificarea procesorului și a controlorului 38
- Clauze ale protecției datelor 40
- Acordul privind transferul datelor 42

**Standardele noastre în relațiile noastre cu Autoritățile de Rețea și de Supraveghere** > pag. 45

- Responsabilul cu protecția datelor 46
- Rețeaua de protecție a datelor și părțile interesate 48
- Autoritățile de supraveghere 50
- Guvernanța 52
- Răspunderea 54
- Documentație 56
- Evaluarea impactului asupra vieții private 58
- Confidențialitate prin proiectare și implicită 60
- Notificarea privind încălcarea datelor 62
- Revizuire și monitorizare 64

Documente de referinţă 66
Bibliografie 67
Surse 68

# Scop

## Ce este Politica de confidenţialitate şi protecţie a datelor?

Grupul Roquette a stabilit o Politică de confidențialitate și protecție a datelor („Politica") pentru a aborda în mod optim problemele de confidențialitate și protecție a datelor în conformitate cu imaginea sa, cu interesele sale și cu legile și reglementările aplicabile privind protecția datelor.

Această politică definește principiile și cerințele pentru protecția datelor cu caracter personal și indică regulile de confidențialitate și protecție a datelor care trebuie respectate de toți angajații, managerii, directorii și terții care acționează pentru Roquette.

Principiile și regulile acestei Politici de protecție a datelor cu caracter personal sunt detaliate într-o platformă documentară cu trei niveluri:

- Angajamentul conducerii Cod de conduită
- Reguli interne: Manualul și directivele privind protecția datelor cu caracter personal.
- Documentația sistemului de management al protecției datelor (DPMS): Proceduri, linii directoare, metodologii, instruire etc.

Toată documentația corespunde cerințelor legale și normative privind protecția datelor.

## Ce este Ghidul de conduită privind confidenţialitatea şi protecţia datelor?

Ghidul privind confidențialitatea și protecția datelor („Ghidul") ne poate ajuta să implementăm și să respectăm politica noastră privind confidențialitatea și protecția datelor.

Acesta prezintă - într-un mod simplificat - regulile și cele mai bune practici care sunt conforme cu directivele Grupului nostru și cerințele legilor și reglementărilor aplicabile pentru noi în ceea ce privește protecția datelor.

Este împărțit pe teme inspirate din Codul de conduită, dintre care „Confidențialitatea și protecția datelor” este unul dintre subiectele de conformitate.

# Descriere

## Pentru cine se aplică Ghidul de conduită privind confidenţialitatea şi protecţia datelor?

Politica și codul de conduită reprezintă un punct comun pentru toate entităţile din întreaga lume. Acestea includ:

- Toţi angajaţii, directorii şi managerii („Angajaţii”)
- Orice terţi care acţionează în numele Roquette, inclusiv:
  - Contractanţi, inclusiv consultanţi, liber-profesionişti şi personal temporar
  - Stagiari
  - Personalul detaşat de la o entitate care nu face parte din Roquette
  - Lucrătorii ocazionali
  - Alţi reprezentanţi
  - Și orice terță parte angajată sau plătită de Roquette.

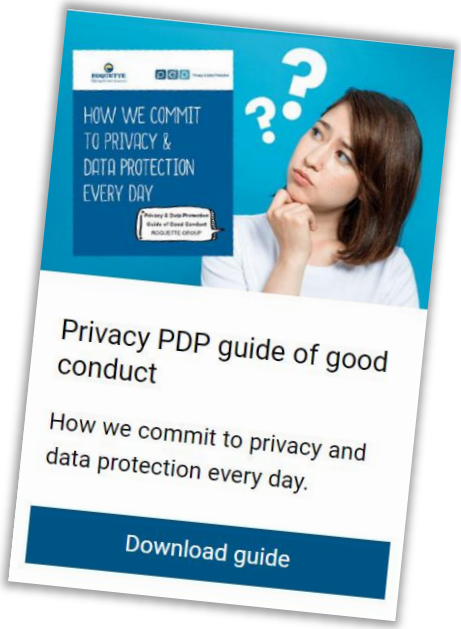
## Unde putem găsi Ghidul de conduită privind confidenţialitatea şi protecţia datelor?

Toți angajații și terții care acționează pentru Roquette trebuie să înțeleagă și să respecte principiile de confidențialitate și protecție a datelor conținute în documentația noastră și în special în prezentul Ghid.

Ghidul este la îndemână la:

https://www.roquette.com/data-protection.

Acest Ghid este transmis ca parte a unei comunicări dedicate, însoțită de un set de instrumente cu cursuri de e-learning privind principiile de confidențialitate și protecție a datelor (definite de standardele internaționale și cerințele specifice ale RGPD).



# Responsibilități

## Cui îi revine responsabilitatea pentru implementarea Principiilor operaţionale?

*Confidențialitatea datelor se adresează - și este responsabilitatea - tuturor celor din organizația noastră.*

Cu toții avem responsabilitatea de a respecta Principiile operaționale descrise în documentația DPMS furnizată de Echipa Biroului de conformitate și Rețeaua de protecție a datelor. Acest ghid susține această implementare și crește nivelul nostru de conformitate.

## Cum ne putem asigura că luăm decizia corectă?

Ghidul este conceput astfel încât să ne ajute să facem faţă celor mai multe situaţii din viaţa noastră profesională care ar putea ridica probleme de etică. Acesta nu poate totuşi să prevadă toate situaţiile cu care ne putem confrunta în exercitarea activităţilor noastre profesionale.

Dacă avem îndoieli, în orice moment, cu privire la atitudinea pe care trebuie să o adoptăm, trebuie să ne folosim discernământul şi să ne adresăm următoarele întrebări:

- Această situaţie este în conformitate cu legea?
- Se reflectă această situaţie bine asupra mea şi asupra companiei?
- I-aş spune unui prieten, rudelor sau unui coleg despre această situaţie?
- M-aş simţi confortabil dacă această situaţie ar fi făcută publică?

Dacă răspunsul la oricare dintre aceste întrebări este negativ, nu trebuie să continuăm. Dacă avem îndoieli, trebuie să vorbim cu persoana de contact relevantă (vezi datele de contact din secţiunea „Formularea de întrebări sau preocupări”).

## Ce se întâmplă dacă nu respectăm Principiile privind confidenţialitatea şi protecţia datelor?

Nerespectarea Principiilor poate avea un efect negativ asupra companiei noastre. Consecințele pot fi foarte grave, fi foarte grave, atât pentru companie, cât şi pentru persoanele implicate (sancţiuni disciplinare, amendă, închisoare, afectarea reputaţiei etc.).

Toate rapoartele privind încălcări reale sau suspecte ale Principiilor vor fi luate în serios. Vom investiga cu promptitudine, în mod echitabil şi în conformitate cu cerinţele legale.

În funcţie de natura încălcării, pot fi impuse măsuri disciplinare, în conformitate cu legile locale şi regulamentele companiei.

Tuturor angajaţilor li se cere să coopereze pe deplin cu orice investigaţie. Roquette va proteja confidenţialitatea oricărei persoane implicate.

# Întrebări adresate sau preocupări

Angajaţii, terţii care acţionează în numele Roquette şi alte părţi interesate sunt încurajaţi să adreseze întrebări sau să semnaleze preocupări care vor ajuta Roquette să prevină şi să reducă orice daune asupra companiei.

## Ce tip de probleme pot fi semnalate?

Poate fi adresată orice întrebare şi poate fi semnalată orice încălcare potenţială sau reală a Principiilor de confidențialitate și protecție a datelor, a regulamentelor companiei sau a legilor aplicabile.

## Pe cine trebuie să contactăm?

În cazul unei încălcări a securității datelor, vă rugăm să contactați responsabilul cu protecția datelor la dpo@Roquette.com și/sau să raportați un incident prin intermediul formularului nostru web de alertă de confidențialitate.

**Dacă trebuie să raportați o potențială încălcare a conformității**, puteți lua legătura cu punctul dvs. de contact obișnuit sau puteți raporta o problemă prin intermediul instrumentului Speakup©. Toate alertele primite prin intermediul acestui instrument sunt tratate confidențial, respectând legile și reglementările relevante.

SpeakUp®

Roquette nu va tolera nicio formă de reprimare sau represalii împotriva unui angajat sau a unei terţe părţi care raportează, cu bună-credinţă, o încălcare potenţială sau reală a pricipiilor de confidențialitate și protecție a datelor, ori a legilor aplicabile.

Prin urmare, în cazul în care autorul unei alerte trebuie să se identifice, identitatea sa trebuie să fie tratată în mod confidențial de către organizație, pentru a evita riscul de represalii, discriminare sau măsuri disciplinare împotriva sa ca urmare de denunțării.

# Conformitatea cu legile şi reglementările

Fiecare dintre noi, în fiecare entitate a Grupului, trebuie să respectăm legile și reglementările în vigoare privind protecția datelor.

În cazurile în care reglementările locale sunt mai stricte decât Politica noastră și Codul nostru de conduită, vor prevala primele.

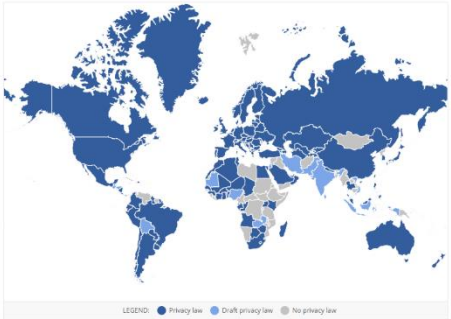
În caz contrar (absența legislației locale sau legislația mai puțin restrictivă), bunele noastre practici interne vor prevala în măsura permisă de lege.

## Considerăm că:

- Trebuie să implementăm cât mai repede posibil toate noile reglementări locale şi aplicabile.
- Fiecare dintre noi trebuie să fie conştient de faptul că orice încălcare a legilor şi a reglementărilor poate fi pasibilă de sancţiuni civile şi/sau penale, atât pentru persoana implicată, cât şi pentru companie.
- Protecția persoanelor fizice în ceea ce privește procesarea datelor cu caracter personal reprezintă un drept fundamental.
- Principiile și regulile privind protecția persoanelor fizice în ceea ce privește procesarea datelor lor cu caracter personal ar trebui, indiferent de naționalitatea sau reședința acestora, să respecte drepturile și libertățile fundamentale, în special dreptul la protecția datelor cu caracter personal.
- Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția sa în societate și trebuie echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității.

*Care țară a adoptat o legislație specifică privind protecția datelor sau are o autoritate de protecție a datelor?*

Pentru o prezentare generală, consultați această hartă: https://www.cnil.fr/en/data-protection-around-the-world.



## Responsabilităţile noastre:

- În toate împrejurările, trebuie să respectăm toate legile şi reglementările aplicabile în ţările în care ne desfăşurăm activitatea şi toate normele în vigoare în fiecare dintre locaţiile companiei.

- Ca parte a activităților noastre profesionale, trebuie să raportăm orice comportament pe care îl considerăm contrar legilor și reglementărilor aplicabile privind protecția datelor (de exemplu: GDPR) la responsabilul nostru cu protecția datelor la dpo@Roquette.com și instrumentul confidențial de alertă Roquette: Speakup©.

- Trebuie să implementăm măsuri de protecție a datelor cu caracter personal care sunt adecvate și proporționale cu contextul, facilitând în același timp respectarea altor legi și reglementări. Pe de altă parte, acțiunile noastre de ne conforma cu legile și reglementările aplicabile Grupului trebuie să respecte regulile și bunele practici pentru protecția datelor cu caracter personal (de exemplu: în programul de conformitate antimită și anticorupție trebuie să asigurăm protecția informatorului prin măsuri de confidențialitate și protecție a datelor sale cu caracter personal).

### Sunteți subiect al Regulamentului general privind protecția datelor (GDPR)?

Ca **procesator** (1) sau **controlor** (2) intrați în domeniul de aplicare al RGPD:

- dacă sunteți stabilit în UE sau;
- atunci când nu sunteți stabilit în UE, dacă: "activitățile dumneavoastră de procesare sunt legate de
  - oferirea de bunuri sau servicii subiecților de date din UE;
  - sau monitorizarea comportamentului acestora în măsura în care comportamentul lor are loc în cadrul UE".

**Text oficial:** Articolul 3 din RGPD privind domeniul de aplicare teritorial

(1) și (2): Vezi definițiile de la pagina 38.

# Principii ale protecției datelor

## Datele cu caracter personal trebuie să fie:

- securizate.
- exacte și actualizate.
- procesate în mod corect și legal.
- procesate în scopuri limitate.
- adecvate, relevante și nu excesive.
- păstrate pentru o perioadă limitată și determinată de timp.
- procesate în conformitate cu drepturile subiectului de date.
- protejate prin măsuri legale adecvate dacă sunt transferate în alte țări.

## Drepturile dvs.:

În conformitate cu legile și reglementările aplicabile aveți dreptul de a accesa, de a rectifica și de a vă opune procesării datelor dvs. din motive legitime, precum și dreptul de ștergere din motive legitime, dreptul la portabilitatea datelor și dreptul de a limita procesare datelor dvs.

Pentru a vă exercita aceste drepturi completați formularul disponibil la: Roquette.com/Protecția datelor.

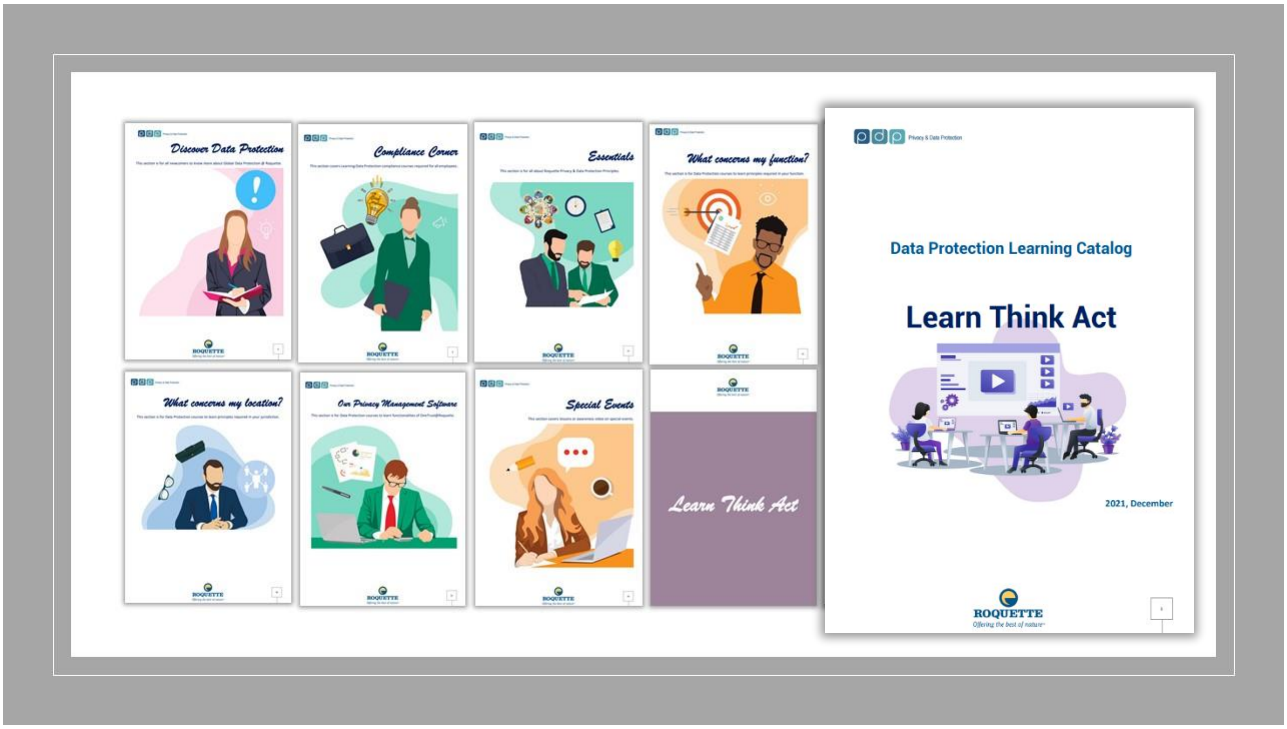
Pentru întrebări contactați **responsabilul cu protecția datelor** (dpo@Roquette.com).

