

**GRUPUL DE LUCRU PRIVIND PROTECȚIA DATELOR INSTITUIT
ÎN TEMEIUL ARTICOLULUI 29**



**538/14/RO
WP 212**

Avizul 02/2014 referitor la un referențial privind cerințele pentru regulile corporatiste obligatorii prezentate autorităților naționale de protecție a datelor din UE și pentru regulile transfrontaliere privind protecția vieții private prezentate agenților APEC cu responsabilități în materie de CBPR

Adoptat la 27 februarie 2014

Acest grup de lucru a fost creat în temeiul articolului 29 din Directiva 95/46/CE și este un organism consultativ european independent care se ocupă cu protecția datelor și a vieții private. Sarcinile sale sunt prezentate la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Drepturi fundamentale și cetățenia Uniunii) a Comisiei Europene, Direcția Generală Justiție, B-1049 Bruxelles, Belgia, Biroul MO-59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/index_ro.htm

Activitate comună a experților din Grupul de lucru instituit în temeiul articolului 29 și din economiile APEC cu privire la un referențial privind cerințele pentru regulile corporatiste obligatorii prezentate autorităților naționale de protecție a datelor din UE și pentru regulile transfrontaliere privind protecția vieții private prezentate agenților APEC cu responsabilități în materie de CBPR

PREZENTARE GENERALĂ

Obiectivul referențialului:

Obiectivul prezentului referențial este de a servi ca listă de verificare pragmatică informală pentru organizațiile care solicită aprobarea BCR („binding corporate rules” – reguli corporatiste obligatorii) și/sau certificarea CBPR („cross border privacy rules” – reguli transfrontaliere privind protecția vieții private). Prin urmare, acesta facilitează elaborarea și adoptarea de politici în materie de protecție a datelor cu caracter personal care să fie în conformitate cu fiecare dintre sistemele respective.

Referențialul nu urmărește să realizeze recunoașterea reciprocă a celor două sisteme. Cu toate acestea, referențialul ar putea servi ca fundament pentru **certificarea dublă**. În orice caz, politicile în materie de protecție a datelor ale întreprinderilor internaționale solicitante care își desfășoară activitatea atât în zona UE, cât și în zona APEC **trebuie să fie aprobate** de către organismele relevante din statele membre ale UE și, respectiv, din economiile APEC în conformitate cu procedurile de aprobare aplicabile.

Context:

Experții din Grupul de lucru instituit în temeiul articolului 29 al autorităților de protecție a datelor din UE (denumit în continuare „WP29”)¹ și din economiile membre ale Subgrupului APEC privind confidențialitatea datelor au creat un instrument practic pentru a prezenta cerințele pentru BCR și, respectiv, pentru CBPR (denumit în continuare „referențial”)².

Referențialul enumeră într-un singur document principalele elemente solicitate de către autoritățile pentru protecția datelor din UE (denumite în continuare „APD”) pe de o parte, și de către organismele relevante din economiile APEC, pe de altă parte, cu privire la politicile în materie de protecție a vieții private înaintate în vederea aprobării ca BCR de către APD naționale din UE, în conformitate cu legile în materie de protecție a datelor aplicabile în statele membre ale UE, și/sau ca CBPR, în conformitate cu normele aplicabile în economiile APEC.

¹ WP29 a fost instituit în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. WP29 este alcătuit dintr-un reprezentant al autorității (autorităților) de supraveghere desemnat de fiecare stat membru al UE, un reprezentant al Autorității Europene pentru Protecția Datelor și un reprezentant al Comisiei Europene. Grupul are caracter consultativ și acționează independent.

² În viitor, este posibil ca sectorul industriei și societatea civilă să furnizeze date către APEC și WP29 în conformitate cu mecanismele APEC de angajament al părților interesate și, respectiv, cu mecanismele de consultare ale WP29.

Referențialul a fost aprobat de către înalții funcționari ai APEC în cadrul reuniunii acestora din 27-28 februarie 2014, iar Grupul de lucru instituit în temeiul articolului 29 a adoptat un aviz/document de lucru cu privire la acesta în cadrul reuniunii sale plenare din 26-27 februarie 2014.

Structura referențialului:

Pentru fiecare dintre principiile și cerințele esențiale ale sistemului, referențialul conține:

- un „**bloc comun**” care descrie principalele elemente comune sau similare ale BCR și CBPR;
- „**blocuri suplimentare**” care prezintă principalele diferențe dintre acestea și elementele suplimentare specifice BCR, pe de o parte, și CBPR, pe de altă parte.

Deși blocul comun arată că există puncte comune între cerințele obligatorii ale sistemului CBPR și cele ale sistemului BCR, acesta nu este suficient în sine pentru a obține certificarea unor CBPR de către un agent cu responsabilități în acest domeniu recunoscut de APEC, nici autorizarea unor BCR de către o APD națională din UE. În plus, elementele cuprinse în blocul suplimentar al BCR **trebuie să fie luate în considerare, de asemenea**, de către o organizație care solicită aprobarea BCR proprii de către APD, iar elementele enumerate în blocul suplimentar al CBPR **trebuie să fie luate în considerare, de asemenea**, de către o organizație care solicită certificarea CBPR proprii de către un agent al APEC cu responsabilități în acest domeniu.

**REFERENȚIAL PRIVIND CERINȚELE PENTRU REGULILE
CORPORATISTE OBLIGATORII PREZENTATE AUTORITĂȚILOR
NAȚIONALE DE PROTECȚIE A DATELOR DIN UE ȘI PENTRU
REGULILE TRANSFRONTALIERE PRIVIND PROTECȚIA VIEȚII
PRIVATE PREZENTATE AGENȚILOR CU RESPONSABILITĂȚI ÎN
MATERIE DE CBPR RECUNOSCUȚI DE APEC**

Cuprins

Introducere	7
Scop și structură	7
Domeniu de aplicare.....	8
Referențial privind cerințele pentru BCR și CBPR în materie de protecție a datelor cu caracter personal și a vieții private.....	11
1. Obiectivul regulilor unei organizații privind protecția datelor cu caracter personal și a vieții private.....	11
2. Domeniul de aplicare al regulilor unei organizații privind protecția datelor cu caracter personal și a vieții private.....	13
3. Obligație executorie în cadrul unei organizații	15
4. Măsuri reparatorii pentru drepturile persoanelor vizate și ale beneficiarilor terți.....	17
5. Răspunderea	19
6. Obligații executorii privind transferurile către terți.....	21
7. Relații cu persoane împuternicite de către operator care sunt membri ai grupului.....	24
8. Restricții privind transferurile și transferurile ulterioare către persoanele externe împuternicite de operator și către operatorii externi (care nu sunt membri ai grupului).....	27
9. Definiții	30
10. Colectarea, prelucrarea și utilizarea informațiilor cu caracter personal	31
11. Calitatea și proporționalitatea/integritatea datelor.....	32
12. Motive pentru prelucrarea datelor cu caracter personal	33
13. Date sensibile	37
14. Dreptul la transparență și informare/notificare.....	39
15. Drepturile de acces, rectificare, ștergere și blocare a datelor/acces și corectare.....	42
16. Dreptul de opoziție/dreptul de a alege.....	45
17. Decizii individuale automate.....	48
18. Securitate și confidențialitate	49
19. Programul de formare.....	51

20. Programul de monitorizare și audit	52
21. Conformitatea și monitorizarea conformității	54
22. Mecanisme interne de soluționare a plângerilor.....	56
23. Actualizarea regulilor unei organizații privind protecția datelor cu caracter personal și a vieții private.....	57
24. Acțiuni în situația în care legislația locală riscă să împiedice respectarea regulilor organizației privind protecția datelor cu caracter personal și a vieții private și în cazul cererilor de acces formulate de autoritățile de aplicare a legii.....	59
25. Asistența reciprocă și cooperarea cu APD naționale din UE/PEA ale APEC.....	61
26. Relația dintre legislația locală și regulile unei organizații privind protecția datelor cu caracter personal și a vieții private	62
27. Dispoziții finale	64
Apendice	65
Apendicele 1: Documentația care trebuie furnizată de o organizație care dorește aprobarea BCR proprii de către APD naționale din UE și de o organizație care dorește certificarea CBPR proprii de către agenții delegați ai APEC	66

Introducere

Prezentul document (denumit în continuare „referențial”) identifică cerințele comune sau similare pentru regulile corporatiste obligatorii (denumite în continuare „BCR”), astfel cum sunt autorizate de obicei de către autoritățile naționale de protecție a datelor din Uniunea Europeană (denumită în continuare „UE”) pentru transferurile de date cu caracter personal în afara UE, însă în cadrul unui grup corporatist, precum și pentru sistemul de reguli transfrontaliere privind protecția vieții private (denumit în continuare „CBPR”) al Organizației de Cooperare Economică Asia-Pacific (denumită în continuare „APEC”).

De asemenea, referențialul identifică elementele suplimentare necesare pentru aprobarea BCR și certificarea CBPR în cadrul procesului de autorizare și de evaluare a conformității desfășurat atât de autoritățile naționale de protecție a datelor din UE (denumite în continuare „APD”), cât și de agenții cu responsabilități în materie de CBPR recunoscuți de APEC. Referențialul nu aduce atingere aprobării individuale a BCR de către APD naționale în conformitate cu legislația UE în materie de protecție a datelor, nici certificării CBPR de către agenții cu responsabilități în materie de CBPR recunoscuți de APEC (denumiți în continuare „agenți ai APEC cu responsabilități în materie de CBPR”). De asemenea, acesta nu aduce atingere aplicării legii de către autoritățile relevante de supraveghere și/sau de aplicare a legii.