## Responsabilitățile noastre:

Noi trebuie să:

- Respectăm legislația locală și regulile Politicii Grupului privind protecția datelor cu caracter personal.
- Informăm responsabilul cu protecția datelor cu privire la orice procesare nouă sau modificări.
- Nu colectăm, utilizăm, divulgăm sau stocăm date cu caracter personal decât în scopuri specifice, legitime și necesare.
- Ne asigurăm că persoanele au fost informate că datele lor sunt colectate.
- Protejăm aceste date în timpul colectării, procesării, utilizării, comunicării, stocării sau transferului.
- Asigurăm securitatea și confidențialitatea datelor procesate.
- Păstrăm datele numai pentru perioada necesară procesării și să respectăm legile aplicabile.
- Contactăm responsabilul cu protecția datelor în cazul unui incident de securitate care implică date cu caracter personal.

## Ne instruim angajații și ne îmbunătățim procesele interne.



# Riscul de confidențialitate

## Ce este un risc de confidențialitate?

Un risc este un scenariu ipotetic care descrie un eveniment temut și toate amenințările care ar permite producerea acestuia. Mai exact, descrie:

- cum sursele de risc (de ex.: un angajat mituit de un concurent)
- ar putea exploata vulnerabilitățile activelor de susținere(de ex.: sistemul de gestionare a fișierelor care permite manipularea datelor)
- într-un context de amenințări (de ex.: utilizare abuzivă prin trimiterea de e-mailuri)
- și să permită apariția evenimentelor temute (de ex.: acces neautorizat la datele cu caracter personal)
- cu privire la datele cu caracter personal (de ex: fișier al clientului)
- generând astfel un impact asupra confidențialității subiecților de date (de ex.: solicitări nedorite, sentimente de invazie a confidențialității, probleme personale sau profesionale).

---

*Efectul incertitudinii asupra confidențialității*

---

Severitatea reprezintă magnitudinea unui risc. Este estimată în primul rând în ceea ce privește amploarea potențialelor impacturi **(fizice, materiale**, **morale**) asupra subiecților de date, luând în considerare controalele existente, planificate sau suplimentare.

## Exemplu:

Cel mai important risc prezentat de sistemul de alertă profesională pentru informator: riscul de represalii, discriminare sau măsuri disciplinare luate împotriva acestuia pentru că a raportat faptele.

## Considerăm că:

Drepturile persoanelor fizice se aplică în întregime, indiferent de nivelul de risc al procesării.

Vom fi însă obligați să ne adaptăm conformitatea cu protecția datelor în funcție de nivelul de risc pe care operațiunile noastre de procesare a datelor cu caracter personal îl prezintă pentru drepturile și libertățile fundamentale ale persoanelor.

GDPR oferă un impuls suplimentar acestei practici. În consecință, operațiunile de procesare care implică riscuri mai mici pentru drepturile și libertățile fundamentale ale persoanelor fizice pot duce, în general, la mai puține obligații de conformitate, în timp ce operațiunile de procesare „cu risc ridicat" vor impune obligații de conformitate suplimentare, cum sunt evaluările impactului asupra protecției datelor (DPIA) (1)

## Responsabilitățile noastre:

Evaluarea riscurilor este fundamentală. În conformitate cu RGPD, evaluarea riscurilor stă la baza responsabilității organizaționale și a oricăror procesări de date.

Trebuie să efectuăm evaluări ale riscurilor ca parte a DPIA pentru procesarea cu risc ridicat, precum și în legătură cu multe alte cerințe GDPR, inclusiv securitatea datelor, notificările privind încălcarea securității și a confidențialității datelor, confidențialitatea prin proiectare, interesul legitim, limitarea scopului și procesarea echitabilă.

(1): Vezi definiția de la pagina 58.

# Riscuriîn caz de neconformitate

Persoanele juridice și fizice care nu respectă legile și reglementările privind protecția datelor (de ex. GDPR) riscă sancțiuni și costuri, sub formă de:

**Sancțiuni penale:**

- Închisoare.
- Amendă pentru persoanele juridice.

**Sancțiuni civile:**

- Daune civile.

**Sancțiuni administrative:**

- Notificare formală.
- Avertisment.
- Obligare.
- Limitarea temporară sau definitivă a procesării.
- Retragerea unei certificări sau obligarea la retragerea unei certificări.
- Suspendarea transferurilor de date.
- Obligarea de a înceta procesarea sau retragerea autorizării.
- Publicarea sancțiunilor impuse.
- Sancțiuni fără notificare formală prealabilă (criteriu de urgență).
- În funcție de încălcare, o amendă administrativă.

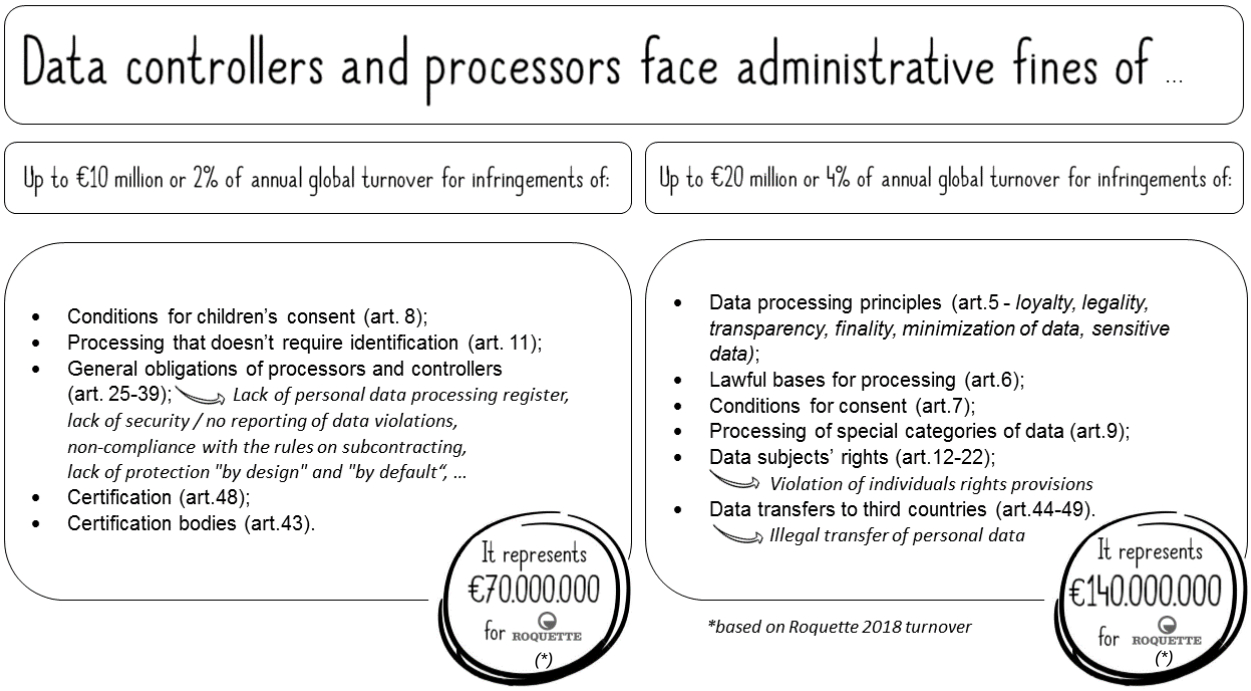
**Costuri semnificative:**

- Pierdere a veniturilor ca urmare a daunelor aduse reputației acestora.

## Care este amenda administrativă maximă în conformitate cu RGPD?

Amenzile sunt discreționare și nu obligatorii. Acestea trebuie impuse de la caz la caz și trebuie să fie „eficiente, proporționale și disuasive”.

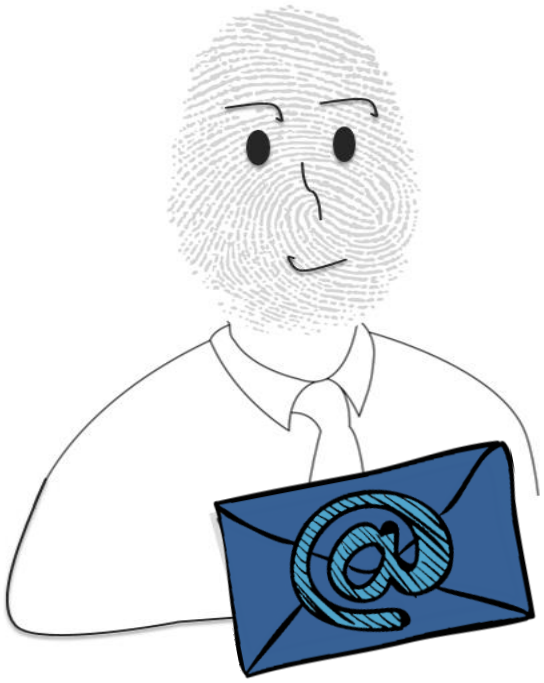
Amenzile se bazează pe articolele specifice ale Regulamentului pe care organizația le-a încălcat.




## Care pot fi sancțiunile penale?

Câteva exemple din legislația franceză:

- Actul de colectare a datelor cu caracter personal prin mijloace frauduloase, inechitabile sau ilegale va fi pedepsit cu cinci ani de închisoare și o amendă de 300 000 € (Art. 226-18 Cod penal).
- Pentru a garanta un drept real și protecția informatorului, legea anticorupție (Sapin II) pedepsește sever orice obstacol în calea unei alerte. Confidențialitatea care înconjoară alerta este un element esențial al reglementării. Astfel, divulgarea elementelor confidențiale ale alertei (identitatea informatorului, a reclamatului, informațiile furnizate în sprijinul alertei), cu excepție în ceea ce privește autoritatea judiciară, este pedepsită cu doi ani de închisoare și o amendă de 30 000 €.



# 1 Standardele noastre în RELAŢIILE CU SUBIECȚII DE DATE

# Cultură de confidențialitate

**Protecția datelor** este un set de legi, reglementări și cele mai bune practici care guvernează colectarea și utilizarea datelor cu caracter personal ale persoanelor fizice.

**Datele cu caracter personal** înseamnă toate informaţiile referitoare la o persoană fizică identificată sau identificabilă.

**Protecția datelor se** referă la gestionarea datelor cu caracter personal.

## Cine este afectat?

Confidențialitatea datelor este relevantă pentru - și responsabilitatea - tuturor celor din organizația noastră.

## De ce este important acest lucru?

Datele gestionate incorect pot avea consecințe grave pentru organizații, angajații și clienții lor.

Încălcarea confidențialității poate duce la sancțiuni financiare nelimitate, presă defăimătoare, deteriorarea reputației, pierderea încrederii clienților, pierderea afacerii și a angajaților, reclamații și posibil, reclamații în cazul încălcării confidențialității datelor lor proprii cu caracter personal, perspectiva unor acțiuni disciplinare în alte cazuri. Este în interesul nostru să tratăm datele în mod corespunzător.

## Considerăm că:

- Toți angajații de la Roquette trebuie să fie conștienți de rolurile și responsabilitățile lor în ceea ce privește protecția datelor cu caracter personal. Sensibilizarea are ca scop consolidarea culturii respectului pentru confidențialitate și protecția datelor cu caracter personal în cadrul Roquette.

[DIDPGR001RO – Regula 1]

- Trebuie asigurată instruirea angajaților cu privire la implementarea politicii de protecție a datelor cu caracter personal.

[DIDPGR001RO – Regula 2]

# GÂNDIȚI CONFIDENȚIALITATEA

## Suntem responsabili!

Avem nevoie de datele cu caracter personal ale clienților și angajaților pentru a ne desfășura cu succes activitatea.

Ni se acordă încredere pentru a gestiona aceste informații esențiale.

Fiecare angajat are responsabilitatea de a respecta legile corespunzătoare privind protecția datelor.

## Este reputația noastră!

Reputația este greu de câștigat și ușor de pierdut.

Tratarea cu grijă și respect a datelor clienților și angajaților noștri este esențială pentru protejarea reputației noastre.

DVS. sunteți cea mai bună apărare împotriva daunelor de reputație.

## Este vorba despre respect!

Deciziile pe care clienții și angajații noștri le iau cu privire la modul în care sunt utilizate datele lor cu caracter personal trebuie respectate dacă dorim să menținem încrederea pe care ne-o acordă.

## Alegerea vă aparține!

Cu toții suntem responsabili să ne asigurăm că datele cu caracter personal ale clienților și angajaților sunt păstrate în siguranță și sunt confidențiale.

Trebuie acordată o atenție deosebită oricăror informații care trebuie trimise sau preluate în afara locației.

## Ne instruim angajații și ne îmbunătățim procesele interne.

- Codul de conduită - Confidențialitate și protecția datelor - p. 42 - 43.
- Pentru nou veniți: Mai multe informații și e-learning despre protecția datelor sunt furnizate în timpul onboardingului global.
- Pentru angajaţi: Cursurile sunt încărcate pe platforma Learning.
- Pentru coordonatorii protecției datelor: Documentația este partajată pe comunitatea noastră „Rețeaua de protecție a datelor”.
- Pentru toți: Mai multe informații sunt disponibile pe portalul intern > Protecția datelor.

# Procesarea datelor cu caracter personal

**Procesarea datelor cu caracter personal** înseamnă orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, prin mijloace automate sau nu, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, recuperarea, consultarea, utilizarea, divulgarea prin transmitere, diseminare sau punerea la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

O cerință privind protecția datelor (și RGPD) pe care va trebui să o cunoașteți este că trebuie să aveți o „bază legală" pentru colectarea oricăror date cu caracter personal.

În funcție de legislația locală, pot exista diferite baze legale.

## Care este „baza mea legală" pentru procesarea datelor cu caracter personal?

Trebuie să puteți răspunde clar la întrebarea:

*„Cum mi-ați obținut [datele] și de ce aveți voie să le dețineți?"*

Mai exact, aceasta înseamnă că trebuie să respectați cel puțin una dintre cele șase baze legale pentru procesarea datelor. În conformitate cu RGPD, nu puteți procesa date decât dacă:

1. Consimțământ
2. Contract
3. Obligație legală
4. Interese vitale
5. Sarcina publică
6. Interes legitim

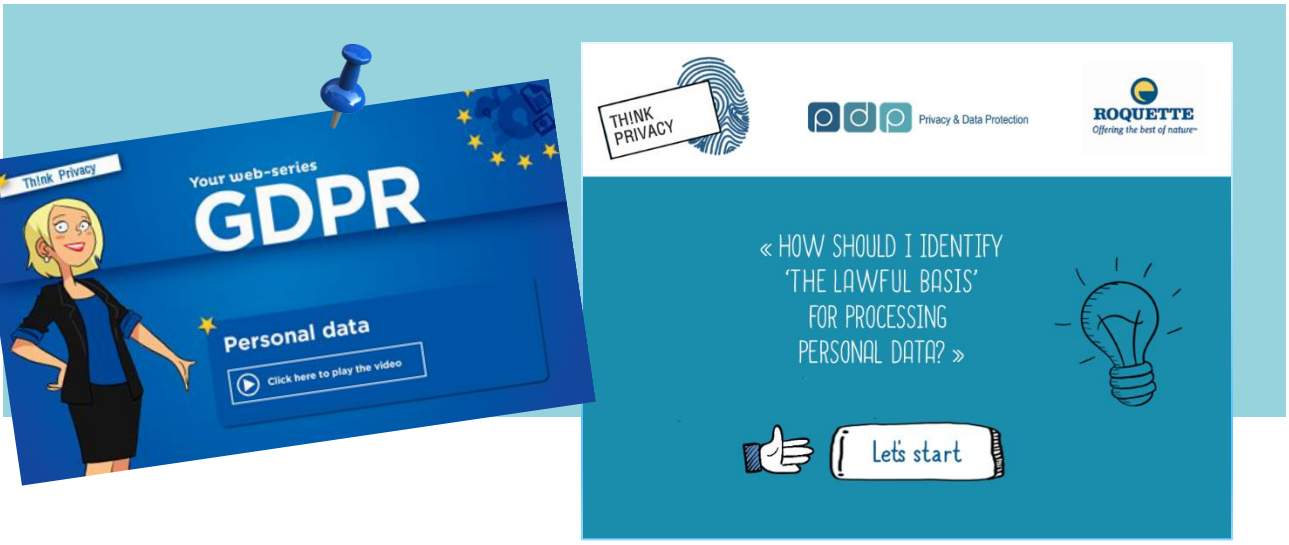
# Legalitate, echitabilitate și transparență

## Responsabilitățile noastre:

Trebuie să aplicăm reguli pentru a asigura procesarea legală a datelor cu caracter personal.

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Acționați cu legalitate, echitate și transparență la colectarea datelor | DIDPGR002RO Regula 1 | Art. 5 1. a) |
| • Demonstrați că este respectat consimțământul subiecților de date (dacă este necesar) | DIDPGR002RO Regula 2 | Art. 7 |
| • Respectați scopurile stabilite în timpul colectării datelor | DIDPGR002RO Regula 3 | Art. 5 1. b) |
| • Limitați informațiile colectate pe hârtie sau în format digital la ceea ce este strict necesar | DIDPGR002RO Regula 4 | Art. 5 1. c) |
| • Limitați păstrarea datelor la ceea ce este strict necesar | DIDPGR002RO Regula 5 | Art. 5 1. e) |
| • Luați măsuri pentru transferul datelor cu caracter personal către țări terțe sau organizații internaționale | DIDPGR002RO Regula 6 | Art. 44 până la 50 |

## Ne instruim angajații și ne îmbunătățim procesele interne.



# Drepturile subiecților de date

Un **subiect de date** este o persoană fizică care poate fi identificată, în mod direct sau indirect, în special prin referire la un identificator precum un nume, un număr de identificare, date de localizare, un identificator online sau unul ori mai mulţi factori specifici identităţii fizice, fiziologice, genetice, mentale, economice, culturale sau sociale a persoanei fizice respective.

## Ce este un „subiect de date”?

Acesta este termenul tehnic pentru persoana despre care se referă anumite date cu caracter personal.

## Ce este o solicitare de acces a subiectului?

Unul dintre principalele drepturi pe care legile privind protecția datelor în vigoare le acordă persoanelor fizice este dreptul de acces la datele lor cu caracter personal.

O persoană vă poate trimite o „solicitare de acces a subiectului”, prin care vă solicită să îi comunicați informațiile cu caracter personal pe care le dețineți despre aceasta și să îi furnizați o copie a acestor informații. În majoritatea cazurilor trebuie să răspundeți la o solicitare de acces validă a subiectului în termen de 30 (*) zile calendaristice de la primirea acesteia.

(*): Această perioadă poate varia în funcție de legislația aplicabilă sau de natura procesării datelor.

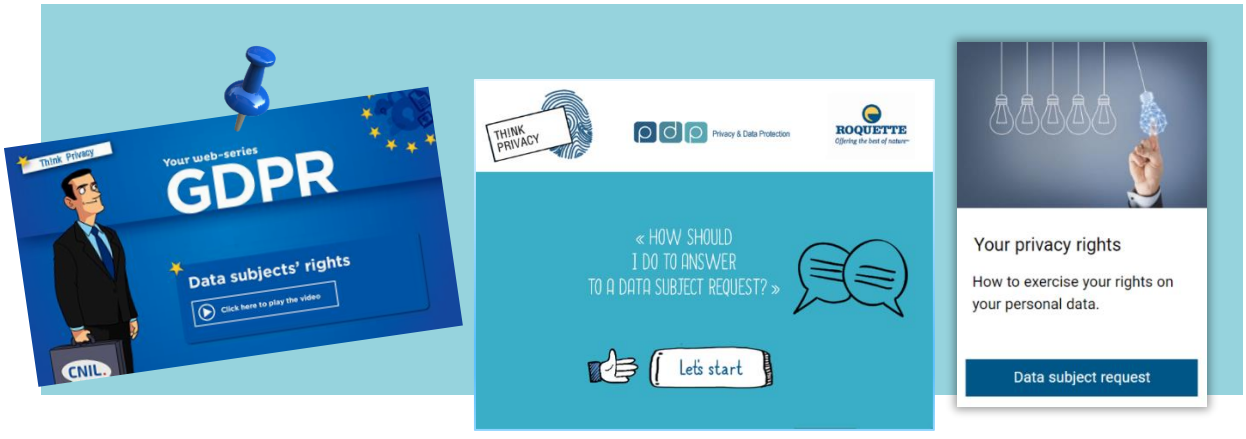
# Care sunt celelalte „drepturi” ale subiecților de date?

## Responsabilitățile noastre:

Trebuie să aplicăm reguli pentru a asigura drepturile subiecților de date.

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Asigurați-vă că notificările legale respectă obligațiile | DIDPGR006RO Regula 1 | Art. 12 |
| • Permiteți subiecților de date să își exercite drepturile de acces | DIDPGR006RO Regula 2 | Art. 15 |
| • Permiteți subiecților de date să își exercite dreptul la rectificare | DIDPGR006RO Regula 3 | Art. 16 |
| • Permiteți subiecților de date să își exercite dreptul la portabilitatea datelor | DIDPGR006RO Regula 4 | Art. 20 |
| • Permiteți subiecților de date să își exercite dreptul la ștergere („dreptul de a fi uitați”) | DIDPGR006RO Regula 5 | Art. 17 |
| • Permiteți subiecților de date să își exercite dreptul la restricționarea procesării | DIDPGR006RO Regula 6 | Art. 18 |
| • Notificați rectificarea sau ștergerea datelor cu caracter personal ori restricționarea procesării | DIDPGR006RO Regula 7 | Art. 19 |
| • Controlați luarea automată a deciziilor individuale, inclusiv crearea de profiluri | DIDPGR006RO Regula 8 | Art. 22 |

## Ne instruim angajații și ne îmbunătățim procesele interne.



# Politica de confidențialitate

## Dreptul la informare în cazul utilizării datelor cu caracter personal

Trebuie să vă informăm pe dvs., ca angajați și pe toți terții cu care Roquette are relații, dacă utilizăm datele dvs. cu caracter personal/datele lor cu caracter personal.

Trebuie să furnizăm informații detaliate despre următoarele:

- De ce Roquette utilizează datele dvs./ale acestora.
- Ce tip de date utilizează Roquette.
- Cât timp vor fi păstrate datele.
- Drepturile dvs./ale acestora la informare.
- De unde provin datele.
- Informații dacă Roquette va transfera datele dumneavoastră/ale acestora către terți, inclusiv numele dumneavoastră/ale acestora și motivele transferului.
- Informații dacă va transfera datele într-o altă jurisdicție, inclusiv țara implicată și ce se va face cu datele.
- Dacă Roquette utilizează datele la profilare (un tip de procesare automatizată în care datele cu caracter personal sunt utilizate pentru a analiza sau a prezice lucruri precum performanța dvs. la locul de muncă, situația economică, sănătatea).
- Cum puteți contacta DPO.
- În caz de îngrijorare, dreptul dumneavoastră/al lor de a depune o plângere la autoritatea de supraveghere.

Aceasta se numește **Informații privind confidențialitatea** sau **Politica de confidențialitate**.

Trebuie să vă oferim/le oferim informații privind confidențialitatea în momentul în care Roquette colectează datele dvs./ale acestora. Dacă Roquette obține datele dumneavoastră/ale acestora dintr-o altă sursă, trebuie să furnizeze informații privind confidențialitatea. Acest lucru se poate face sub forma unei declarații de confidențialitate.

Acest lucru se numește **dreptul la informare**.

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Asigurați-vă că notificările legale respectă obligațiile | DIDPGR006RO Regula 1 | Art. 12 |

Exemplu:

- Informații privind confidențialitatea pe site-ul web Roquette, disponibile la: https://www.roquette.com/privacy-notice-website .

## Când poate Roquette să nu vă informeze despre activitățile sale?

În general, trebuie să vă oferim/le oferim informații privind confidențialitatea, dar în unele circumstanțe nu trebuie să facem acest lucru. Aici sunt incluse cazurile în care:

- dumneavoastră/aceștia aveți deja informațiile privind confidențialitatea și nimic nu s-a schimbat,
- furnizarea informațiilor privind confidențialitatea este imposibilă sau ar necesita un „efort disproporționat”, ori
- furnizarea informațiilor privind confidențialitatea ar face imposibilă utilizarea datelor dvs. sau ar deteriora grav motivele utilizării acestora.

*Notă: În cazul în care sunt necesare măsuri provizorii pentru a evita ascunderea sau distrugerea dovezilor, aceste informații pot fi emise după adoptarea măsurilor provizorii.*

## Ne instruim angajații și ne îmbunătățim procesele interne.

# Minimizarea datelor

## Ce este principiul minimizării datelor?

GDPR - Articolul 5(1)(c) specifică:

„1. Datele cu caracter personal trebuie să fie:

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt procesate (minimizarea datelor)"

Formularele pe hârtie sau digitale concepute de funcțiile globale pentru colectarea datelor cu caracter personal trebuie să conțină numai câmpuri de informații strict necesare în scopul procesării, pentru a evita colectarea datelor care nu sunt justificate de procesare.

## Responsabilitățile noastre:

Trebuie să ne asigurăm că datele cu caracter personal pe care

- adecvate - suficiente pentru îndeplinirea corespunzătoare a scopului specificat;
- relevante - au o legătură rațională cu acest scop; și
- limitate la ceea ce este necesar - nu dețineți mai mult decât aveți nevoie în acest scop.

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Limitați informațiile colectate pe hârtie sau în format digital la strictul necesar. | DIDPGR002RO Regula 4 | Art. 5 1. c) |

## Listă de verificare:

- ☑ Colectăm numai datele cu caracter personal de care avem nevoie în scopurile specificate.
- ☑ Deținem suficiente date cu caracter personal pentru a îndeplini în mod corespunzător aceste scopuri.
- ☑ Revizuim periodic datele pe care le deținem și ștergem tot ceea de ce nu avem nevoie.
- ☑ Trebuie să identificăm cantitatea minimă de date cu caracter personal de care avem nevoie pentru a ne îndeplini scopul. Ar trebui să păstrăm atâtea informații, și nu mai multe.

Principiul responsabilității înseamnă că trebuie să puteți demonstra că aveți procese adecvate pentru a vă asigura că sunt colectate și păstrate numai datele cu caracter personal de care aveți nevoie.

De asemenea, rețineți că GDPR stipulează că persoanele au dreptul de a completa orice date incomplete care sunt inadecvate pentru scopul dvs., în baza dreptului la rectificare. De asemenea, au dreptul de a vă solicita să ștergeți datele care nu sunt necesare pentru scopul dvs., în conformitate cu dreptul la ștergere (dreptul de a fi uitat).

## Ne instruim angajații și ne îmbunătățim procesele interne.

# Securitatea datelor

**Securitatea cibernetică** este o activitate transversală a cărei implementare asigură faptul că datele pot fi partajate și utilizate cu un nivel adecvat și garantat de protecție a informațiilor și activelor conexe:

- **Confidențialitate**: asigură păstrarea confidențialității informațiilor și nedivulgarea acestora către persoane sau entități necorespunzătoare,
- **Integritate**: asigură corectitudinea și caracterul complet al informațiilor și metodelor de procesare,
- **Disponibilitate**: asigură accesul utilizatorilor autorizați la informații, aplicații și servicii atunci când este necesar,
- **Trasabilitate**: se referă la capacitatea de a păstra evidențe relevante și atunci când este necesar, dovezi ale acțiunilor efectuate în sistemele noastre. Trasabilitatea acoperă, de asemenea, obiectivele legale, cum ar fi nerepudierea sau responsabilitatea.

**Activele de informații cu caracter personal includ:**

- Documente pe hârtie (texte, hărți, imagini...),
- Informații digitale în mediul de birou,
- Informații digitale în mediul mobil,
- Know-how și abilități profesionale (deținute de persoane fizice sau partajate verbal),
- Articole fizice (cum ar fi probe, tulpini, modele...).