Referențialul nu reprezintă neapărat o analiză cuprinzătoare a tuturor elementelor BCR și CBPR și nici unica modalitate de a prezenta cele două sisteme. Acesta nu ar trebui să fie considerat ca oferind consultanță juridică și nici ca o reflectare a poziției oficiale a vreuneia dintre organizațiile care au participat la elaborarea sa.

Scop și structură

Prezentul referențial își propune să faciliteze punerea în aplicare a normelor privind protecția datelor cu caracter personal și a vieții private de către organizații cu scopul de a sprijini respectarea cerințelor privind BCR și CBPR. Acesta urmărește să servească drept listă de verificare pragmatică pentru organizațiile care doresc să elaboreze și să pună în aplicare politici în materie de protecție a vieții private cu scopul de a solicita în același timp autorizarea unor BCR de către APD naționale din UE și certificarea unor CBPR de către un agent al APEC cu responsabilități în materie de CBPR.

Referențialul se dorește a fi un instrument comparativ util organizațiilor care au în vedere solicitarea aprobării BCR de către APD naționale din UE și a certificării CBPR de către un agent al APEC cu responsabilități în materie de CBPR, și anume, o dublă certificare. Acesta oferă o comparație a cerințelor pentru BCR și CBPR într-un document unic, pentru a facilita formularea de către o organizație a regulilor privind protecția datelor cu caracter personal și a vieții private în vederea îndeplinirii cerințelor ambelor sisteme, precum și punerea în aplicare a acestor reguli privind protecția datelor cu caracter personal și a vieții private în cadrul entităților, al filialelor și al întreprinderilor sale afiliate (denumite în continuare „grupul”). Stabilirea oficială a conformității cu oricare dintre cele două sisteme poate fi realizată numai prin procesele corespunzătoare recunoscute aplicabile în cadrul fiecărui sistem, în concordanță cu cerințele stabilite de cadrul aplicabil.

Referențialul are următoarea structură: pentru fiecare cerință identificată, există un bloc de elemente comune sau similare necesare atât pentru BCR, cât și pentru CBPR. Urmează în continuare blocuri suplimentare pentru fiecare cerință privind BCR și CBPR, cuprinzând elemente care sunt diferite în cele două sisteme. Blocurile suplimentare pot include, de asemenea, derogări și clarificări referitoare la cerințele din cele două sisteme. Deși blocurile comune arată că există puncte comune între cerințele din sistemul CBPR și cele din sistemul BCR, acestea nu sunt suficiente în sine pentru a obține certificarea unor CBPR de către un agent al APEC cu responsabilități în materie de CBPR, nici autorizarea unor BCR de către o APD națională din UE. În plus, elementele cuprinse în blocul suplimentar al BCR trebuie să fie luate în considerare, de asemenea, de către o organizație care solicită aprobarea BCR proprii de către APD naționale din UE, iar elementele enumerate în blocul suplimentar al CBPR trebuie să fie luate în considerare, de asemenea, de către o organizație care solicită certificarea CBPR proprii de către un agent al APEC cu responsabilități în materie de CBPR.

Trebuie remarcat faptul că pot exista diferențe semnificative între cerințele impuse în general de către APD naționale din UE pentru autorizarea BCR, în special cele provenite din legislația UE privind protecția datelor, și cerințele programului CBPR. De asemenea, există diferențe între obiectivele, domeniile de aplicare și procesele de examinare ale sistemelor BCR și CBPR. Ca urmare a diferențelor, unele cerințe privind BCR și CBPR nu sunt pe deplin compatibile. Prin urmare, pentru a se evita orice conflict cu legislația aplicabilă, organizațiile solicitante trebuie să precizeze cu exactitate domeniul de aplicare al regulilor proprii privind protecția datelor cu caracter personal și a vieții private. În cererea lor, acestea trebuie să menționeze clar cazurile în care aplică legislația UE privind protecția datelor și/sau cerințele programului CBPR al APEC, întrucât datele cu caracter personal trebuie să fie prelucrate în conformitate cu cerințele corespunzătoare ale legislației UE privind protecția datelor și/sau cu legislația economiilor APEC.

Regulile unei organizații în materie de protecție a datelor cu caracter personal și a vieții private ar trebui să fie elaborate astfel încât să reflecte structura grupului în cadrul căruia acestea sunt aplicate, modul de prelucrare a datelor de către grup, precum și politicile și procedurile existente de protecție a datelor cu caracter personal. Prin urmare, organizațiile ar trebui să țină cont de faptul că APD naționale din UE și agenții APEC cu responsabilități în materie de CBPR nu vor accepta o simplă transcriere a acestui cadru.

Domeniu de aplicare

Certificarea CBPR este limitată la organizațiile certificate într-o economie care participă la sistemul CBPR. Domeniul de aplicare al certificării CBPR a unei anumite organizații este limitat la entitățile, filialele și întreprinderile afiliate ale acesteia identificate în cererea sa de certificare a CBPR.

Orice organizație care dorește să transfere date cu caracter personal din statele membre ale UE către destinatari aflați în țări din afara UE poate depune o cerere la o APD națională din UE în vederea aprobării regulilor sale corporatiste obligatorii. Domeniul de aplicare al BCR ale unei anumite organizații este limitat la entitățile, filialele și întreprinderile afiliate ale acesteia identificate în cererea sa de aprobare a BCR. Punerea în aplicare corectă a BCR, odată aprobate,

oferă garanții adecvate pentru transferurile de date din respectivele entități identificate din UE către entități, filiale și întreprinderi afiliate (astfel cum sunt specificate în cererea organizației) din afara UE identificate în același mod.

Regulile privind protecția datelor cu caracter personal și a vieții private aplicabile transferurilor transfrontaliere de date cu caracter personal pot să devină, dacă sunt aprobate în conformitate cu procedurile corespunzătoare, politica organizației sau a grupului pentru toate datele cu caracter personal prelucrate de către organizație sau de către grup, astfel cum este stabilită în urma aprobării BCR ale organizației sau ale grupului de către APD naționale din UE și a certificării CBPR de către agenții APEC cu responsabilități în materie de CBPR. În cazul în care datele cu caracter personal sunt prelucrate³ în UE⁴, se aplică, de asemenea, dispozițiile legislației UE în materie de protecție a datelor. În cazul în care datele cu caracter personal sunt prelucrate în cadrul unei economii APEC, se aplică legislația jurisdicției relevante.

Prezentul referențial se bazează pe următoarele documente:

UE:

- Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, denumită în continuare „**Directiva 95/46**”;
- legislația națională de punere în aplicare a Directivei 95/46/CE;
- *Documentul de lucru: Transferurile de date cu caracter personal către țările terțe: Aplicarea articolului 26 alineatul (2) din Directiva UE privind protecția datelor în cazul regulilor corporatiste obligatorii pentru transferurile internaționale de date (WP74)*, adoptat de Grupul de lucru instituit în temeiul articolului 29 la 3 iunie 2003, denumit în continuare „**WP74**”;
- *Documentul de lucru privind stabilirea unui model de cerere sub formă de listă de verificare pentru aprobarea regulilor corporatiste obligatorii (WP108)*, adoptat de Grupul de lucru instituit în temeiul articolului 29 la 3 iunie 2003, denumit în continuare „**WP108**”;
- *Recomandarea 1/2007 privind cererea-tip pentru aprobarea regulilor corporatiste obligatorii pentru transferul de date cu caracter personal (WP133)*, adoptată de Grupul

³ Conceptul de prelucrare include stocarea, precum și orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal, cum ar fi colectarea, înregistrarea, organizarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea [a se vedea articolul 2 litera (b) din Directiva 95/46/CE].

⁴ Legislația națională a statelor membre ale UE privind protecția datelor se aplică prelucrării datelor cu caracter personal (inclusiv stocarea) în cazul în care: (a) prelucrarea este efectuată în cadrul activităților operatorului cu sediul **pe teritoriul UE**; (c) operatorul **nu este stabilit în UE**, dar în scopul prelucrării datelor cu caracter personal recurge la mijloace automate sau neautomate, situate pe teritoriul UE, cu excepția cazului în care aceste mijloace sunt folosite numai în vederea tranzitului pe teritoriul UE; (b) operatorul nu este stabilit pe teritoriul UE, ci într-un loc în care se aplică dreptul intern al unui stat membru al UE, în temeiul dreptului internațional public [a se vedea articolul 4 alineatul (1) din Directiva 95/46/CE].

de lucru instituit în temeiul articolului 29 la 10 ianuarie 2007, denumită în continuare „**WP133**”;

- *Documentul de lucru privind elaborarea unui tabel cuprinzând elementele și principiile care trebuie să se regăsească în regulile corporatiste obligatorii (WP153), adoptat de Grupul de lucru instituit în temeiul articolului 29 la 24 iunie 2008, denumit în continuare „**WP153**”;*
- *Documentul de lucru privind stabilirea unui cadru pentru structura regulilor corporatiste obligatorii (WP154), adoptat de Grupul de lucru instituit în temeiul articolului 29 la 24 iunie 2008, denumit în continuare „**WP154**”;*
- *Documentul de lucru privind întrebări frecvente (FAQ) referitoare la regulile corporatiste obligatorii (WP155), adoptat de Grupul de lucru instituit în temeiul articolului 29 la 24 iunie 2008, astfel cum a fost revizuit ultima oară și adoptat la 8 aprilie 2009, denumit în continuare „**WP155**”.*

APEC:

- *Cadrul APEC privind protecția vieții private, denumit în continuare „**Cadrul privind protecția vieții private**”;*
- *Sistemul de reguli transfrontaliere, politici, norme și orientări ale APEC privind protecția vieții private, denumit în continuare „**Politici, norme și orientări**”;*
- *Acordul de cooperare al APEC privind aplicarea transfrontalieră a normelor referitoare la protecția vieții private, denumit în continuare „**CPEA**”;*
- *Avizul-tip de notificare a intenției de participare la sistemul APEC de reguli transfrontaliere privind protecția vieții private, denumit în continuare „**Avizul-tip de notificare a intenției de participare**”;*
- *Cererea de recunoaștere a unui agent cu responsabilități în materie de CBPR de către APEC, denumită în continuare „**Cererea de recunoaștere**”;*
- *Chestionarul de admitere în sistemul APEC de reguli transfrontaliere privind protecția vieții private, denumit în continuare „**Chestionarul de admitere**”;*
- *Cerințele programului privind sistemul APEC de reguli transfrontaliere privind protecția vieții private, denumite în continuare „**Cerințele programului**”.*

Referențial privind cerințele pentru BCR și CBPR în materie de protecție a datelor cu caracter personal și a vieții private

1. Obiectivul regulilor unei organizații privind protecția datelor cu caracter personal și a vieții private

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie:

- să asigure un nivel adecvat de protecție pentru transferul și prelucrarea datelor cu caracter personal de către grup, astfel cum se solicită în cadrul proceselor de aprobare a BCR și de certificare a CBPR [5] și
- să reprezinte o obligație executorie a organizației de a asigura conformitatea cu regulile privind protecția datelor cu caracter personal și a vieții private [6] (a se vedea secțiunile 3 și 21 din referențial);
- să conțină trimiteri la legislația în vigoare în domeniul protecției datelor [7].

<p>Elemente suplimentare necesare pentru aprobarea BCR</p> <p>Regulile unei organizații cu privire la protecția datelor cu caracter personal și a vieții private trebuie să conțină obligația clară pentru toți membrii grupului și pentru angajați de a interpreta și a respecta regulile organizației privind protecția datelor cu caracter personal și a vieții private în conformitate cu legislația aplicabilă [8].</p>	<p>Elemente suplimentare necesare pentru certificarea CBPR</p> <p>În cazul în care cerințele legale interne depășesc cerințele presupuse de sistemul CBPR, legislația și reglementările interne respective vor continua să se aplice integral.</p> <p>În cazul în care cerințele sistemului CBPR depășesc cerințele prevăzute în legislația și reglementările interne, organizațiile vor trebui să îndeplinească benevol cerințele suplimentare pentru a putea participa. Cu toate acestea, autoritățile însărcinate cu aplicarea normelor de protecție a vieții private din economia respectivă ar trebui să aibă capacitatea de a întreprinde acțiuni de punere în aplicare în temeiul legilor și reglementărilor interne aplicabile, cu scopul de a proteja informațiile cu caracter personal în conformitate cu cerințele programului CBPR [9] (<i>a se vedea, de asemenea, 26 – Relația dintre legislația locală și regulile organizației privind protecția datelor cu caracter personal și a vieții private</i>).</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

- [5] UE: a se vedea WP74, punctul 3.1, pp. 7-9; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul I, 14, p. 11.
- [6] UE: a se vedea WP154, Introducere, p. 3 și WP74 p. 10-14; APEC: a se vedea Politici, norme și orientări privind CBPR, 8, p.4; Cerințele programului CBPR 39, p. 40.
- [7] UE: a se vedea WP154, Introducere, p. 3; APEC: a se vedea Cererea de recunoaștere, Anexa A, 4, p. 5.
- [8] UE: a se vedea WP74, punctul 3.3.1, pp. 10-11; WP153, punctul 1.1, p. 3.
- [9] APEC: a se vedea Politici, norme și orientări, 44, p. 10

2. Domeniul de aplicare al regulilor unei organizații privind protecția datelor cu caracter personal și a vieții private

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină descrierea domeniului de aplicare al acestora, inclusiv:

- domeniul de aplicare geografic (a se vedea secțiunile 4 și 15 din prezentul referențial) [10];
- domeniul de aplicare material (și anume natura datelor, clienți/potențiali clienți, angajați/potențiali angajați, furnizori etc.) [11];
- lista entităților care au obligația să respecte regulile organizației privind protecția datelor cu caracter personal și a vieții private [12] și
- scopurile transferului și/sau ale prelucrării [13].

<p>Elemente suplimentare necesare pentru aprobarea BCR</p> <p>Prelucrarea datelor cu caracter personal care sunt disponibile public face obiectul cerințelor din legislația UE privind protecția datelor și nu este exceptată de la BCR.</p> <p>Organizațiile care aleg să participe la sistemul BCR ar trebui să pună în aplicare politici și practici privind protecția vieții private conforme cu cerințele programului BCR pentru toate datele cu caracter personal care sunt transferate în cadrul grupului către destinatari aflați în afara Uniunii Europene. Deși nu este necesar pentru aprobarea BCR, organizațiile participante pot aplica aceleași politici și proceduri privind protecția vieții private tuturor datelor cu caracter personal care sunt prelucrate în cadrul grupului la nivel mondial, cu condiția să se asigure respectarea legislației UE privind protecția datelor, în cazul în care datele cu caracter personal sunt prelucrate în UE.</p>	<p>Elemente suplimentare necesare pentru certificarea CBPR</p> <p>N/A</p>
<p>Clarificarea domeniului de aplicare al BCR</p> <p>N/A</p>	<p>Clarificarea domeniului de aplicare al CBPR</p> <p>În unele situații, este posibil ca regulile organizației privind protecția datelor cu caracter personal și a vieții private să nu se aplice informațiilor disponibile public [14].</p> <p>Organizațiile care aleg să participe la sistemul</p>

	<p>CBPR ar trebui să pună în aplicare politici și practici privind protecția vieții private conforme cu cerințele programului CBPR pentru toate informațiile cu caracter personal pe care le-au colectat sau le-au primit și care fac obiectul transferului transfrontalier către alte economii APEC participante. Deși nu este o cerință a sistemului CBPR, organizațiile participante sunt încurajate să aplice aceleași politici și proceduri privind protecția vieții private tuturor informațiilor cu caracter personal pe care le-au colectat sau le-au primit, chiar dacă acestea nu fac obiectul transferului transfrontalier sau dacă fac obiectul unui astfel de transfer numai în afara teritoriului economiilor APEC participante [15].</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

- [10] UE: a se vedea WP153, punctul 4.2 și WP108, punctele 7.1 și 7.2, pp. 7-8; APEC: a se vedea Chestionarul de admitere, v-vi, pp. 2-3.
- [11] UE: a se vedea WP153, punctul 4.2 și WP108, punctele 7.1.1 și 7.2, pp. 7-8; APEC: a se vedea Chestionarul de admitere, iv, p. 2.
- [12] UE: a se vedea WP153 punctul 6.2; WP108, punctul 7.1.3, p. 8; APEC: a se vedea Chestionarul de admitere, ii, p. 2.
- [13] UE: a se vedea WP153 punctul 4.1; WP108, punctul 7.1.2, p. 8; APEC: a se vedea Cerințele programului CBPR 1(b) și 1(c).
- [14] APEC: a se vedea Cadrul APEC privind protecția vieții private, 11, p. 7.
- [15] APEC: a se vedea Politici, norme și orientări, 8, p. 4.

3. Obligație executorie în cadrul unei organizații

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Toate entitățile grupului care doresc aprobarea unor BCR de către o APD națională din UE sau certificarea unor CBPR de către un agent al APEC cu responsabilități în materie de CBPR trebuie să aibă o obligație executorie de respectare a regulilor organizației privind protecția datelor cu caracter personal și a vieții private în temeiul legislației aplicabile care poate fi pusă în aplicare de către individ/persoana vizată și autoritatea de reglementare astfel cum este adecvat [16].

Elemente suplimentare necesare pentru aprobarea BCR: obligativitatea în cadrul unui grup (BCR)	Elemente suplimentare necesare pentru certificarea CBPR
<p>Regulile organizației privind protecția datelor cu caracter personal și a vieții private trebuie să devină obligatorii din punct de vedere juridic între entitățile grupului prin unul sau mai multe dintre instrumentele următoare [17]:</p> <ul style="list-style-type: none">(i) măsuri sau reguli obligatorii din punct de vedere juridic pentru toți membrii grupului;(ii) contracte între membrii grupului;(iii) declarații sau angajamente unilaterale ale întreprinderii-mamă, care sunt obligatorii pentru ceilalți membri ai grupului [18];(iii) includerea altor măsuri de reglementare, de exemplu, obligații cuprinse în coduri statutare într-un cadru juridic definit;iv) încorporarea regulilor organizației privind protecția datelor cu caracter personal și a vieții private în principiile comerciale generale ale unei organizații, cu sprijinul unor politici, acțiuni de audit și sancțiuni corespunzătoare;(v) alte mijloace [19]. <p>De asemenea, regulile organizației privind protecția datelor cu caracter personal și a vieții private trebuie să devină obligatorii pentru angajați, prin unul sau mai multe dintre instrumentele următoare [20]:</p>	N/A

<p>(i) acord/angajament individual și separat, cu sancțiuni;</p> <p>(ii) clauză în contractul de muncă, cu sancțiuni;</p> <p>(iii) politici interne cu sancțiuni;</p> <p>(iv) acorduri colective cu sancțiuni.</p>	
<p>Clarificarea obligativității pentru o organizație (BCR)</p> <p>N/A</p>	<p>Clarificarea răspunderii unei organizații (CBPR)</p> <p>Organizația trebuie să-și mențină răspunderea demonstrând caracterul executoriu al regulilor sale privind protecția datelor cu caracter personal și a vieții private prin unul sau mai multe dintre următoarele instrumente [21]:</p> <ul style="list-style-type: none"> (i) orientări sau politici interne; (ii) contracte; (iii) conformitatea cu legile și reglementările aplicabile în industria sau sectorul respectiv; (iv) alte mijloace. <p>De asemenea, organizația trebuie să dispună de proceduri pentru formarea angajaților cu privire la regulile sale privind protecția datelor cu caracter personal și a vieții private [22].</p>