[DSUG006EN] Managementul Directivei privind securitatea cibernetică

**Pseudonimizarea** înseamnă procesarea datelor cu caracter personal într-o manieră în care datele cu caracter personal nu mai pot fi atribuite unui anumit subiect de date fără a fi utilizate informații suplimentare, cu condiția ca aceste informații suplimentare să fie păstrate separat și să fie supuse măsurilor tehnice și organizatorice pentru a se asigura că datele cu caracter personal nu sunt atribuite unei persoane fizice identificate sau identificabile.

**Anonimizarea** este procesul prin care datele cu caracter personal sunt modificate ireversibil, astfel încât un subiect de date să nu mai poată fi identificat, direct sau indirect, fie de **către controlorul de date**(1) singur, fie în colaborare cu orice altă parte.

**Criptarea** este metoda prin care textul simplu sau orice alt tip de date este convertit dintr-o formă lizibilă într-o versiune criptată, care poate fi decriptată de o altă entitate numai dacă are acces la o cheie de decriptare. Criptarea este una dintre cele mai importante metode de asigurare a securității datelor, în special pentru protecția end-to-end a datelor transmise în rețele.

(1): Vezi definiția de la pagina 38.

## Considerăm că:

Pentru a menține securitatea și a preveni procesarea cu încălcarea legilor și reglementărilor privind protecția datelor, Roquette și subcontractanții noștri ar trebui să evalueze riscurile inerente procesării și să implementeze măsuri pentru a atenua aceste riscuri, cum ar fi **criptarea** sau **pseudonimizarea**.

## Responsabilitățile noastre:

Trebuie să implementăm măsuri de securitate atunci când gestionăm orice tip de date cu caracter personal, dar ceea ce implementăm depinde de circumstanțele noastre particulare. Trebuie să asigurăm confidențialitatea, integritatea și disponibilitatea sistemelor și serviciilor pe care le folosim pentru procesarea datelor cu caracter personal.

Printre altele, acestea pot include politici de securitate a informațiilor, controale ale accesului, monitorizarea securității și scheme de recuperare.

---

*Trebuie luate măsuri de securitate adecvate de-a lungul ciclului de viață al datelor cu caracter personal și de către toate părțile interesate.*

---

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Aplicarea și revizuirea măsurilor de securitate definite în politica și directivele de securitate | DIDPGR007RO Regula 1 | Art.32 |
| • Integrarea revizuirii securității informațiilor și a protecției datelor în proiecte. | DIDPGR007RO Regula 2 | Art.32 |
| • Securitate, confidențialitate și protecție a datelor prin proiectare și implicite | DIDPGR007RO Regula 3 | Art.25 |
| • Integrarea clauzelor privind securitatea informațiilor și protecția datelor cu subcontractanții | DIDPGR007RO Regula 4 | Art.32 |

## Ne instruim angajații și ne îmbunătățim procesele interne.

# Datele cu caracter personal Clasificare

Procesarea datelor cu caracter personal sensibile și a anumitor categorii speciale de date cu caracter personal este interzisă, cu excepția unor cazuri specifice.

Aceste procesări necesită măsuri de protecție în ceea ce privește:

marcarea, accesul, transmiterea, transportul, copierea și imprimarea, stocarea și arhivarea, distrugerea.

**Clasificarea** indică protecția adaptată la sensibilitatea informațiilor sau a documentului.

Decizia de clasificare a oricărei informații sau a unui document este obligatorie și trebuie să aibă loc în cea mai timpurie etapă.

[DISUGR001EN] Directiva privind protecția informațiilor

| Personal data types | Personal data categories |
|---|---|
| Common personal data | Civil status, identity, identification data |
| | Personal life (living habits, marital status, etc. –excluding sensitive or dangerous data) |
| | Professional life (résumé, education and professional training, awards, etc.) |
| | Economic and financial information (income, financial situation, tax situation, etc.) |
| | Connection data (IP addresses, event logs, etc.) |
| | Location data (travels, GPS data, GSM data, etc.) |
| Personal data perceived as sensitive | Social security number |
| | Biometric data |
| | Bank data |
| Sensitive personal data in the meaning of [DP-Act] | Philosophical, political, religious and trade-union views, sex life, health data, racial or ethnic origin, data concerning health or sex life |
| | Offenses, convictions, security measures |

## Responsabilitățile noastre:

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Respectarea cadrului legal pentru procesarea datelor sensibile | DIDPGR004RO Regula 1 | Art.9 |
| • Interzicerea procesării datelor cu privire la condamnări penale și infracțiuni | DIDPGR004RO Regula 2 | Art.10 |
| • Limitați accesul la datele de sănătate numai la profesioniști autorizați | DIDPGR004RO Regula 3 | Art.9 |
| • Interziceți utilizarea numărului de identificare național ca identificator unic | DIDPGR004RO Regula 4 | Art.87 |
| • Restricționați accesul la și la utilizarea datelor bancare | DIDPGR004RO Regula 5 | Art.9 |
| • Restricționați accesul la datele sensibile la persoanele autorizate | DIDPGR004RO Regula 6 | Art.9 |
| • Efectuați evaluări ale impactului asupra confidențialității datelor subiecților de date implicați în procesarea datelor sensibile | DIDPGR004RO Regula 7 | Art.35 |
| • Limitați utilizarea câmpului de comentariu la informații generale | DIDPGR004RO Regula 8 | Cele mai bune practici |

## Sfaturi practice...

Exemple de măsuri de protecție care trebuie luate pentru fiecare categorie de active de informații clasificate (hârtie, digital, know-how, fizice).

# Păstrarea datelor

Necesitatea tot mai mare de a dematerializa operațiunile și schimbul de informații între Grup, clienții și partenerii noștri de afaceri, precum și cerințele legale și de reglementare, au supus Roquette unei serii de obligații în ceea ce privește durata perioadei de păstrare a datelor și politicile de gestionare a înregistrărilor.

Pe baza activităților noastre, Roquette achiziționează și procesează o cantitate mare de date sensibile legate de strategia noastră, rezultatele financiare, dezvoltarea comercială sau angajamentele noastre, **precum și date cu caracter personal legate de clienții, partenerii noștri de afaceri și membrii personalului**.

Informațiile trimise sau primite de Roquette în legătură cu activitățile noastre trebuie păstrate pentru o perioadă minimă de păstrare, chiar dacă nimic nu împiedică compania să le păstreze în arhive pentru perioade mai lungi, **cu excepția cazului în care conțin informații cu caracter personal**.

Această perioadă de timp, în care autoritățile administrative și competente pot efectua inspecții ulterioare, variază în funcție de natura informațiilor de păstrat și de cerințele legale relevante.

---

*Perioadele de stocare infinite sau nedeterminate sunt interzise.*

---

GDPR art. 5 1. E)

„limitarea stocări"

Datele cu caracter personal vor fi păstrate într-o formă care să permită identificarea subiecților nu mai mult decât este necesar pentru scopurile în care sunt procesate datele.

Datele cu caracter personal pot fi stocate pentru perioade mai lungi în măsura în care sunt procesate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică sau în scopuri statistice, sub rezerva implementării măsurilor tehnice și organizatorice adecvate necesare pentru protejarea drepturilor și libertăților subiectului de date.

## Responsabilitățile noastre:

- Roquette, în calitate de controlor de date, trebuie să definească perioade de stocare specifice și adecvate pentru fiecare categorie de date cu caracter personal colectate și procesate.
- Înainte de implementarea procesării datelor cu caracter personal, proprietarul proiectului, cu asistența unui coordonator pentru protecția datelor, trebuie să specifice în registrul nostru durata de păstrare a datelor.
- Trebuie să păstrăm datele cu caracter personal numai pentru perioada necesară procesării și să respectăm legile aplicabile.

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Limitați păstrarea datelor la ceea ce este strict necesar | DIDPGR002RO Regula 4 | Art. 5 1. E) |

În acest sens, Funcțiile globale, GBU-urile și zonele se angajează să respecte regulile de păstrare a informațiilor companiei și să mențină procedurile asociate în stare operațională.

## Exemplu:

La sfârșitul unui proces de recrutare trebuie să ștergem informațiile despre candidații nereușiți, cu excepția cazului în care aceștia sunt de acord să rămână în „pool-ul” nostru pentru o perioadă limitată de timp (2 ani).

## Ne instruim angajații și ne îmbunătățim procesele interne.

# 2 Standardele noastre în RELAȚIILE CU AFILIAȚII și SUBCONTRACTANȚII

# Calificarea procesatorului și a controlorului

**Controlor** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singure sau împreună cu alții, determină scopurile și mijloacele procesării datelor cu caracter personal.

**Controlor comun înseamnă** doi sau mai mulți controlori care determină împreună scopurile și mijloacele procesării. Însă, indiferent de aceste aranjamente, fiecare controlor rămâne responsabil pentru respectarea tuturor obligațiilor controlorilor în conformitate cu RGPD.

**Procesator** înseamnă o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism care procesează date cu caracter personal în numele controlorului.

## Cine este procesator în sensul Regulamentului general privind protecția datelor?

(Articolul 4 din RGPD – Definiții).

**O mare varietate de furnizori de servicii au capacitatea de procesatori** în sensul legal al termenului. Activitățile procesatorilor pot fi legate de o sarcină foarte specifică (subcontractarea livrării de poștă) sau pot fi mai generale și mai largi (gestionarea întregului serviciu în numele unei alte organizații, cum ar fi gestionarea salariilor angajaților, de exemplu).

**Următoarele sunt vizate în special de RGPD:**

- furnizori de servicii IT (găzduire, întreținere etc.), integratori de software, companii de securitate cibernetică sau companii de consultanță IT (cunoscute anterior ca fiind companii de servicii de inginerie IT) care au acces la date,
- agenții de marketing sau comunicare care procesează date cu caracter personal în numele clienților și
- mai general, orice organizație care oferă un serviciu care implică procesarea datelor cu caracter personal în numele unei alte organizații,
- o autoritate publică sau o asociație poate fi considerată ca atare.

În măsura în care nu au acces la date cu caracter personal sau nu le procesează, producătorii de software și producătorii de echipamente (cum ar fi terminalele de pontare, echipamentele biometrice sau echipamentele medicale) nu sunt vizați.

### Exemplu de calificare a procesatorului și a controlorului:

Firma A oferă un serviciu de livrare a scrisorilor de marketing utilizând fișierele cu date ale clienților firmelor B și C.

Compania A este un procesator pentru companiile B și C în măsura în care procesează datele necesare ale clienților pentru expedierea scrisorilor în numele și la comanda companiilor B și C.

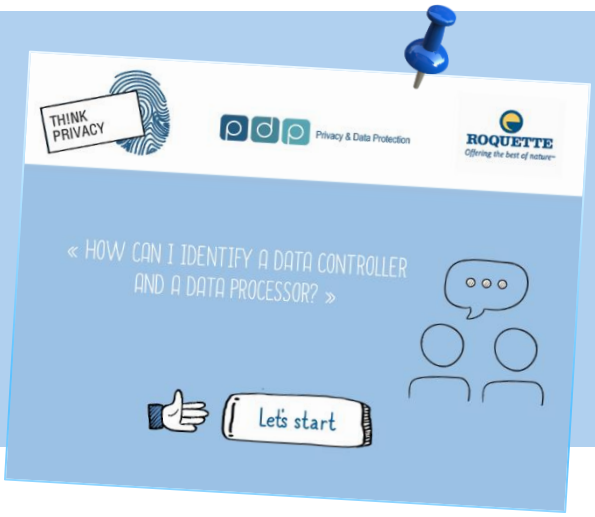
Companiile B și C sunt controlori de management ai clienților lor, inclusiv în ceea ce privește livrarea de scrisori de marketing.

Compania A este, de asemenea, controlor în ceea ce privește managementul personalului pe care îl angajează și managementul clienților săi, care includ companiile B și C.

## Text oficial

- Articolul 4 din RGPD pentru definițiile controlorului și procesatorului
- Articolul 28.10 din RGPD referitor la noțiunea de controlor

## Ne instruim angajații și ne îmbunătățim procesele interne.



# Clauze de protecție a datelor

## Când este necesar un contract și de ce este important?

Ori de câte ori, în calitate de controlor, utilizăm un procesator pentru a procesa date cu caracter personal în numele nostru, trebuie să existe un contract scris între părți.
Contractul este important pentru ca ambele părți să înțeleagă responsabilitățile și obligațiile noastre.

Contractele cu clauze specifice de protecție a datelor și/sau acordul de protecție a datelor dintre Roquette, în calitate de controlor și procesatorii săi asigură înțelegerea obligațiilor, responsabilităților și răspunderilor noastre. Contractele ne ajută, de asemenea, să respectăm GDPR și să demonstrăm persoanelor fizice și autorităților de reglementare conformitatea noastră, așa cum impune principiul responsabilității.

## Ce responsabilități și răspunderi avem noi, în calitate de controlor, atunci când utilizăm un procesator?

Trebuie să folosim numai procesatori care pot oferi garanții suficiente că vor implementa măsuri tehnice și organizatorice adecvate pentru a se asigura că procesarea lor va respecta cerințele RGPD și va proteja drepturile subiecților de date.

În calitate de controlor suntem responsabili în primul rând pentru conformitatea generală cu RGPD și cu alte legi privind confidențialitatea datelor în vigoare, precum și pentru demonstrarea acestei respectări. În cazul în care acest lucru nu este realizat putem fi obligați să plătim despăgubiri în cadrul procedurilor judiciare sau putem fi supuși amenzilor sau altor sancțiuni ori măsuri corective.

## Ce este nou conform RGPD?

GDPR impune ca cerință contracte scrise între controlori și procesatori, iar acestea să nu fie doar o modalitate de a demonstra conformitatea cu principiul protecției datelor (măsuri de securitate adecvate) în conformitate cu legile aplicabile privind protecția datelor.

Aceste contracte trebuie să includă acum termeni minimi specifici. Aceste condiții sunt concepute pentru a asigura faptul că procesarea efectuată de un procesator îndeplinește toate cerințele RGPD, nu doar cele legate de păstrarea securității datelor cu caracter personal.

| Regulă | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Integrarea clauzelor de securitate a informațiilor și protecție a datelor cu subcontractanții. | DIDPGR007RO Regula 4 | Art. 32 |
| • Securitatea contractanților | DSUG016EN | |

## Ce trebuie inclus în contract?

Contractele trebuie să stabilească:

- ☑ obiectul și durata procesării;
- ☑ natura și scopul procesării;
- ☑ tipul datelor cu caracter personal și categoriile subiecților de date; și
- ☑ obligațiile și drepturile controlorului.

Contractele trebuie să includă, de asemenea, termeni sau clauze specifice privind:

- ☑ procesarea numai pe baza instrucțiunilor documentate ale controlorului;
- ☑ obligația de confidențialitate;
- ☑ măsurile de securitate adecvate;
- ☑ utilizarea subcontractanților;
- ☑ drepturile subiecților de date;
- ☑ asistarea controlorului;
- ☑ clauze de terminare a contractului; și
- ☑ audituri și inspecții.

## Ne instruim angajații și ne îmbunătățim procesele interne.

- Ghid privind protecția datelor pentru subcontracte în conformitate cu RGPD.
- Modelul de acord de procesare a datelor disponibil în sistemul nostru de management al confidențialității: OneTrust@Roquette> Modulul de management al riscului furnizorilor.

# Acordul privind transferul datelor

Un **transfer de date** este orice comunicare, copiere sau tranzit de date cu caracter personal (cum ar fi serverele de găzduire, trimiterea de atașamente prin e-mail, instrumentele de acces de la distanță, partajarea ecranelor etc.) destinate procesării în alte țări care nu au aceleași legi aplicabile privind protecția datelor cu caracter personal.

Suntem mai conectați ca niciodată. Pentru Roquette, care operează la scară globală, transferul internațional de date este un element esențial al operațiunilor zilnice. Roquette, de exemplu, stochează datele cu caracter personal ale angajaților într-un serviciu cloud găzduit în străinătate și partajează datele cu caracter personal ale angajaților și clienților între filialele sale stabilite în întreaga lume.

Cum vor afecta GDPR și alte legi privind protecția datelor în vigoare astfel de transferuri internaționale de date?

## Responsabilitățile noastre:

Orice transfer de date cu caracter personal în curs de procesare sau destinat procesării după transferul într-o țară terță sau către o organizație internațională trebuie să aibă loc numai dacă:

- Legislația locală o permite și/sau autoritatea de supraveghere a decis că țara terță, un teritoriu sau unul ori mai multe sectoare specificate din această țară terță, sau organizația internațională în cauză asigură un nivel adecvat de protecție sau și-a dat autorizația și/sau

- Se ia o măsură legală (de ex.: Reguli corporative obligatorii sau clauze contractuale standard pentru transferul datelor cu caracter personal către procesatorii stabiliți în țări terțe în conformitate cu Directiva 95/46/CE a Parlamentului European și a Consiliului etc.).

| Regulă | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Luați măsuri pentru transferul datelor cu caracter personal către țări terțe sau organizații internaționale | DIDPGR002RO Regula 5 | Art. 44 până la 50 |

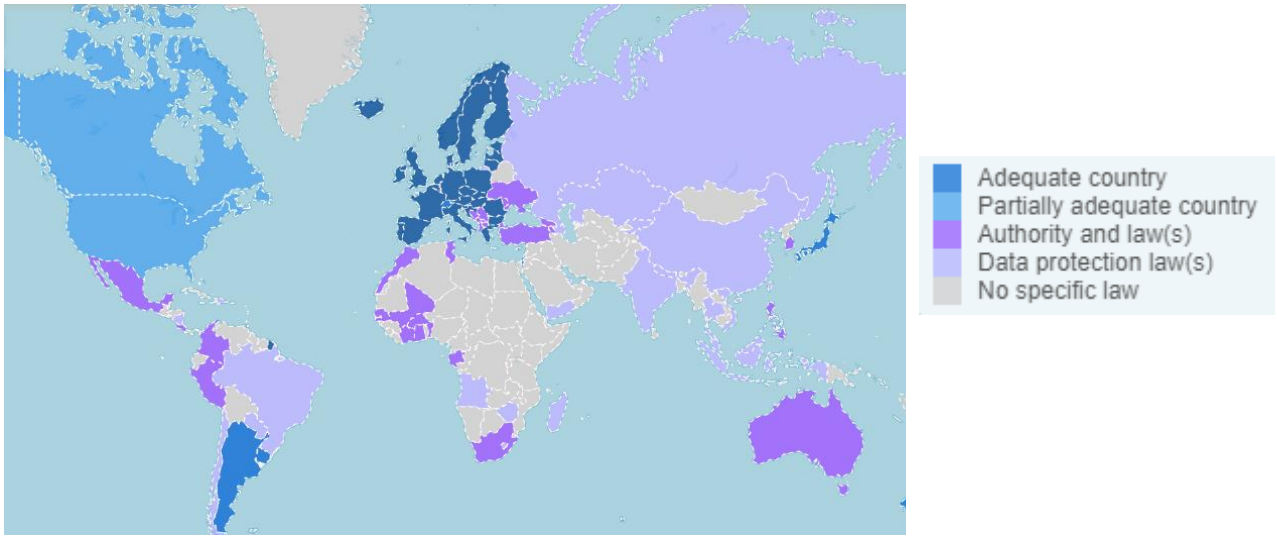
În orice caz, vă rugăm să contactați mai întâi DPO.

## În ce țară pot transfera date cu caracter personal și în ce condiții?

Pentru o imagine generală, consultați această hartă:

https://www.cnil.fr/en/data-protection-around-the-world.

Această hartă vă permite să vedeți nivelul de protecție a datelor în fiecare țară.




## Ne instruim angajații și ne îmbunătățim procesele interne.

- secțiunea Acord de transfer al datelor, inclusiv în modelul nostru de Acord de procesare a datelor.
- Întrebări frecvente pentru a aborda unele probleme ridicate de intrarea în vigoare a Deciziei Comisiei UE privind clauzele contractuale standard pentru transferul datelor cu caracter personal către procesatorii stabiliți în țări terțe.

# 3 Standardele noastre în RELAȚIILE cu REȚEAUA noastră și AUTORITĂȚILE DE SUPRAVEGHERE

# Responsabilul cu protecția datelor

Grupul a desemnat un responsabil cu protecția datelor.

**Responsabilul cu protecția datelor** sau DPO ne ajută să monitorizăm conformitatea internă, informează și consiliază cu privire la obligațiile noastre de protecție a datelor, oferă sfaturi cu privire la evaluările impactului asupra protecției datelor (DPIA) și acționează ca punct de contact pentru subiecții de date și autoritatea de supraveghere.

DPO trebuie să fie independent, expert în protecția datelor, să dispună de resurse adecvate și să raporteze la cel mai înalt nivel de management.

DPO ne poate ajuta să demonstrăm conformitatea și face parte din accentul sporit pus pe responsabilitate.

| Sarcinile DPO | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Responsabilul nostru cu protecția datelor are sarcina de a monitoriza conformitatea cu RGPD și cu alte legi privind protecția datelor, politicile noastre de protecție a datelor, sensibilizarea, instruirea și auditurile. | MA DPGR001EN Manual de protecție a datelor cu caracter personal | GDPR Articolul 39 Sarcinile responsabilului cu protecția datelor |
| • Vom lua în considerare recomandările responsabilului cu protecția datelor și informațiile pe care le furnizează cu privire la obligațiile noastre de protecție a datelor. | | |
| • Când efectuăm o DPIA, solicităm sfatul responsabilului nostru cu protecția datelor, care monitorizează și procesul. | | |
| • Responsabilul nostru cu protecția datelor acționează ca punct de contact pentru autoritățile de supraveghere. | | |
| • În îndeplinirea sarcinilor sale, responsabilul nostru cu protecția datelor ține cont în mod corespunzător de riscurile asociate operațiunilor de procesare și ia în considerare natura, domeniul de aplicare, contextul și scopurile procesării. | | |

Responsabilul cu protecția datelor din cadrul Grupului a fost desemnat la CNIL de către CEO pentru a prelua funcția la data de 25 mai 2018, data aplicării RGPD.

## Accesibilitatea DPO:

- Responsabila noastră cu protecția datelor, Jennifer Godin, este ușor accesibilă ca punct de contact pentru angajații noștri, persoanele fizice și autoritatea de supraveghere.
- Am publicat datele de contact ale DPO și le-am comunicat autorităților de supraveghere.
  - ☑ https://www.Roquette.com/data-protection

**Your point of contact**

Our Group Data Protection Officer is a single point of contact for our employees, individuals and the Supervisory Authorities concerning all privacy and data protection topics.

**Jennifer Godin, Group Data Protection Officer**
Roquette Frères, Legal & Compliance
Rue de la Haute Loge, 62136 Lestrem France

Email to DPO@roquette.com

## Contactați DPO în caz de:

- ☑ Procesarea datelor cu caracter personal
- ☑ Solicitări ale subiecților de date
- ☑ Violare a datelor cu caracter personal
- ☑ Necesar de sfaturi sau asistență

## Ne instruim angajații și ne îmbunătățim procesele interne.

# Rețeaua de protecție a datelor

Relațiile cu departamentele și DPO-urile sau coordonatorii locali reprezintă o rețea care permite responsabilului cu protecția datelor din cadrul Grupului, respectiv, să implementeze regulile privind protecția datelor cu caracter personal în fiecare unitate de afaceri și departament de asistență și să respecte cerințele legilor și reglementărilor relevante privind protecția datelor din țările în care își desfășoară activitatea Grupul.

RPD/Coordonatorii locali vor avea cel puțin următoarele sarcini:

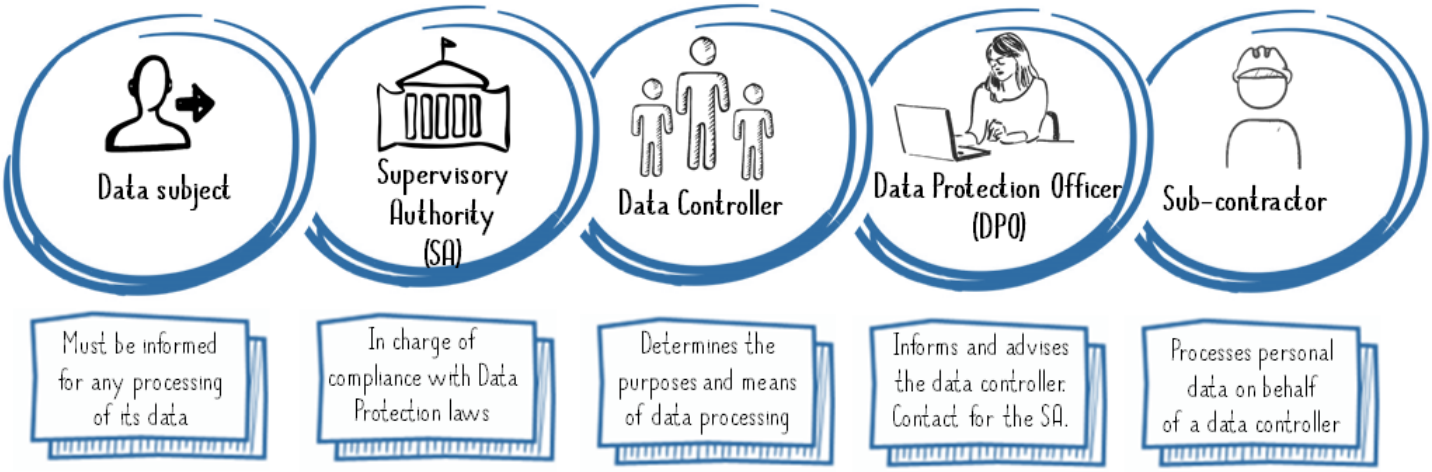
- Să informeze și să consilieze la nivel local cu privire la obligațiile care decurg din Politica Roquette privind protecția datelor cu caracter personal definită de DPO al Grupului Roquette și cerințele legilor locale aplicabile privind protecția datelor;
- Să monitorizeze conformitatea cu legislația locală, cu alte legislații și cu reglementările aplicabile privind protecția datelor, acolo unde este necesar, cu asistența DPO al Grupului Roquette și cu politicile legate de protecția datelor cu caracter personal;
- Să ofere consultanță la nivel local, acolo unde este necesar, cu privire la evaluarea impactului asupra protecției datelor și să monitorizeze performanța acesteia;
- Să coopereze cu autoritatea locală de supraveghere;
- Să acționeze ca punct de contact pentru DPO al Grupului Roquette cu privire la problemele legate de procesare și să consulte DPO al Grupului Roquette, dacă este cazul, cu privire la orice alte chestiuni;
- Să raporteze activitățile sale către DPO al Grupului Roquette pentru a contribui la sistemul de management al protecției datelor al Grupului.

## Ne instruim angajații și ne îmbunătățim procesele interne.

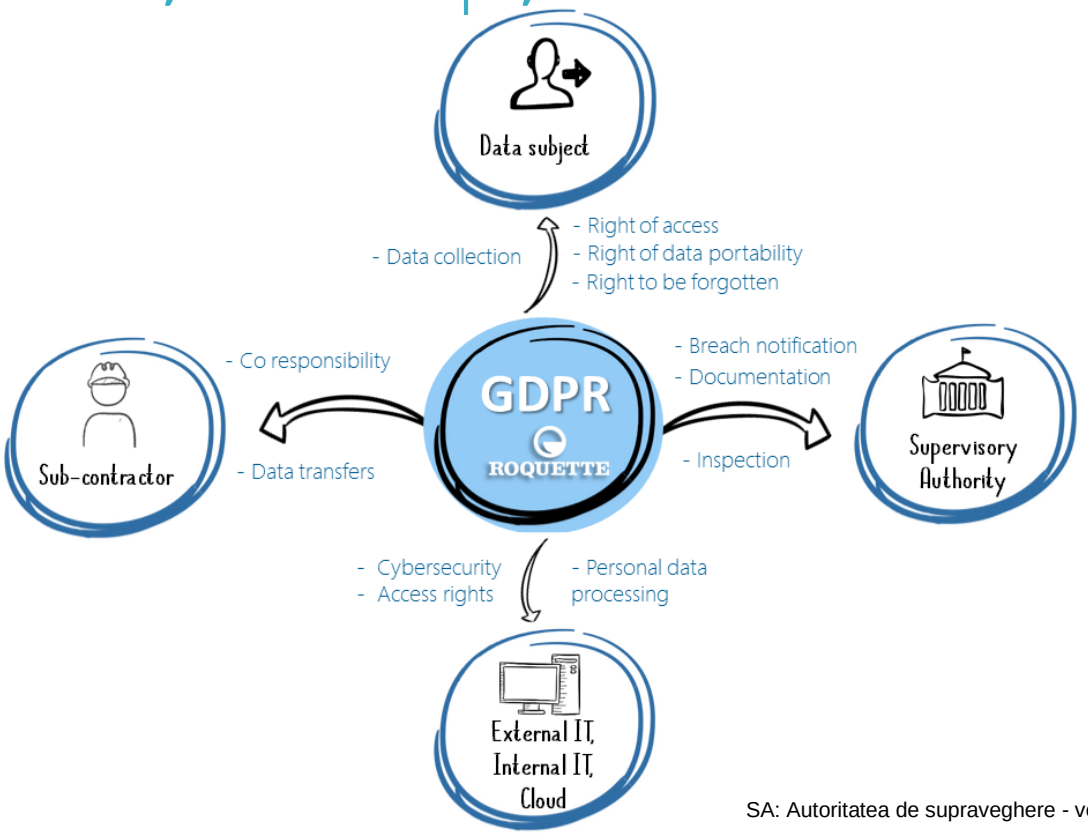
Seminarul nostru anual PDP este locul de întâlnire pentru rețeaua noastră de contribuitori la protecția datelor și confidențialitate.