Referințe

- [16] UE: a se vedea WP153 punctele 1.1 și 1.2; WP74, punctul 3.3.1, pp. 10-11; APEC: a se vedea Cerințele programului, Q39, p. 24; anexele A și B;
- [17] UE: a se vedea WP153, punctul 1.2.i, p.3; WP108, punctul 5.6, p. 5;
- [18] Trebuie să se menționeze faptul că în unele state membre ale UE este posibil ca simplele declarații unilaterale să nu fie considerate obligatorii din punct de vedere juridic în temeiul dreptului civil și administrativ. În acest caz, numai contractele sunt considerate obligatorii. Prin urmare, o organizație ar trebui să recurgă la consiliere juridică locală în cazul în care intenționează să se bazeze pe alte mijloace legale decât contractele;
- [19] UE: WP74, punctul 3.3.1, pp. 10-11, WP153, punctul 1.1, p. 3;
- [20] EU: a se vedea WP74, punctul 3.3.1, pp. 10-11; WP153, punctul 1.1, p. 3 și punctul 1.2.ii, p. 3;
- [21] APEC: a se vedea Cerințele programului, Q39, p. 24; Q46, p. 26; anexele A și B;
- [22] APEC: a se vedea Cerințele programului, Q44, pp. 25-26.

4. Măsuri reparatorii pentru drepturile persoanelor vizate și ale beneficiarilor terți

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

N/A

Elemente necesare pentru aprobarea BCR	Elemente necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să ofere persoanelor vizate dreptul de a obține aplicarea regulilor organizației privind protecția datelor cu caracter personal și a vieții private în calitate de beneficiari terți. Regulile trebuie să precizeze căile de atac în justiție clare, accesibile și eficiente pentru orice încălcare a regulilor privind protecția datelor cu caracter personal și a vieții private, precum și dreptul de a obține reparații (a se vedea articolele 22 și 23 din Directiva 95/46/CE) [23].</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă, de asemenea, că persoanele vizate au dreptul de a alege oricare dintre următoarele căi pentru a face o reclamație:</p> <ul style="list-style-type: none">- instanțele competente asupra exportatorului de date stabilit în UE sau- instanțele competente pentru sediul din UE/membrul UE cu responsabilități delegate sau- APD naționale competente din UE. <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, garanția că toate persoanele vizate care dețin drepturi de beneficiari terți au, de asemenea, acces facil la această clauză [24].</p>	<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă că persoanele vizate pot să obțină aplicarea acestora prin:</p> <ul style="list-style-type: none">- procedura operatorului de soluționare a plângerilor [25] sau- procedura de soluționare a litigiilor a agentului APEC cu responsabilități în materie de CBPR [26]. <p>De asemenea, persoanele vizate trebuie să aibă posibilitatea de a depune o plângere împotriva unui agent al APEC cu responsabilități în materie de CBPR în mod direct la Grupul comun de supraveghere [27].</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, prevederea că persoanele vizate pot depune o plângere la agenții APEC cu responsabilități în materie de CBPR [28].</p> <p>În funcție de economiile participante la sistemul CBPR, persoanele vizate pot avea un drept privat de a acționa în temeiul legilor naționale privind confidențialitatea datelor, care poate fi utilizat pentru a asigura respectarea CBPR.</p>

Referințe

[23] UE: a se vedea WP74, punctul 3.3.2, pp. 11-13.

[24] UE: a se vedea WP153, punctul 1.7, p. 5.

[25] APEC: a se vedea Chestionarul de admitere, Q41-43, pp. 21-22.

[26] APEC: a se vedea Cererea de recunoaștere, anexa A, 9-10, p. 7.

[27] APEC: a se vedea Politici, norme și orientări, 35, p. 9.

[28] APEC: a se vedea Cererea de recunoaștere, anexa A, 9-10, p. 7.

5. Răspunderea

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă, în principiu, că răspunderea revine unei singure entități [29].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, următoarele angajamente [30]:</p> <ul style="list-style-type: none">- Sediul din UE sau membrul din UE căruia i s-au delegat responsabilități acceptă răspunderea pentru actele altor membri ai grupului din afara UE și este de acord să ia măsurile necesare pentru a remedia actele respective și să plătească reparații pentru eventualele prejudicii rezultate din încălcarea, de către membrii grupului, a regulilor organizației privind protecția datelor cu caracter personal și a vieții private.- Sarcina probei îi revine fie sediului din UE, fie membrului din UE căruia i s-au delegat responsabilități, pentru a demonstra că membrul din afara UE nu este răspunzător de încălcarea care a provocat prejudiciile invocate de către persoana vizată. <p>Dacă sediul din UE sau membrul din UE căruia i s-au delegat responsabilități poate dovedi că membrul din afara UE nu este răspunzător de încălcare, aceasta poate fi exonerat de răspundere.</p> <p>În cazul în care, pentru anumite grupuri cu structuri corporatiste deosebite, nu este posibil ca unei entități specifice să i se impună să-și asume întreaga răspundere pentru orice încălcare a BCR în afara UE, APD naționale din UE pot accepta alte mecanisme de răspundere, de la caz la caz, dacă se oferă suficiente garanții că drepturile</p>	<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă, de asemenea, că răspunderea îi revine entității ale cărei CBPR sunt certificate. Cu toate acestea, aceasta nu exclude eventuala răspundere suplimentară a filialelor/întreprinderilor afiliate în temeiul legilor statului în care s-a produs încălcarea.</p>

persoanelor vizate vor fi aplicabile și că acestea nu vor fi defavorizate în ceea ce privește exercitarea lor [31].	
---------------------------------------------------------------------------------------------------------------------	--

Referințe

[29] UE: a se vedea WP74, punctul 5.5.2, pp. 18-19; APEC: a se vedea Chestionarul de admitere, ii, p. 2.

[30] UE: a se vedea WP74, punctul 5.5.2, pp. 18-19.

[31] Printre mecanismele de răspundere posibile se numără mecanismul răspunderii solidare a importatorilor și exportatorilor de date, conform Clauzelor contractuale standard ale UE 2001/497/CE din 15 iunie 2001, sau stabilirea unui mecanism de răspundere alternativ, bazat pe obligații de diligență, astfel cum se prevede în Clauzele contractuale standard 2004/915/CE din 27 decembrie 2004. O ultimă posibilitate, rezervată în mod specific transferurilor efectuate de către operatori către persoanele împuternicite de către operatori, este aplicarea mecanismului de răspundere din Clauzele contractuale standard 2002/16/CE din 27 decembrie 2001.

6. Obligații executorii privind transferurile către terți

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină o obligație executorie conform căreia organizația transferă date numai terților care aplică măsuri de protecție prelucrării datelor cu caracter personal, precum și explicații cu privire la modul în care regulile organizației privind protecția datelor cu caracter personal și a vieții private devin executorii pentru astfel de destinatari ai datelor în jurisdicția relevantă [32].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină reguli privind restricționarea transferurilor și a transferurilor ulterioare de date în afara grupului, precum și obligația de a se asigura faptul că [33]:</p> <ul style="list-style-type: none">- persoanele externe împuternicite de către operatori aflate în UE sau într-o țară recunoscută de către Comisia Europeană ca asigurând un nivel adecvat de protecție trebuie să fi încheiat un acord scris care stipulează că persoana împuternicită de către operator acționează numai pe baza instrucțiunilor primite de la operator și este răspunzătoare de punerea în aplicare a măsurilor corespunzătoare de securitate și confidențialitate;- toate transferurile de date către operatorii externi aflați în afara UE și nu într-o țară recunoscută de Comisia Europeană ca asigurând un nivel adecvat de protecție trebuie să respecte normele europene privind fluxurile de date transfrontaliere (articolele 25-26 din Directiva 95/46/CE: de exemplu, utilizarea Clauzelor contractuale standard ale UE 2001/497/CE sau 2004/915/CE ale UE, aprobate de către Comisie, sau prin alte mijloace contractuale adecvate în conformitate cu articolele 25 și 26 din directiva UE);	N/A

<p>- toate transferurile de date către persoane externe împuternicite de către operator aflate în afara UE trebuie să respecte normele referitoare la persoanele împuternicite de către operatori (articolele 16-17 din Directiva 95/45/CE), pe lângă regulile privind fluxurile transfrontaliere de date (articolele 25-26 din Directiva 95/46/CE).</p>	
<p>Clarificarea obligativității pentru terți (BCR)</p> <p>N/A</p>	<p>Clarificarea răspunderii cu privire la transferurile către terți (CBPR)</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină explicații cu privire la modul în care datele cu caracter personal sunt protejate atunci când se utilizează o persoană împuternicită de operator, un agent, un contractant sau un alt prestator de servicii. În special se solicită următoarele:</p> <ul style="list-style-type: none"> - operatorul trebuie să aleagă o persoană împuternicită, un agent, un contractant sau un alt prestator de servicii care oferă garanții suficiente în ceea ce privește măsurile tehnice de securitate și măsurile organizatorice aplicate prelucrării care urmează să fie efectuată și trebuie să asigure respectarea măsurilor respective [34]; - operatorul trebuie să însărcineze persoana împuternicită să se asigure, în special, că: <ul style="list-style-type: none"> (i) persoana împuternicită de către operator, agentul, contractantul sau un alt prestator de servicii trebuie să acționeze numai conform instrucțiunilor primite de la operator [35]; (ii) regulile referitoare la securitate și confidențialitate reprezintă o obligație pentru persoana împuternicită de către operator,

	<p>agent, contractant sau un alt prestator de servicii [36].</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private pot dobândi caracter obligatoriu prin unul sau mai multe dintre instrumentele următoare [37]:</p> <ul style="list-style-type: none"> (i) orientări sau politici interne; (ii) contracte; (iii) conformitatea cu legile și reglementările aplicabile în industria sau sectorul relevant. (iv) alte mijloace.
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

[32] UE: a se vedea WP74, punctul 3.2, pp. 9-10; APEC: a se vedea Cerințele programului, Q39, p. 24; Q46, p. 26; anexele A și B; Chestionarul de admitere, Q47, p. 22.