# & părțile interesate

## Cine sunt noii actori?




## Care sunt relațiile dintre aceste părți interesate?




SA: Autoritatea de supraveghere - vezi pagina 50

# Autorități de supraveghere

În întreaga lume, multe țări au o lege privind protecția datelor și o

autoritate independentă pentru protecția datelor (DPA).

Aceste autorități sunt regulatorul național independent pentru confidențialitate și libertatea informațiilor. Aceștia promovează și mențin drepturile subiecților de date de a accesa informațiile deținute de organizații și le protejează datele cu caracter personal.

## Care este rolul unei autorități de supraveghere în contextul RGPD?

Fiecare stat membru va prevede ca una sau mai multe autorități publice independente să fie responsabile pentru monitorizarea aplicării legilor privind datele cu caracter personal și confidențialitatea, pentru a proteja drepturile și libertățile fundamentale ale subiecților de date în contextul procesării datelor cu caracter personal și pentru a facilita libera circulație a acestor date cu caracter personal în cadrul UE.

În contextul RGPD, toate statele membre ale UE au o autoritate de protecție a datelor, care, în general, servește ca principal punct de contact al părților interesate din statul membru respectiv.

Pentru a ne asigura că GDPR este aplicat în mod consecvent în UE, fiecare autoritate de supraveghere trebuie să colaboreze cu celelalte și cu Comisia Europeană.

Fiecare autoritate de supraveghere de pe teritoriul său trebuie să promoveze conștientizarea publicului și înțelegerea riscurilor, regulilor, garanțiilor și drepturilor în legătură cu procesarea datelor cu caracter personal.

Acestea sunt, de asemenea, locul la care să vă adresați în cazul unei încălcări a legislației privind protecția datelor și pentru sfaturi și întrebări specifice și/sau asistență din perspectiva organizațiilor.

Pe scurt, responsabilitățile autorităților de supraveghere (SA) sunt:

- să asigure aplicarea regulilor, inclusiv prin amenzi,
- să clarifice aplicarea regulilor, dacă este necesar, de ex. prin normative,
- să promoveze o cultură a dialogului cu toate părțile interesate, inclusiv cu companiile,
- să colaboreze.

CNIL : Comisia Națională de Informatică și Libertăți - French DPA.

## Autoritatea principală

- Autoritatea de supraveghere abilitată la sediul principal al controlorului sau al procesatorului trebuie să acționeze ca autoritate principală. Aceasta ar trebui să coopereze cu celelalte autorități implicate.

- Identificarea unei autorități de supraveghere principale este relevantă numai atunci când un controlor sau un procesator efectuează procesarea transfrontalieră a datelor cu caracter personal.

## Cum se identifică „autoritatea principală de supraveghere"?

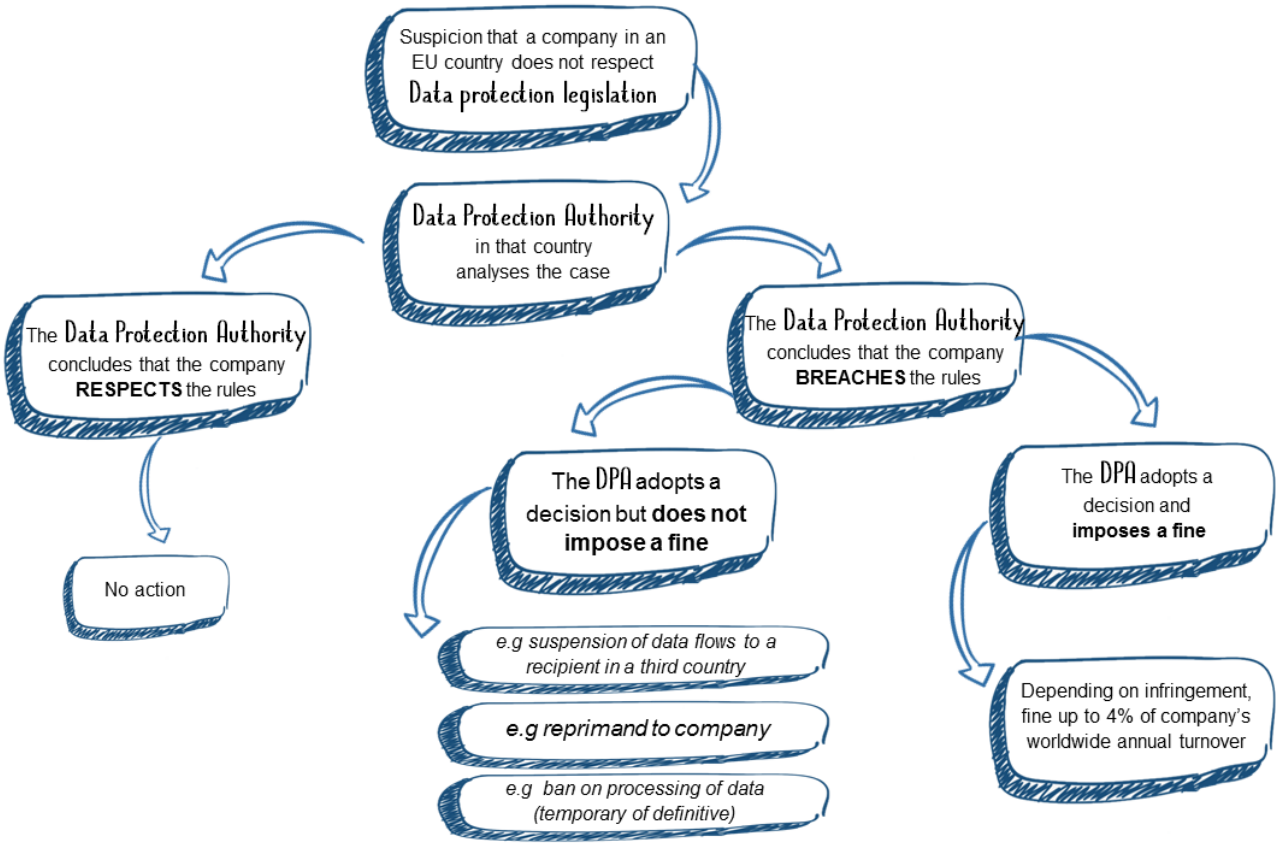
Identificați locul de administrare centrală al controlorului principal în UE.
Autoritatea de supraveghere a țării în care se află sediul administrației centrale este autoritatea principală a controlorului.

---

**CNIL** *este autoritatea principală de supraveghere a Roquette*

---

## Cum funcționează în practică mecanismul de sancționare GDPR?



# Guvernanță

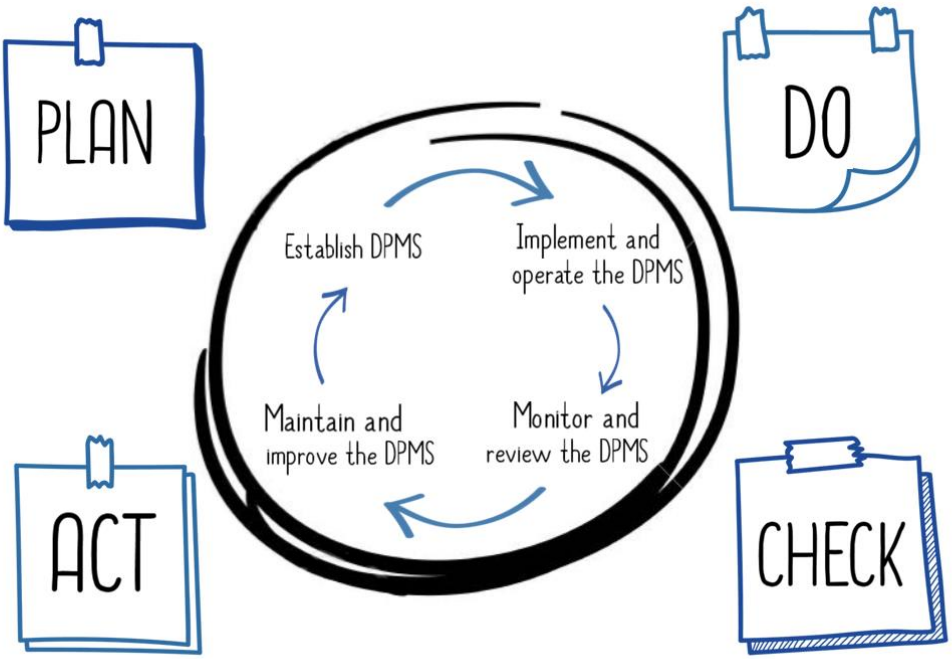
„**Organizația de protecție a datelor** este structurată în principal în jurul responsabilului cu protecția datelor, a coordonatorilor săi per locație și per funcție, directorului executiv în calitate de controlor de date, șefilor Funcțiilor globale în calitate de responsabili pentru implementarea procesării datelor cu caracter personal și subcontractanților în calitate de procesatori ." [M DPG001EN]

Adoptăm o abordare procesuală pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, întreținerea și îmbunătățirea sistemului de management al protecției datelor personale (DPMS) la Roquette.

Procesul și abordarea pentru managementul protecției datelor cu caracter personal definite în această guvernanță încurajează utilizatorii săi să sublinieze importanța:

1) înțelegerii cerințelor Roquette privind protecția datelor și necesității de a stabili directive și proceduri pentru protecția datelor;
2) implementării și operării controalelor pentru a gestiona riscurile de protecție a datelor la Roquette în contextul riscurilor generale de afaceri ale Roquette;
3) monitorizării și revizuirii performanței și eficacității DPMS; și
4) îmbunătățire continuă pe baza măsurării obiective.

Adoptăm modelul „Planificare-Executare-Verificare-Acționare" (PDCA),care este aplicat pentru a structura toate procesele sistemului de management al protecției datelor (DPMS).



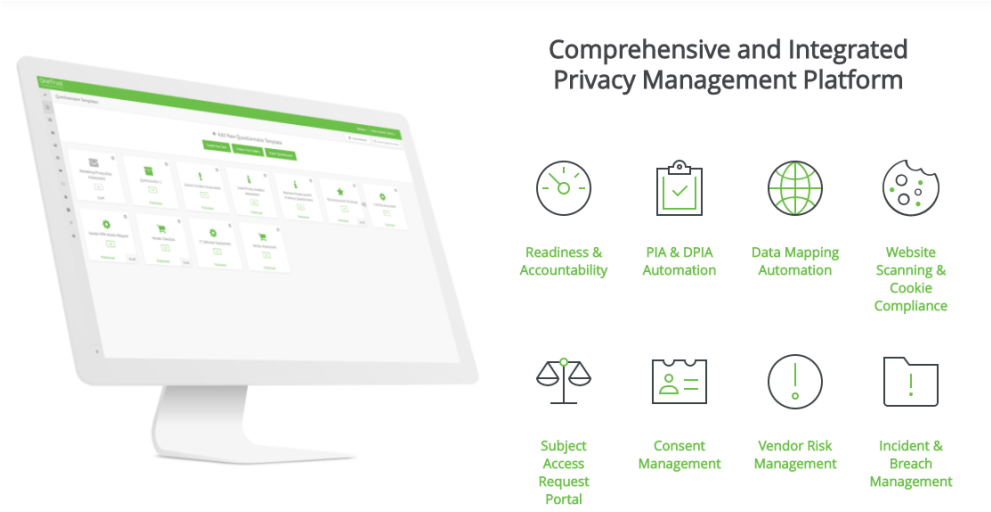
## Abordarea noastră:

Programul nostru de conformitate cu RGPD se axează pe:

- Înțelegerea modului în care organizația noastră colectează, stochează, utilizează și transferă datele pentru a asigura conformitatea,
- Crearea unei culturi a conformității în cadrul organizației noastre,
- Evaluarea impactului asupra confidențialității
- Pregătirea pentru o breșă de securitate a datelor,
- Alocarea resurselor pentru Programul de confidențialitate,
- Implementarea unui sistem de management al protecției datelor (Planificare - Executare - Verificare - Acționare).

Pentru a atinge aceste obiective, avem ca parte a programului nostru:

- Definirea unei Politici de protecție a datelor și a guvernanței și documentației asociate,
- A gestionat un proiect de conformitate cu RGPD pentru revizuirea procesării, gestionarea încălcărilor securității datelor, revizuirea contractelor, clauzelor privind protecția datelor, acordului de transfer al datelor etc.,
- Implementarea unui software de management al confidențialității în conformitate cu GDPR.




Principalele caracteristici ale acestei platforme de management sunt:

- Menținerea registrului de procesare a datelor (cartografierea datelor),
- Managementul riscurilor asociate procesării (din PIA etc.),
- Gestionarea solicitărilor și drepturilor (acces, rectificare, opoziție etc.),
- Managementul incidentelor și încălcărilor securității datelor,
- Managementul documentației de conformitate.

# Răspunderea

**Responsabilitatea** este unul dintre principiile protecției datelor. Aceasta ne face responsabili pentru respectarea RGPD și stabilește că trebuie să putem demonstra conformitatea noastră.

## De ce este importantă responsabilitatea?

Asumarea responsabilității pentru ceea ce facem cu datele cu caracter personal și demonstrarea măsurilor pe care le-am luat pentru a proteja drepturile oamenilor nu duce doar la o mai bună conformitate legală, ci ne oferă și un avantaj competitiv. Responsabilitatea este o oportunitate reală pentru noi de a arăta și de a dovedi modul în care respectăm confidențialitatea oamenilor. Acest lucru ne poate ajuta să dezvoltăm și să menținem încrederea oamenilor.

În plus, dacă ceva nu merge bine, capacitatea de a arăta că am luat în considerare în mod activ riscurile și am pus în aplicare măsuri și garanții ne poate ajuta să deținem protecție împotriva oricărei potențiale acțiuni de aplicare a legii. Pe de altă parte, dacă nu putem demonstra bune practici de protecție a datelor, ne putem expune amenzilor și daunelor de reputație.

## Ce înseamnă, în mod concret, respectarea principiului responsabilității?

Procesarea datelor cu caracter personal implică o obligație de diligență și adoptarea de măsuri concrete și practice pentru protecția acestora. Respectarea principiului responsabilității înseamnă:

- documentarea și comunicarea, după caz, a tuturor directivelor, procedurilor și practicilor legate de confidențialitate („Politica noastră");
- atribuirea unei persoane specificate din cadrul organizației (care, la rândul său, poate delega alte persoane din organizație, după caz) sarcina de implementare a Politicii;
- atunci când sunt transferate date cu caracter personal către terți, asigurarea că destinatarul terț va fi obligat să ofere un nivel echivalent de confidențialitate și protecție

a datelor prin mijloace contractuale sau de altă natură, cum ar fi politicile interne obligatorii (legislația aplicabilă poate conține cerințe suplimentare cu privire la transferurile internaționale de date);

- asigurarea unei instruiri adecvate pentru personalul controlorului de date care va avea acces la datele cu caracter personal;
- stabilirea unor proceduri interne eficiente de gestionare a reclamațiilor și de remediere pentru utilizarea de către Subiectul de date;
- informarea subiecților de date cu privire la încălcări ale confidențialității care le pot cauza daune substanțiale (cu excepția cazului în care acest lucru este interzis, de exemplu, în timpul lucrului cu autoritățile de aplicare a legii), precum și cu privire la măsurile luate pentru remediere;
- notificarea tuturor părților interesate relevante în materie de confidențialitate cu privire la încălcările confidențialității, după cum este necesar în unele jurisdicții (de exemplu, autoritățile de protecție a datelor) și în funcție de nivelul de risc;
- permiterea unui subiect de date afectat accesul la sancțiuni și/sau remedii adecvate și eficiente, cum ar fi rectificarea, eliminarea sau restituirea în cazul în care a avut loc o încălcare a confidențialității; și
- luarea în considerare a procedurilor de despăgubire pentru situațiile în care va fi dificil sau imposibil să se readucă starea de confidențialitate a persoanei fizice într-o poziție ca și cum nu s-ar fi întâmplat nimic.

## Listă de verificare:

- ☑ Ne asumăm responsabilitatea de a respecta GDPR, la cel mai înalt nivel de management și în întreaga noastră organizație.
- ☑ Păstrăm evidențe ale măsurilor pe care le luăm pentru a respecta RGPD.

Am implementat măsuri tehnice și organizatorice adecvate, cum ar fi:

- ☑ adoptarea și punerea în aplicare a regulilor de protecție a datelor;
- ☑ adoptarea unei abordări de „protecție a datelor prin proiectare și implicită” - implementarea măsurilor adecvate de protecție a datelor pe parcursul întregului ciclu de viață al operațiunilor noastre de procesare;
- ☑ încheierea de contracte în scris cu organizații care procesează date cu caracter personal în numele nostru;
- ☑ păstrarea documentației activităților noastre de procesare;
- ☑ implementarea măsurilor de securitate adecvate;
- ☑ înregistrarea și dacă este necesar, raportarea încălcărilor securității datelor cu caracter personal;
- ☑ efectuarea de evaluări ale impactului protecției datelor pentru utilizări ale datelor cu caracter personal care sunt susceptibile să ducă la un risc ridicat pentru interesele persoanelor;
- ☑ desemnarea unui responsabil cu protecția datelor; și
- ☑ respectarea codurilor de conduită relevante și înscrierea în scheme de certificare (dacă este posibil).

- ☑ Ne revizuim și actualizăm măsurile de responsabilizare la intervale adecvate.

# Documentație

## Ce este documentația?

Suntem obligați să păstrăm o evidență a activităților noastre de procesare, care acoperă domenii precum scopurile procesării, partajarea și păstrarea datelor; denumim aceasta **documentație**.

Documentarea activităților noastre de procesare este importantă, nu numai pentru că este o cerință legală în sine, ci și pentru că poate susține buna guvernanță a datelor și ne poate ajuta să demonstrăm conformitatea cu alte aspecte ale RGPD și cu legile aplicabile privind protecția datelor.

## Listă de verificare:

**Documentarea activităților de procesare - cerințe**

- ☑ În calitate de controlor de date pentru datele cu caracter personal pe care le procesăm, documentăm toate informațiile aplicabile în conformitate cu articolul 30(1) din RGPD.
- ☑ Noi documentăm în scris activitățile noastre de procesare.
- ☑ Ne documentăm activitățile de procesare într-un mod granular, cu legături semnificative între diferitele informații.
- ☑ Efectuăm revizuiri regulate ale datelor cu caracter personal pe care le procesăm și ne actualizăm documentația în consecință.

**Documentarea activităților de procesare - cele mai bune practici**

- ☑ Ne documentăm activitățile de procesare în format electronic, astfel încât să putem adăuga, elimina și modifica cu ușurință informații.

Când ne pregătim să ne documentăm activitățile de procesare:

- ☑ efectuarea de audituri de informații pentru a afla ce date cu caracter personal deține organizația noastră;
- ☑ utilizăm chestionare prin intermediul instrumentelor noastre digitale, de securitate și confidențialitate și discutăm cu personalul din întreaga organizație pentru a obține o imagine mai completă a activităților noastre de procesare; și
- ☑ revizuirea politicilor, directivelor, procedurilor, contractelor și acordurilor noastre pentru a aborda domenii precum păstrarea, securitatea și partajarea datelor.

Ca parte a evidenței activităților noastre de procesare, documentăm, sau facem legătura cu documentația, următoarele:

- ☑ informații necesare pentru notificările privind confidențialitatea;
- ☑ înregistrări ale consimțământului atunci când este necesar;
- ☑ contracte între controlor și procesator;
- ☑ locația datelor cu caracter personal;
- ☑ Rapoarte de evaluare a impactului asupra protecției datelor; și de asemenea,
- ☑ înregistrări ale încălcărilor securității datelor cu caracter personal;
- ☑ înregistrările solicitărilor subiecților de date.

# Unde se află documentația noastră privind protecția datelor?

**ONE**
Global Function
Data Protection

Privacy & Data Protection

"Data Protection is relevant to and the responsibility of everyone in our organization"

Content

- Laws and regulations
- Information and awareness
- Best practises and policies

**ONE**
Community
Data Protection Network

Data Protection Network

"We are all actors in the protection of personal data"

Content

- Personal Data Protection Policy
- Data Protection Management System
- Local Legislation
- Human resources
- Global Digital
- Legal & Compliance
- Internal Audit & Control
- GBU & Commercial
- Innovation, R&D
- Global Security
- Insurance & Risk Management

**OneTrust**
Privacy Management Software

OneTrust
Privacy Management Software
@ ROQUETTE

"Our Privacy Management tool dedicated to Privacy Security & Third Party Risk"

Modules

CULTURE → COMPLIANCE → ACCOUNTABILITY

# Evaluarea impactului asupra confidențialității

**Evaluarea impactului asupra confidențialității sau PIA** este un proces conceput pentru a descrie procesarea, pentru a evalua necesitatea și proporționalitatea acesteia și pentru a ajuta la gestionarea riscurilor pentru drepturile și libertățile persoanelor fizice rezultate din procesarea datelor cu caracter personal, evaluându-le și determinând măsurile pentru a le aborda.

Acronimul „**PIA** ” este utilizat interschimbabil pentru a face referire la Evaluarea impactului asupra confidențialității și **Evaluarea impactului asupra protecției datelor** (**DPIA**).

## Cum se desfășoară PIA?

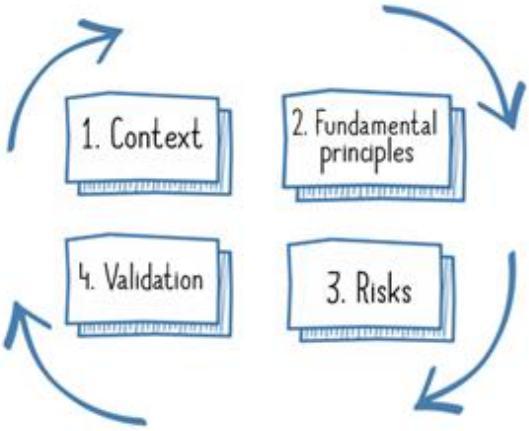
Abordarea conformității implementată prin efectuarea unui PIA se bazează pe doi piloni:

1) **drepturile și principiile fundamentale**, care sunt „nenegociabile”, stabilite prin lege și care trebuie respectate, indiferent de natura, gravitatea și probabilitatea riscurilor;
2) **managementul riscurilor de confidențialitate ale subiecților de date,** care determină măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal.

Compliance approach using a PIA

Pentru a rezuma, pentru a efectua un PIA este necesar să:

1) să definească și să descrie contextul procesării datelor cu caracter personal luate în considerare;
2) să analizeze măsurile de control care garantează respectarea principiilor fundamentale: proporționalitatea și necesitatea procesării, precum și protecția drepturilor subiecților de date;
3) să evalueze riscurile privind confidențialitatea asociate securității datelor și să se asigure că acestea sunt tratate în mod corespunzător;
4) să documenteze în mod formal validarea PIA în vederea faptelor anterioare sau să decidă să revizuiască pașii anteriori.




General approach for carrying out a PIA

Acesta este un proces de îmbunătățire continuă. Prin urmare, uneori este nevoie de mai multe iterații pentru a obține un sistem acceptabil de protecție a confidențialității. De asemenea, necesită monitorizarea modificărilor în timp (în context, controale, riscuri etc.), de exemplu în fiecare an și se actualizează de fiecare dată când are loc o modificare semnificativă.

Abordarea trebuie implementată de îndată ce este proiectată o nouă procesare a datelor cu caracter personal. Implementarea acestei abordări de la început face posibilă stabilirea controalelor necesare și suficiente și astfel, optimizarea costurilor. Pe de altă parte, implementarea sa după crearea sistemului și implementarea controalelor poate pune sub semnul întrebării alegerile făcute.

## Responsabilităţile noastre:

- În cazul în care un tip de procesare, în special prin utilizarea noilor tehnologii, și ținând cont de natura, domeniul de aplicare, contextul și scopurile procesării, este de natură să ducă la un risc ridicat pentru drepturile și libertățile persoanelor fizice, Roquette, în calitate de controlor, va efectua, înainte de procesare, o evaluare a impactului operațiunilor de procesare preconizate asupra protecției datelor cu caracter personal.
- Proprietarul proiectului va solicita sfatul responsabilului cu protecția datelor desemnat atunci când efectuează o evaluare a impactului asupra protecției datelor.

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Efectuarea PIA în caz de risc ridicat | DIDPGR003RO Regula 1 | Art. 35 |
| • Conținutul unui PIA | DIDPGR003RO Regula 2 | |
| • Sarcinile DPO cu privire la PIA | DIDPGR003RO Regula 3 | |
| • Revizuirea PIA | DIDPGR003RO Regula 4 | |

## Ne instruim angajaţii și ne îmbunătăţim procesele interne. și îmbunătăţim procesele noastre interne.

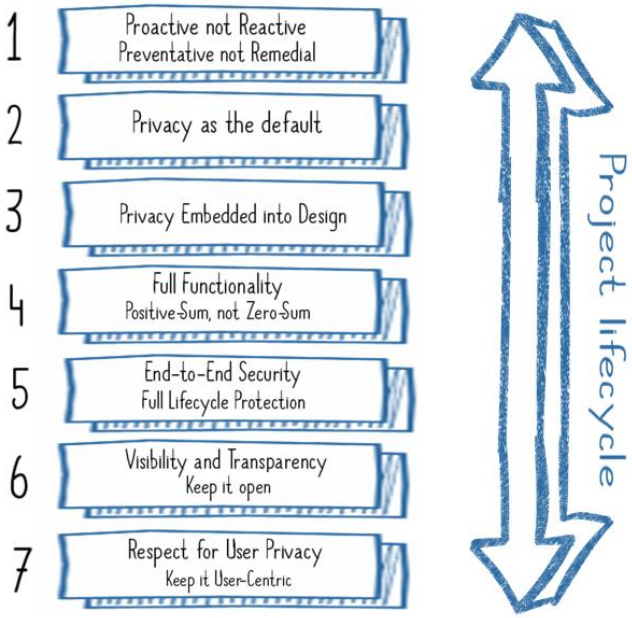
- Introducerea analizei securității și confidențialității în proiecte și contracte.
- Șablonul de evaluare a impactului asupra confidențialității se lansează automat în software-ul nostru de management al confidențialității OneTrust@Roquette atunci când este necesar.

## Aflaţi mai multe de aici:

Metodologia CNIL PIA, ediția 2018 - https://www.CNIL.fr/en/home

# Confidențialitate prin proiectare și implicită

**Confidențialitatea prin** proiectare înseamnă integrarea confidențialității în proiectarea, operarea și gestionarea unui anumit sistem, proces de afaceri sau specificație de proiectare.




## Ce este protecția datelor prin proiectare?

Legislația privind protecția datelor conține principii de bază pentru protejarea confidențialității subiecților de date.

Protecția datelor prin proiectare și implicită ajută la asigurarea faptului că sistemele informaționale pe care le utilizăm respectă aceste principii de protecție a datelor și protejează drepturile subiecților de date.

## Considerăm că:

Roquette se bazează pe sisteme informaționale și baze de date pentru a efectua o serie de sarcini operaționale și administrative. O mare parte din aceste sisteme informaționale procesează date cu caracter personal, prin urmare, respectarea deplină a reglementărilor este de cea mai mare importanță.

Companiile care iau în serios problemele legate de protecția datelor clădesc încredere.

Astfel, măsurile puternice de protecție a datelor pot fi un avantaj competitiv.

Angajamentul conducerii este esențial pentru a lua decizia de aplicare a principiilor de protecție a datelor prin proiectare în achizițiile și dezvoltarea software-ului organizației.

De asemenea, conducerea trebuie să se asigure că furnizează resurse suficiente pentru această sarcină.

Luarea în considerare a protecției datelor pe parcursul întregului proces de dezvoltare este atât rentabilă, cât și mai eficientă decât modificarea unui software existent.

## Responsabilitățile noastre:

Conform RGPD, protecția datelor prin proiectare a devenit pentru prima dată o obligație legală. Aceasta înseamnă că protecția datelor și confidențialitatea trebuie integrate în specificațiile de proiectare și arhitectura sistemelor și tehnologiilor de informare și comunicare.

Roquette, în calitate de controlor de date, trebuie să respecte cerințele care reglementează protecția datelor prin proiectare în timpul dezvoltării software-ului și la comandarea sistemelor, soluțiilor și serviciilor.