[33] UE: a se vedea WP153, punctul 6.1 (vi); WP154, punctul 12, p. 7.

[34] APEC: a se vedea Chestionarul de admitere, Q35, p. 15.

[35] APEC: a se vedea Chestionarul de admitere, Q47-48, pp. 22-23.

[36] APEC: a se vedea Chestionarul de admitere, Q35, pp. 15-16.

[37] APEC: a se vedea Cerințele programului, Q39, p. 24; Q46, p. 26; anexele A și B.

7. Relații cu persoane împuternicite de către operator care sunt membri ai grupului

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină explicații cu privire la modul în care datele cu caracter personal sunt protejate atunci când se utilizează o persoană împuternicită de către operator care este membră a grupului și, în special, următoarele cerințe [38]:

- operatorul trebuie să aleagă o persoană împuternicită care oferă garanții suficiente în ceea ce privește măsurile tehnice de securitate și măsurile organizatorice aplicate prelucrării care urmează să fie efectuată și trebuie să asigure respectarea măsurilor respective [39];
- operatorul trebuie să însărcineze persoana împuternicită să se asigure, în special, că:
 - persoana împuternicită de către operator acționează numai conform instrucțiunilor primite de la operator [40];
 - regulile referitoare la securitate și confidențialitate reprezintă o obligație pentru persoana împuternicită de către operator [41].

<p>Elemente suplimentare necesare pentru aprobarea BCR</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă faptul că instrucțiunile trebuie să fie transmise numai prin mijloace contractuale scrise, în conformitate cu legislația aplicabilă [42].</p>	<p>Elemente suplimentare necesare pentru certificarea CBPR</p> <p>În cazul în care operatorul intenționează să transfere date cu caracter personal către persoane împuternicite de către operator, agenți, contractanți sau alți prestatori de servicii, acesta ar trebui să obțină consimțământul persoanei vizate sau să îndeplinească obligațiile de diligență și ar trebui să ia măsuri rezonabile pentru a se asigura că persoana sau organizația destinatară va proteja datele într-un mod conform cu regulile organizației privind protecția datelor cu caracter personal și a vieții private [43].</p> <p>În situațiile în care obligațiile de diligență și măsurile rezonabile necesare pentru a asigura respectarea regulilor organizației privind protecția datelor cu caracter personal și a vieții private sunt nepractice sau imposibile, operatorul trebuie să ofere explicații și să descrie celelalte mijloace folosite pentru a se asigura că datele sunt protejate totuși în conformitate cu principiile APEC privind</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>protecția vieții private.</p> <p>Instrucțiunile pot fi furnizate de către operator prin [44]:</p> <ul style="list-style-type: none"> - orientări sau politici interne sau - contracte sau - respectarea legilor și reglementărilor aplicabile în industria sau sectorul respectiv sau - respectarea codului și/sau a normelor de autoreglementare ale organizației sau - alte mijloace. <p>Astfel de acorduri necesită, în general, ca persoanele împuternicite de către operator pentru a prelucra date cu caracter personal, agenții, contractanții sau alți prestatori de servicii [45] să adopte măsuri de protecție adecvate dintre următoarele opțiuni:</p> <ul style="list-style-type: none"> - respectă politicile și practicile operatorului cu privire la protecția vieții private, care sunt în conformitate cu normele APEC, astfel cum se precizează în declarația de confidențialitate a operatorului; - pun în aplicare practici privind protecția vieții private care sunt, în mare măsură, similare cu politicile sau practicile operatorului cu privire la protecția vieții private, astfel cum se precizează în declarația de confidențialitate a operatorului; - respectă instrucțiunile furnizate de operator cu privire la modul în care trebuie să fie tratate datele cu caracter personal ale operatorului; - impun restricții privind subcontractarea, cu excepția cazului în care operatorul și-a dat consimțământul; - obțin certificarea CBPR de către un agent al APEC cu responsabilități în materie de CBPR din jurisdicția lor;
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Persoanele împuternicite de către operator, agenții, contractanții sau alți prestatori de servicii trebuie să informeze operatorul atunci când li se aduce la cunoștință o încălcare a confidențialității sau a securității datelor cu caracter personal ale operatorului [46].</p> <p>Persoanele împuternicite de către operator, agenții, contractanții sau alți prestatori de servicii trebuie să ia, fără întârziere, măsuri pentru a rectifica/a soluționa deficiența de securitate care a provocat încălcarea confidențialității sau a securității [47].</p> <p>Persoanele împuternicite de către operator, agenții, contractanții sau alți prestatori de servicii trebuie să ofere operatorului autoevaluări pentru a asigura conformitatea cu instrucțiunile operatorului și/sau cu acordurile/contractele încheiate cu acesta [48].</p> <p>Operatorul trebuie să efectueze periodic verificări la fața locului sau monitorizări vizând persoanele împuternicite de acesta în vederea prelucrării de date cu caracter personal, agenții, contractanții sau alți prestatori de servicii, pentru a asigura conformitatea cu instrucțiunile sale și cu acordurile/contractele pe care le-a încheiat [49].</p>
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

- [38] UE: a se vedea Directiva 95/46, articolul 17 alineatul (2); WP154, punctul 11, pp. 6-7.
- [39] APEC: a se vedea Chestionarul de admitere, Q35, p. 15.
- [40] APEC: a se vedea Chestionarul de admitere, Q47-48, pp. 22-23.
- [41] APEC: a se vedea Chestionarul de admitere, Q35, pp. 15-16.
- [42] UE: a se vedea Directiva 95/46, articolul 17 alineatul (2); WP154, punctul 11, pp. 6-7.
- [43] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul IX, 26, p. 28.
- [44] APEC: a se vedea Chestionarul de admitere, Q46, p. 22.
- [45] APEC: a se vedea Chestionarul de admitere, Q47, pp. 22-23.
- [46] APEC: a se vedea Chestionarul de admitere, Q35-b), p. 15.
- [47] APEC: a se vedea Chestionarul de admitere, Q35-c), p. 16.
- [48] APEC: a se vedea Chestionarul de admitere, Q48, p. 23.
- [49] APEC: a se vedea Chestionarul de admitere, Q49, p. 23.

8. Restricții privind transferurile și transferurile ulterioare către persoanele externe împuternicite de operator și către operatorii externi (care nu sunt membri ai grupului)

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină următoarea cerință: contractanții care primesc datele și le prelucrează trebuie să protejeze datele cu caracter personal în conformitate cu regulile organizației-sursă privind protecția datelor cu caracter personal și a vieții private [50].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, explicații cu privire la măsurile instituite pentru a restricționa transferurile și transferurile ulterioare în afara grupului, precum și obligația de a se asigura faptul că:</p> <ul style="list-style-type: none">- persoanele externe împuternicite de către operatori aflate în UE sau într-o țară recunoscută de către Comisia Europeană ca asigurând un nivel adecvat de protecție trebuie să fi încheiat un acord scris care stipulează că persoana împuternicită de către operator acționează numai pe baza instrucțiunilor primite de la operator și este răspunzătoare de punerea în aplicare a măsurilor corespunzătoare de securitate și confidențialitate [51];- toate transferurile de date către operatorii externi aflați în afara UE și nu într-o țară recunoscută de către Comisia Europeană ca asigurând un nivel adecvat de protecție trebuie să respecte normele europene privind fluxurile de date transfrontaliere (articolele 25-26 din Directiva 95/46/CE: de exemplu, utilizarea Clauzelor contractuale standard 2001/497/CE sau 2004/915/CE ale UE, aprobate de către Comisie, sau prin alte mijloace contractuale adecvate, în conformitate cu articolele 25 și 26 din	<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină explicații cu privire la modul în care datele cu caracter personal sunt protejate atunci când se utilizează o persoană împuternicită de operator, un agent, un contractant sau un alt prestator de servicii. În special, se solicită următoarele:</p> <ul style="list-style-type: none">- operatorul trebuie să aleagă o persoană împuternicită, un agent, un contractant sau un alt prestator de servicii care oferă garanții suficiente în ceea ce privește măsurile tehnice de securitate și măsurile organizatorice aplicate prelucrării care urmează să fie efectuată și trebuie să asigure respectarea măsurilor respective [54];- operatorul trebuie să însărcineze persoana împuternicită, agentul, contractantul sau un alt prestator de servicii să se asigure, în special, că:<ul style="list-style-type: none">(i) acționează numai conform instrucțiunilor primite de la operator [55];(ii) respectă regulile referitoare la securitate și confidențialitate, care reprezintă o obligație pentru persoana împuternicită de către operator, agent, contractant sau un alt prestator de servicii [56].