În consecință, cerințele trebuie să fie incluse și la încheierea contractelor cu furnizorii și la utilizarea consultanților (cf. standardelor noastre cu subcontractanții).

| Regulă | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Securitate, confidențialitate și protecție a datelor prin proiectare și implicite | DIDPGR007EN Regula 3 | Art. 25 |

## Listă de verificare:

- ☑ Analiza evaluării impactului asupra protecției datelor (DPIA)
- ☑ Evitați, limitați sau minimizați necesitatea de a colecta și procesa date cu caracter personal sensibile
- ☑ Limitare și minimizare a expunerii la funcții inutile și la date cu caracter personal în interfața utilizatorului
- ☑ Anonimizare sau pseudonimizare a datelor cu caracter personal ori de câte ori este posibil
- ☑ Toate configurațiile care asigură confidențialitatea trebuie să fie activate în mod implicit
- ☑ Urmărirea de la un site web la altul trebuie dezactivată în mod implicit
- ☑ Retragerea consimțământului prin intermediul unui meniu din software. Rețineți că colectarea datelor cu caracter personal trebuie să înceteze dacă este retras consimțământul
- ☑ Setările trebuie prezentate într-un meniu în care subiectul de date trebuie să facă o alegere conștientă de a „modifica” activ setările astfel încât să fie mai puțin favorabile confidențialității
- ☑ Urmărirea dispozitivului trebuie dezactivată în mod implicit

## Ne instruim angajații și ne îmbunătățim procesele interne.

- Ghidul comunității noastre „Rețeaua de protecție a datelor”.
- Metodologii: Revizuirea securității și conformității în proiecte și contracte.
- Învățare pe platforma HR.

# Notificare privind violarea datelor

## Ce este o violare a securității datelor cu caracter personal?

**Încălcarea securității datelor cu caracter personal** înseamnă o încălcare a securității care duce la distrugerea accidentală sau ilegală, pierderea, modificarea, divulgarea neautorizată sau accesul la datele cu caracter personal transmise, stocate sau procesate în orice alt mod.

*Aceasta înseamnă că o violare a securității datelor înseamnă mai mult decât **pierderea** datelor cu caracter personal.*

## Exemple:

- Pierderea unei baze de date a clientului
- Dezvăluirea evaluării performanțelor angajaților

## Responsabilitățile noastre:

Trebuie să aplicăm reguli pentru a trata orice încălcare a securității datelor cu caracter personal într-un mod care să limiteze impactul asupra subiecților de date și să împiedice reapariția acesteia.

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Notificarea unei încălcări a securității datelor cu caracter personal către responsabilul cu protecția datelor. | DIDPGRO08RO Regula 1 | Art. 33 |
| • Notificarea unei încălcări a securității datelor cu caracter personal către autoritatea de supraveghere. | DIDPGRO08RO Regula 2 | |
| • Comunicarea unei încălcări a securității datelor cu caracter personal către subiectul de date. | DIDPGRO08RO Regula 3 | Art. 34 |

## Cât timp avem la dispoziție pentru a raporta o încălcare?

Trebuie să raportăm o încălcare (care trebuie raportată) autorității de supraveghere fără întârziere nejustificată, dar nu mai târziu de 72 de ore de la luarea la cunoștință a acesteia.

## Ce încălcări trebuie să raportăm autorității de supraveghere competente?

Suntem obligați să informăm autoritatea de supraveghere competentă cu privire la o încălcare numai dacă aceasta poate duce la un risc pentru drepturile și libertățile persoanelor fizice. Dacă nu este remediată, este probabil ca o astfel de încălcare să aibă un efect dăunător semnificativ asupra persoanelor. De exemplu:

- să conducă la discriminare;
- deteriorarea reputației;
- pierderi financiare; sau
- pierderea încrederii sau orice alt dezavantaj economic sau social semnificativ.

Trebuie să evaluăm acest lucru de la caz la caz și trebuie să putem justifica decizia dvs. de a raporta o încălcare autorității de supraveghere.

## Când trebuie să înștiințăm persoanele?

Dacă este probabil ca o încălcare să ducă la un **risc ridicat** pentru drepturile și libertățile persoanelor fizice, trebuie să informăm direct persoanele afectate fără întârziere nejustificată.

Obligația de a notifica o persoană cu privire la o încălcare nu se aplică dacă:

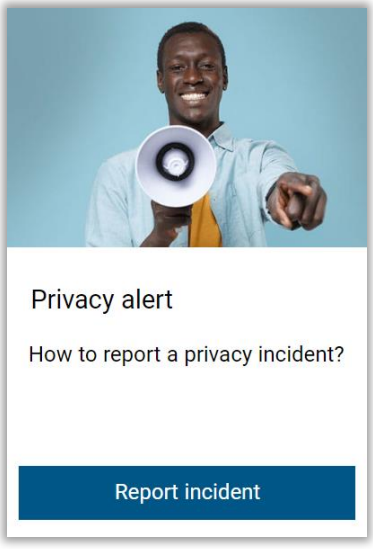
- am implementat măsuri tehnice și organizatorice adecvate care au fost aplicate datelor cu caracter personal afectate de încălcare;
- am luat măsuri ulterioare care vor asigura faptul că nu mai este probabil să se materializeze niciun risc ridicat pentru drepturile și libertățile persoanelor; sau
- ar implica un efort disproporționat.

În cazul în care comunicarea unei încălcări ar implica un efort disproporționat, trebuie să punem informațiile la dispoziția persoanelor într-un alt mod, la fel de eficient, cum ar fi o comunicare publică.

## Pe cine trebuie să contactăm în cazul unei încălcări a securității datelor?

Vă rugăm să contactați **responsabilul cu protecția datelor** la dpo@Roquette.com și/sau să raportați incidentul prin intermediul formularului nostru web„Alertă de confidențialitate".

**Dacă trebuie să raportați o potențială încălcare a** conformității, puteți lua legătura cu punctul dvs. de contact obișnuit sau puteți raporta o problemă prin intermediul instrumentului confidențial de alertă Roquette: Speakup©.




SpeakUp

# Monitorizare și revizuire

## Considerăm că:

Roquette se angajează să:

- ☑ asigure o **monitorizare** juridică și tehnologică a cerințelor de protecție a datelor,
- ☑ **să** revizuim și **să** îmbunătățim sistemul nostru de management al protecției datelor (DPMS)

pentru a ține cont de evoluțiile normative și tehnologice, precum și de constrângerile interne ale serviciilor. [DIDPGR009EN]

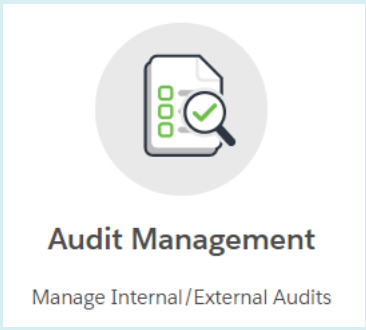
## Responsabilitățile noastre:

| Reguli | Referință OneDoc | Referință GDPR |
|---|---|---|
| • Asigurarea unei monitorizări și revizuiri legale și tehnologice a protecției datelor cu caracter personal | DIDPGR009RO Regula 1 | |
| • Monitorizarea regulată a implementării DPMS și a directivelor privind protecția datelor | DIDPGR009RO Regula 2 | Cele mai bune practici |
| • Revizuirea periodică a politicii de protecție a datelor cu caracter personal și a documentației DPMS | DIDPGR009RO Regula 3 | |

## Ne instruim angajații și ne îmbunătățim procesele interne.

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

pdp Privacy & Data Protection News



*Proiectarea și susținerea Programului nostru de confidențialitate*

## Software de cercetare în domeniul reglementărilor:

Utilizăm o platformă care oferă o gamă de soluții de confidențialitate concepute pentru a ne ajuta să monitorizăm evoluțiile normative, să reducem riscurile și să obținem conformitatea globală:

- ☑ Urmărirea reglementărilor
- ☑ Grafice comparative transfrontaliere
- ☑ Ghiduri de utilizare
- ☑ Portal GDPR
- ☑ Modele și liste de verificare
- ☑ Cereți un serviciu de analist
- ☑ Cercetare juridică

## Auditul și revizuirea sistemului de management al protecției datelor:

Efectuăm audituri interne pentru a stabili dacă măsurile sistemului DPMS sunt:

- ☑ în conformitate cu cerințele acestui ghid, ale politicii și ale legislației sau reglementărilor aplicabile;
- ☑ implementate și menținute în mod eficient; și
- ☑ executate conform așteptărilor.

Realizăm o revizuire a managementului DPMS pentru a ne asigura că domeniul de aplicare rămâne adecvat și că sunt identificate îmbunătățiri în procesul DPMS.

Pentru aceasta, măsurile sunt:

- ☑ Obiectivele, controalele, procesele și procedurile DPMS;
- ☑ Rezultatele auditurilor și controalelor anterioare de conformitate;
- ☑ Feedback de la părțile interesate;
- ☑ Tehnici, produse sau proceduri care ar putea fi utilizate în organizație pentru a îmbunătăți performanțele și eficacitatea DPMS;
- ☑ Starea acțiunilor preventive și corective;
- ☑ Vulnerabilități sau amenințări care nu au fost abordate în mod adecvat în evaluarea anterioară a riscurilor;
- ☑ Rezultatele măsurătorilor eficacității;
- ☑ Acțiunile ulterioare din evaluările anterioare ale managementului;
- ☑ Orice modificări care ar putea afecta DPMS; și
- ☑ Recomandări de îmbunătățire

# Documente de referinţă

- [Codul de conduită] Codul de conduită al Grupului Roquette
- [GDPG001RO] Glosar de definiții referitoare la protecția datelor
- [MDPG001RO] Manual de protecție a datelor cu caracter personal
- [DIDPGR001EN] Directiva privind cultura respectării confidențialității și protecției datelor
- [DIDPGR002EN] Directiva privind legalitatea procesării datelor cu caracter personal
- [DIDPGR003EN] Directiva privind evaluarea impactului asupra confidențialității
- [DIDPGR004EN] Directiva privind procesarea datelor sensibile
- [DIDPGR005EN] Directiva privind evidența activităților de procesare
- [DIDPGR006EN] Directiva privind respectarea drepturilor persoanelor
- [DIDPGR007RO] Directiva privind securitatea datelor cu caracter personal
- [DIDPGR008EN] Directiva privind notificarea unei încălcări a securității datelor cu caracter personal
- [DIDPGR009EN] Directiva privind revizuirea sistemului de management al protecției datelor cu caracter personal
- [DIDPGR010RO] Directiva privind confidențialitatea și protecția datelor în sistemul de management al alertelor
- [DISUGR001EN] Directiva privind protecția informațiilor și confidențialitatea

# Bibliografie

[Carta UE] Carta drepturilor fundamentale a Uniunii Europene, 2010/C 83/02.

[RGPD] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește procesarea datelor cu caracter personal și libera circulație a acestor date și abrogarea Directivei 95/46/CE (Regulamentul general privind protecția datelor).

[DP-Act] Legea franceză privind protecția datelor nr. 78-17 din 6 ianuarie 1978, modificată.

[WP29 - Instrucțiuni] Instrucțiuni pentru identificarea autorității principale de supraveghere a controlorului sau a procesatorului | WP 244 rev.01 (5 aprilie 2017).

[Directivele WP29 ] Directive privind evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă procesarea este „probabilă să ducă la un risc ridicat" în sensul Regulamentului 2016/679 | WP 248 rev.01 (13 octombrie 2017).

[Directive WP29] Directive privind aplicarea și stabilirea amenzilor administrative în sensul Regulamentului 2016/679 | WP 253 (21 octombrie 2017).

[Directive WP29] Directive privind luarea automatizată a deciziilor individuale și crearea de profiluri în sensul Regulamentului 2016/679 | WP 251 rev.01 (13 februarie 2018).

[Directive WP29] Directive privind responsabilii cu protecția datelor („DPO") | WP 243 rev.01 (5 aprilie 2017).

[Directive WP29] Directive privind transparența în conformitate cu Regulamentul 2016/679 | WP260 rev.01 (11 aprilie 2018).

[Directive WP29] Directive privind consimțământul în conformitate cu Regulamentul 2016/679 | WP259 rev.01 (11 aprilie 2018).

[Aviz EDPB] Avizul 23/2018 privind propunerile Comisiei privind producția europeană și ordinele de păstrare a dovezilor electronice în materie penală (art. 70.1.b) (26 septembrie 2018).

[Aviz EDPB ] Avizul 28/2018 privind decizia de punere în aplicare a proiectului Comisiei Europene privind protecția adecvată a datelor cu caracter personal în Japonia (5 decembrie 2018).

[Aviz EDPB ] Avizul 14/2019 privind proiectul de clauze contractuale standard prezentat de DK SA (articolul 28(8) RGPD) (12 iulie 2019).

[Recomandarea EDPB] Recomandarea 01/2019 privind proiectul de listă al Autorității Europene pentru Protecția Datelor cu privire la operațiunile de procesare care fac obiectul cerinței unei evaluări a impactului asupra protecției datelor (articolul 39(4) din Regulamentul (UE) 2018/1725) (10 iulie 2019).

[Răspunsul comun EDPB - EDPS ] Răspunsul comun EPDB-EDPS adresat Comitetului LIBE privind impactul legii cloud-ului din SUA asupra cadrului juridic european pentru protecția datelor cu caracter personal (Anexă) (10 iulie 2019).

[Avizul EDPB] Avizul 13/2019 privind proiectul de listă al autorității de supraveghere competente din Franța cu privire la operațiunile de procesare scutite de obligația unei evaluări a impactului asupra protecției datelor (articolul 35 (5) din RGPD) (10 iulie 2019).

# Surse

- Comisia Națională pentru Informatică și Libertăți
    - https://www.cnil.fr/en/home
    - Mai 2022
    - Licență: CC-BY-ND 3.0 FR
- Biroul comisarului pentru informații
    - https://ico.org.uk/
    - Mai 2022
    - Licențiat în baza licenței guvernamentale deschise
- Uniunea Europeană
    - https://eur-lex.europa.eu
    - 1998-2022
- https://www.iso.org/home.html
- https://www.dataguidance.com/
- https://www.onetrust.com/
- https://www.corporatefiction.fr/
- https://pixabay.com/fr/service/license/

Aceste surse sunt utilizate exclusiv și strict în scopuri educaționale, de învățare și de sensibilizare.

Actorii menționați nu susțin și nu oferă nicio garanție cu privire la conținutul acestei lucrări.

Drepturile de proprietate intelectuală, inclusiv drepturile de autor asupra materialelor, le aparțin în continuare.

Referinţă este versiunea în limba engleză a acestui Cod de conduită.
Traducerile acestui document pot fi supuse interpretării.
Prima ediţie: Septembrie 2019
Ediția a doua: Mai 2022
Publicată de ROQUETTE FRERES
Autor: Jennifer Godin, responsabilă cu protecția datelor
Designul şi grafica editorială: Biroul de conformitate
Fotografie: utilizare liberă

Toate drepturile rezervate. Nicio parte a acestui document nu poate fi reprodusă sau utilizată sub nicio formă, electronică sau mecanică, inclusiv prin fotocopiere, scanare, înregistrare sau prin sisteme de stocare sau recuperare a informațiilor, fără permisiunea explicită în scris a dpo@roquette.com.

**Utilizare externă autorizată.**

ROQUETTE

*Offering the best of nature™*