<p>directiva UE) [52];</p> <p>- toate transferurile de date către persoane externe împuternicite de către operator aflate în afara UE trebuie să respecte normele referitoare la persoanele împuternicite de către operatori (articolele 16-17 din Directiva 95/45/CE), pe lângă regulile privind fluxurile transfrontaliere de date (articolele 25-26 din Directiva 95/46/CE) [53].</p>	<p>Instrucțiunile pot fi furnizate de operator prin următoarele mijloace [57]:</p> <ul style="list-style-type: none"> - orientări sau politici interne sau - contracte sau - respectarea legilor și reglementărilor aplicabile industriei sau sectorului respectiv sau - respectarea codului și/sau a normelor de autoreglementare ale organizației sau - alte mijloace. <p>Astfel de acorduri necesită, în general, ca persoanele împuternicite de către operator pentru a prelucra date cu caracter personal, agenții, contractanții sau alți furnizori de servicii să adopte măsuri de protecție adecvate dintre următoarele opțiuni [58]:</p> <ul style="list-style-type: none"> - respectă politicile și practicile operatorului cu privire la protecția vieții private, care sunt în conformitate cu normele APEC, astfel cum se precizează în declarația de confidențialitate a operatorului; - pun în aplicare practici privind protecția vieții private care sunt, în mare măsură, similare cu politicile sau practicile operatorului cu privire la protecția vieții private, astfel cum se precizează în declarația de confidențialitate a operatorului; - respectă instrucțiunile furnizate de operator cu privire la modul în care trebuie să fie tratate datele cu caracter personal ale operatorului; - impun restricții privind subcontractarea, cu excepția cazului în care operatorul și-a dat consimțământul; - obțin certificarea CBPR de către un agent al APEC cu responsabilități în materie de CBPR din jurisdicția lor; - alte mijloace.
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>Persoanele împuternicite de către operator, agenții, contractanții sau alți prestatori de servicii trebuie să informeze operatorul atunci când li se aduce la cunoștință o încălcare a confidențialității sau a securității datelor cu caracter personal ale operatorului [59].</p> <p>Persoanele împuternicite de către operator, agenții, contractanții sau alți prestatori de servicii trebuie să ia, fără întârziere, măsuri pentru a rectifica/soluționa deficiența de securitate care a provocat încălcarea confidențialității sau a securității [60].</p> <p>Persoanele împuternicite de către operator, agenții, contractanții sau alți prestatori de servicii trebuie să ofere operatorului autoevaluări pentru a asigura conformitatea cu instrucțiunile operatorului și/sau cu acordurile/contractele încheiate cu acesta [61].</p> <p>Operatorul trebuie să efectueze periodic verificări la fața locului sau monitorizări vizând persoanele împuternicite de acesta în vederea prelucrării de date cu caracter personal, agenții, contractanții sau alți prestatori de servicii, pentru a asigura conformitatea cu instrucțiunile sale și/sau cu acordurile/contractele pe care le-a încheiat [62].</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

- [50] UE: a se vedea WP74, punctul 3.2, pp. 9-10; APEC: a se vedea Chestionarul de admitere, Q47, p. 22.
- [51] UE: a se vedea Directiva 95/46, articolul 17 alineatul (2); WP154, punctul 12, p. 7.
- [52] UE: a se vedea WP74, punctul 3.2, pp. 9-10.
- [53] UE: a se vedea WP154, punctul 12, p. 7.
- [54] APEC: a se vedea Chestionarul de admitere, Q35, p. 15.
- [55] APEC: a se vedea Chestionarul de admitere, Q47-48, pp. 22-23.
- [56] APEC: a se vedea Chestionarul de admitere, Q35, pp. 15-16.
- [57] APEC: a se vedea Chestionarul de admitere, Q46, p. 22.
- [58] APEC: a se vedea Chestionarul de admitere, Q47, pp. 22-23.
- [59] APEC: a se vedea Chestionarul de admitere, Q35-b), p. 15.
- [60] APEC: a se vedea Chestionarul de admitere, Q35-c), p. 16.
- [61] APEC: a se vedea Chestionarul de admitere, Q48, p. 23.
- [62] APEC: a se vedea Chestionarul de admitere, Q49, p. 23.

9. Definiții

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

O organizație trebuie să interpreteze termenii din regulile sale privind protecția datelor cu caracter personal și a vieții private în conformitate cu legislația aplicabilă a UE, în special Directiva 95/46/CE și Directiva 2002/58/CE, cu legile aplicabile în economiile participante la sistemul CBPR și cu glosarul privind CBPR al APEC [63].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină angajamentul de a interpreta termenii în conformitate cu legislația aplicabilă a UE, în special Directiva 95/46/CE și Directiva 2002/58/CE, precum și o descriere a principalilor termeni și definițiile acestora: date cu caracter personal [64]; operator [65]; persoană împuternicită de către operator [66]; persoane vizate [67]; date cu caracter personal sensibile [68]; prelucrare [69]; terț [70] și autoritățile UE pentru protecția datelor [71].	N/A

Referințe

[63] UE: a se vedea WP154, punctul 2, p. 4; WP155 Q8, p.5; APEC: a se vedea glosarul privind CBPR.

[64] UE: a se vedea Directiva 95/46, articolul 2 litera (a).

[65] UE: a se vedea Directiva 95/46, articolul 2 litera (d).

[66] UE: a se vedea Directiva 95/46, articolul 2 litera (e).

[67] UE: a se vedea Directiva 95/46, articolul 2 litera (a).

[68] UE: a se vedea Directiva 95/46, articolul 8.

[69] UE: a se vedea Directiva 95/46, articolul 2 litera (b).

[70] UE: a se vedea Directiva 95/46, articolul 2 litera (f).

[71] UE: a se vedea Directiva 95/46, articolul 2 litera (f).

10. Colectarea, prelucrarea și utilizarea informațiilor cu caracter personal

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă că datele cu caracter personal trebuie să fie colectate și prelucrate numai în mod corect și legal [72] în scopuri determinate și nu pot fi utilizate într-un mod incompatibil cu acele scopuri, astfel cum poate fi definit termenul în legislația aplicabilă [73].

Elemente suplimentare necesare pentru aprobarea BCR Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă, de asemenea, că datele cu caracter personal sunt transferate și prelucrate numai în scopuri explicite și legitime [74].	Elemente suplimentare necesare pentru certificarea CBPR N/A
Clarificarea prelucrării datelor cu caracter personal (BCR) N/A	Clarificarea utilizării informațiilor cu caracter personal (CBPR) Informațiile cu caracter personal pot fi utilizate în alte scopuri compatibile sau conexe, cu consimțământul persoanei ale cărei informații cu caracter personal fac obiectul colectării, atunci când este necesar în scopul de a furniza un serviciu sau un produs solicitat de persoana respectivă sau în temeiul legilor și al altor instrumente juridice, al proclamațiilor și declarațiilor cu efect juridic [75].

Referințe

[72] UE: a se vedea Directiva 95/46, articolul 6 alineatul (1) litera (a); WP108, punctul 8.2.1, p. 8; WP153, punctul 6.1.i, p. 10; WP154, punctul 5, p. 4, punctul 6, p. 5; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul III, 18, p. 15; Cerințele programului, Q7, p. 7.

[73] UE: a se vedea Directiva 95/46, articolul 6 alineatul (1) litera (b); WP108, punctul 8.2.2, p. 8; WP153, punctul 6.1.ii, p. 10; WP154, punctul 3, p. 4; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiile III și IV, 18 și 19, pp. 15-16, Cerințele programului, Q6 și Q8, pp. 6, 8.

[74] UE: a se vedea Directiva 95/46, articolul 6 alineatul (1) litera (b); WP108, punctul 8.2.2, p. 8; WP153, punctul 6.1.ii, p. 10; WP154, punctul 3, p. 4.

[75] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul IV, 19, pp. 16-17, Cerințele programului, Q9 și Q13, pp. 8-10.

11. Calitatea și proporționalitatea/integritatea datelor

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină un angajament că

- datele cu caracter personal sunt exacte, complete și, atunci când este necesar, actualizate. Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă, de asemenea, că rectificările sunt comunicate tuturor părților relevante, atunci când este cazul [76].
- datele cu caracter personal sunt adecvate și pertinente în raport cu scopurile pentru care sunt transferate și/sau prelucrate ulterior [77].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, o cerință explicită ca datele cu caracter personal să nu fie excesive în raport cu scopurile în care sunt transferate și prelucrate ulterior [78].</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, o cerință ca datele cu caracter personal să nu poată fi prelucrate o perioadă mai lungă decât este necesar în vederea atingerii scopurilor pentru care au fost colectate sau, dacă este necesar, prelucrate ulterior [79].</p>	N/A

Referințe

[76] UE: a se vedea Directiva 95/46, articolul 6 alineatul (1) litera (d); WP153 punctul 6.1.iii, p. 10; WP108, punctul 8.2.3, p. 8; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VI, 21, p. 20; cerințele programului 21; 22, p. 15; chestionarul de admitere Q22, Q23 și Q24, p. 13.

[77] UE: a se vedea Directiva 95/46, articolul 6 alineatul (1) litera (c); WP153 punctul 6.1.iii, p. 10; WP108, punctul 8.2.3, p. 8; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul III, 18, p. 15, Cerințele programului, Q6, p. 6.

[78] UE: a se vedea Directiva 95/46, articolul 6 alineatul (1) litera (d); WP153 punctul 6.1.iii, p. 10.

[79] UE: a se vedea Directiva 95/46, articolul 6 alineatul (1) litera (e); WP153 punctul 6.1.iii, p. 10; WP108, punctul 8.2.3, p. 8.

12. Motive pentru prelucrarea datelor cu caracter personal

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină un angajament că:

- datele cu caracter personal sunt prelucrate (inclusiv colectate, utilizate, transferate, comunicate sau puse la dispoziție) numai dacă există un motiv valabil pentru prelucrare, de exemplu, în cazul în care persoana vizată și-a exprimat consimțământul în cunoștință de cauză [80].
- datele cu caracter personal sunt prelucrate în conformitate cu legislația aplicabilă [81].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>În cazul în care consimțământul reprezintă temeiul juridic pentru prelucrare, acesta trebuie să fie neechivoc, specific, liber acordat și în cunoștință de cauză [82].</p> <p>Consimțământul ca temei juridic pentru prelucrare nu poate fi eliminat din cauza caracterului evident, nici atunci când datele cu caracter personal sunt disponibile public, nici atunci când consimțământul nu este posibil din motive tehnologice și nici în cazul în care datele cu caracter personal au fost primite din partea unui terț.</p> <p>Consimțământul este numai unul dintre posibilele temeiuri juridice pentru prelucrarea datelor cu caracter personal.</p> <p>Datele cu caracter personal pot fi prelucrate, de asemenea, pentru următoarele motive [83]:</p> <ul style="list-style-type: none">- prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a lua măsuri la cererea persoanei vizate înainte de a încheia un contract sau- prelucrarea este necesară în vederea îndeplinirii unei obligații juridice a UE aplicabile operatorului sau- prelucrarea este necesară pentru a proteja interesele vitale ale persoanei	N/A

<p>vizate sau</p> <ul style="list-style-type: none"> - prelucrarea este necesară în vederea îndeplinirii unei sarcini realizate în interesul public sau în exercițiul autorității oficiale a UE cu care este învestit operatorul sau un terț căruia îi sunt comunicate datele; - prelucrarea este necesară pentru realizarea intereselor legitime ale operatorului sau ale terțului/terților cărora li se comunică datele, cu excepția cazului în care interesele privind drepturile și libertățile fundamentale ale persoanei vizate prevalează asupra intereselor menționate. 	
<p>Clarificarea motivelor pentru prelucrare (BCR)</p> <p>N/A</p>	<p>Clarificarea motivelor pentru prelucrare (CBPR)</p> <p>Persoanele trebuie să dispună de opțiuni în ceea ce privește colectarea, utilizarea și comunicarea informațiilor cu caracter personal care le privesc. Totuși, acest principiu recunoaște, prin formularea introductivă „atunci când este cazul” din însuși Cadrul privind protecția vieții private, că există anumite situații în care consimțământul poate fi, în mod clar, implicit sau în care nu ar fi necesară prevederea unui mecanism pentru exercitarea opțiunilor. Astfel de situații sunt detaliate în „Calificările pentru prevederea mecanismelor de opțiuni” [84].</p> <p>Sub rezerva calificărilor enumerate, se va pune la dispoziția persoanelor:</p> <ul style="list-style-type: none"> - un mecanism clar și evident pentru a-și exercita opțiunile cu privire la colectarea informațiilor cu caracter personal care le privesc; - un mecanism clar și evident pentru a-și exercita opțiunile cu privire la utilizarea informațiilor cu caracter personal care le privesc; - un mecanism clar și evident pentru a-și

	<p>exercita opțiunile cu privire la comunicarea informațiilor cu caracter personal care le privesc;</p> <ul style="list-style-type: none"> - mecanismele respective trebuie să fie clar formulate, ușor de înțeles, ușor accesibile și convenabile ca preț. <p>Calificările aplicabile includ:</p> <ul style="list-style-type: none"> - caracterul evident; - colectarea de informații disponibile public; - caracterul nepractic din punct de vedere tehnologic; - primirea de către terți; - comunicarea către o instituție guvernamentală care a depus o cerere de informații cu autoritate legală; - comunicarea către un terț în conformitate cu o formă legală de proces; - în scopuri de anchetă legitimă; - măsuri în caz de urgență. <p>Pe lângă consimțământ, datele cu caracter personal pot fi prelucrate, de asemenea, din următoarele motive [85]:</p> <ul style="list-style-type: none"> - în scopuri compatibile sau conexe, astfel cum sunt identificate în declarația de confidențialitate și/ sau în avizul prezentat în momentul colectării; - necesitatea de a furniza un serviciu sau un produs solicitat de persoana respectivă; - obligația de a respecta legile aplicabile.
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

- [80] UE: a se vedea Directiva 95/46, articolul 7 litera (a); WP154, punctul 5, p. 4; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul III, 18, p. 15.
- [81] UE: a se vedea WP153, punctul 6.4, p. 11; WP155 Q10, p. 6; APEC: a se vedea Cerințele programului, Q7, p. 7.
- [82] UE: a se vedea Directiva 95/46, articolul 7 litera (a); WP154, punctul 5, p. 4.
- [83] UE: a se vedea Directiva 95/46, articolul 7; WP154, punctul 5, p. 4.
- [84] APEC: a se vedea Cerințele programului Q14; 15; 16; 17; 18; 19, pp. 11-14.
- [85] APEC: a se vedea Cerințele programului Q8; 9; 10; 11; 12; 13, pp. 8-10.

13. Date sensibile

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să identifice măsurile de protecție aplicabile datelor sensibile [86].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă, de asemenea, că prelucrarea datelor sensibile (de exemplu, datele cu caracter personal care indică originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice, apartenența sindicală, datele privind viața sexuală sau referitoare la sănătate) este interzisă, cu excepția următoarelor situații [87]:</p> <ul style="list-style-type: none">- persoana vizată și-a exprimat consimțământul explicit pentru prelucrarea datelor sensibile respective, cu excepția cazului în care legile în vigoare interzic acest lucru sau- prelucrarea este necesară în vederea îndeplinirii obligațiilor și a exercitării drepturilor specifice ale operatorului în domeniul legislației UE privind ocuparea forței de muncă, în măsura în care este autorizată de legislația națională care prevede garanții adecvate sau- prelucrarea este necesară în vederea protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane, în cazul în care persoana vizată se află în incapacitate fizică sau legală de a-și exprima consimțământul sau- prelucrarea este efectuată în cadrul activităților sale legitime, cu garanții adecvate, de către o fundație, o asociație sau un alt organism fără scop lucrativ și cu specific politic, filosofic, religios sau sindical, cu condiția ca prelucrarea să se	<p>Atunci când se stabilesc utilizările permise ale informațiilor, trebuie să se aibă în vedere natura informațiilor [89].</p> <p>Garanțiile puse în aplicare în materie de securitate trebuie să fie rezonabile și proporționale cu probabilitatea și gravitatea prejudiciului potențial, cu sensibilitatea datelor și cu contextul în care sunt deținute acestea [90].</p>

<p>refere numai la membrii acestui organism sau la persoanele cu care acest are contacte regulate în legătură cu scopurile sale și ca datele să nu fie comunicate terților fără consimțământul persoanelor vizate sau</p> <ul style="list-style-type: none"> - prelucrarea vizează date sensibile care sunt făcute publice în mod manifest de către persoana vizată sau - prelucrarea datelor sensibile este necesară în vederea constatării, exercitării sau apărării unui drept în justiție sau - prelucrarea datelor sensibile este necesară în scopuri de medicină preventivă, diagnostic medical, furnizarea de îngrijiri sau tratament sau pentru gestionarea serviciilor medicale și în cazul în care datele sensibile respective sunt prelucrate de către un cadru medical care, în conformitate cu dreptul intern sau cu normele stabilite de autoritățile naționale competente, are obligația de a păstra secretul profesional, ori de către o altă persoană supusă, de asemenea, unei obligații echivalente în ceea ce privește secretul. <p>Prelucrarea datelor sensibile ar trebui să facă obiectul unor măsuri de securitate sporite [88].</p>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Referințe

- [86] UE: a se vedea Directiva 95/46, articolul 8; WP154, punctul 6, p. 5; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VII, 22, p. 21.
- [87] UE: a se vedea Directiva 95/46, articolul 8; WP154, punctul 6, p. 5.
- [88] UE: a se vedea Directiva 95/46, articolul 17 alineatul (1); WP154, punctul 10, p. 7.
- [89] APEC: a se vedea Cerințele programului, p. 8.
- [90] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VII, 22, p. 21; Cerințele programului, Q28, 30, 35(a), pp. 18-20.

14. Dreptul la transparență și informare/notificare

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Organizația trebuie să pună la dispoziția fiecărei persoane vizate o declarație de confidențialitate înainte de colectarea datelor sau în momentul colectării acestora [91]. Declarația trebuie să menționeze:

- modul în care persoanele vizate sunt informate cu privire la transferul și prelucrarea datelor lor cu caracter personal [92];
- identitatea operatorului (operatorilor) și a reprezentanților acestora, dacă este cazul, precum și un punct de contact [93];
- scopurile în care se prelucrează datele colectate [94];
- orice alte informații suplimentare, cum ar fi:
 - i. destinatarii sau categoriile de destinatari ai datelor [95];
 - ii. existența dreptului de acces la date și a dreptului de rectificare a datelor care privesc persoana vizată, precum și modul în care persoanele vizate pot obține accesul la datele lor cu caracter personal [96];

În cazul în care datele nu au fost obținute de la persoana vizată, există circumstanțe în care obligația de a informa persoana vizată poate să nu se aplice [97]. Scutirile sunt diferite în sistemul BCR și în sistemul CBPR. Cerințele specifice programului pentru BCR și pentru CBPR trebuie să fie specificate în regulile unei organizații privind protecția datelor cu caracter personal și a vieții private.

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Persoanele vizate trebuie să primească informații suplimentare în măsura în care informațiile respective sunt necesare, având în vedere circumstanțele specifice în care sunt colectate datele, cu scopul de a garanta prelucrarea corectă cu privire la persoana vizată [98].</p> <p>În cazul în care datele nu au fost obținute de la persoana vizată, obligația de a informa persoana vizată nu se aplică dacă furnizarea informațiilor se dovedește imposibilă sau ar implica un efort disproporționat ori dacă înregistrarea sau comunicarea datelor este prevăzută în mod specific de lege [99].</p> <p>Deși este posibil ca obligația de a informa persoana vizată să nu se aplice în situația de mai sus, aceasta nu este eliminată din cauza caracterului evident, nici atunci când datele cu</p>	<p>Organizația trebuie să informeze, de asemenea, persoanele vizate cu privire la modul în care sunt colectate datele și dacă acestea sunt colectate [100]:</p> <ul style="list-style-type: none">- în mod direct de la persoana în cauză sau- de către terți care efectuează colectarea în numele operatorului sau- în alt mod (acesta trebuie să fie descris). <p>Există circumstanțe în care notificarea poate să nu fie necesară sau practică [101]:</p> <ul style="list-style-type: none">- caracterul evident;- colectarea de informații disponibile în mod public;- impracticabilitate tehnologică;

<p>caracter personal sunt disponibile public, nici atunci când informarea persoanei vizate nu este posibilă din motive tehnologice și nici în cazul în care datele cu caracter personal au fost primite de la un terț.</p>	<ul style="list-style-type: none"> - comunicarea către o instituție guvernamentală care a înaintat o cerere de informații cu autoritate legală; - comunicarea către un terț în conformitate cu o formă legală de proces; - primirea de către terți; - în scopul unei anchete legitime; - măsuri în caz de urgență. <p>Informații suplimentare care trebuie să fie furnizate persoanelor vizate:</p> <ul style="list-style-type: none"> - faptul că se colectează date cu caracter personal [102]; - scopul în care datele sunt puse la dispoziția unor terți [103]; - informații privind utilizarea și comunicarea datelor persoanelor vizate [104]; - opțiunile și mijloacele oferite persoanelor vizate pentru a limita utilizarea și comunicarea datelor lor cu caracter personal [105].
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

- [91] UE: a se vedea Directiva 95/46, articolele 10 și 11; WP153, punctul 1.7, p. 5; WP74, punctul 5.7, p. 19; WP154, punctul 7, p. 5; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul II, 15 și 16, pp. 12-13 și 16, p. 13.
- [92] UE: a se vedea WP74, punctul 5.7, p. 19; WP153, punctul 6.1.i, p. 10; APEC: a se vedea Chestionarul de admitere, Q1, p.4; Q17-19, pp. 10-11.
- [93] UE: a se vedea WP154, punctul 7, p. 5; APEC: a se vedea Chestionarul de admitere, Q1-d), pp. 4-5.
- [94] UE: a se vedea WP154, punctul 7, p. 5; APEC: a se vedea Chestionarul de admitere, Q1-b) și Q3, pp. 4-5.
- [95] UE: a se vedea WP154, punctul 7, p. 5; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul II, 15-c), p. 12.
- [96] UE: a se vedea WP154, punctul 7, p. 5; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul II, 15-e), p. 12; Chestionarul de admitere, Q38- a), p. 18.
- [97] UE: a se vedea Directiva 95/46, articolele 10 și 11; APEC: a se vedea Chestionarul de admitere, Calificări pentru notificare, p. 6.
- [98] UE: a se vedea Directiva 95/46, articolul 10.
- [99] UE: a se vedea Directiva 95/46, articolul 11.

- [100] APEC: a se vedea Chestionarul de admitere, Q1-a), p.4 și Q5, p. 7.
- [101] APEC: a se vedea Chestionarul de admitere, Calificări pentru notificare, p. 6.
- [102] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul II, 15-a), p. 12.
- [103] APEC: a se vedea Chestionarul de admitere, Q1-c), p. 4.
- [104] APEC: a se vedea Chestionarul de admitere, Q1-e), p. 5.
- [105] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul II, 15-e), p. 12;
Chestionarul de admitere, Q15-16, p. 10.

15. Drepturile de acces, rectificare, ștergere și blocare a datelor/acces și corectare

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Organizația trebuie să se asigure că [106]:

- orice persoană vizată poate obține de la operator confirmarea faptului dacă acesta deține sau nu date cu caracter personal despre persoana respectivă [107];
- orice persoană vizată poate obține o copie a tuturor datelor referitoare la aceasta deținute de către organizație; datele relevante trebuie să fie furnizate fără constrângeri, într-un termen rezonabil și fără taxe excesive (în cazul în care se percep taxe) [108];
- orice persoană vizată poate cere unui operator de date să rectifice sau să șteargă date care sunt în special incomplete sau inexacte [109].

Aceste obligații fac obiectul excepțiilor și calificărilor în conformitate cu legile aplicabile [110].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Elementele enumerate în referențialul comun de mai sus sunt drepturi acordate persoanelor vizate.</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să garanteze, de asemenea, că orice persoană vizată are dreptul să ceară unui operator de date să blocheze datele, în special în cazul în care datele sunt incomplete sau inexacte [111].</p>	<p>Operatorii trebuie să ia măsuri pentru a confirma identitatea persoanei vizate care solicită accesul [112].</p> <p>Atunci când se oferă informații unei persoane vizate care și-a exercitat dreptul de acces, informațiile trebuie să fie comunicate într-o modalitate rezonabilă, ușor de înțeles la nivel general și prin mijloace compatibile cu forma de interacțiune obișnuită cu persoana respectivă [113].</p> <p>Operatorii se angajează să efectueze corecturile sau ștergerile într-un termen rezonabil [114].</p> <p>Operatorii trebuie să prezinte persoanei vizate o copie a datelor cu caracter personal corectate sau să confirme că datele au fost corectate sau șterse [115].</p> <p>Operatorii trebuie să explice persoanelor vizate de ce nu li se poate acorda accesul sau de ce nu se poate efectua corectarea și trebuie să le furnizeze acestora informațiile de contact care pot fi utilizate pentru alte întrebări cu privire la interzicerea accesului sau a corectării [116].</p>

Excepții de la drepturile de acces (BCR)

Legile naționale din UE în materie de protecție a datelor pot prevedea unele excepții de la dreptul de acces al persoanelor vizate, în temeiul dreptului intern din UE, care trebuie să fie interpretate într-o manieră restrictivă. În astfel de cazuri, poate fi necesar ca organizațiile să respingă cererile de acces pentru a proteja [117]:

- (a) securitatea națională a statelor membre ale UE;
- (b) apărarea statelor membre ale UE;
- (c) securitatea publică a statelor membre ale UE;
- (d) prevenirea, anchetarea, depistarea și urmărirea penală a infracțiunilor sau a încălcărilor deontologiei pentru profesiile reglementate;
- (e) un interes economic sau financiar important al unui stat membru sau al Uniunii Europene, inclusiv în domeniul monetar, bugetar și fiscal;
- (f) o funcție de monitorizare, de inspecție sau de reglementare legată, chiar și numai ocazional, de exercitarea autorității oficiale în cazurile menționate la literele (c), (d) și (e);
- (g) protecția persoanei vizate sau a drepturilor și libertăților altor persoane.

Legile naționale din UE în materie de protecție a datelor pot prevedea, sub rezerva unor garanții juridice adecvate, cu condiția ca datele să nu fie utilizate pentru a lua măsuri sau decizii privind o anumită persoană, că dreptul de acces al persoanelor vizate poate să fie restricționat în cazul în care este evident că nu există niciun risc de a încălca dreptul la viață privată al unei persoane vizate, atunci când datele sunt prelucrate numai în scopul cercetării științifice sau sunt păstrate în formularul personal o perioadă care nu depășește perioada necesară exclusiv pentru

Excepții privind cererile de acces (CBPR)

Există situații în care poate fi necesar ca organizațiile să respingă cererile de acces [118]:

- sarcină disproporționată;
- protecția informațiilor confidențiale;
- risc aferent părților terțe.

Referințe

- [106] UE: a se vedea Directiva 95/46, articolul 12; WP153, punctul 6.1.v., p. 10; WP108, punctul 8.2.5, p. 8.
- [107] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VIII, 23-a), p. 22; Chestionarul de admitere, Q36, p. 17.
- [108] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VIII, 23-b), p. 22, Chestionarul de admitere, Q37, 37-b, 37-e), pp. 17-18.
- [109] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VIII, 23-c), p. 22; Chestionarul de admitere, Q38, 38-b, pp. 18-19.
- [110] UE: a se vedea Directiva 95/46, articolul 13; APEC: a se vedea Chestionarul de admitere, Calificări pentru prevederea unor mecanisme de acces și de corectare, pp. 19-20.
- [111] UE: a se vedea Directiva 95/46, articolul 12.
- [112] APEC: a se vedea Chestionarul de admitere, Q37-a), p. 17.
- [113] APEC: a se vedea Chestionarul de admitere, Q37-c) și d), p. 18.
- [114] APEC: a se vedea Chestionarul de admitere, Q38-a), p. 19.
- [115] APEC: a se vedea Chestionarul de admitere, Q38-d), p. 19.
- [116] APEC: a se vedea Chestionarul de admitere, partea iii, principiul VIII, 25, p.24, Chestionarul de admitere, Q38-e), p. 19.
- [117] UE: a se vedea Directiva 95/46, articolul 13.
- [118] APEC: a se vedea Chestionarul de admitere, Calificări pentru prevederea unor mecanisme de acces și de corectare, pp. 19-20.

16. Dreptul de opoziție/dreptul de a alege

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Dacă este necesar sau se prevede astfel în legislația aplicabilă, organizația trebuie să se asigure că persoana vizată poate să se opună prelucrării datelor sale cu caracter personal sau să aleagă ca datele sale cu caracter personal să nu fie supuse prelucrării, în conformitate cu legislația aplicabilă [119].

<p>Elemente suplimentare necesare pentru aprobarea BCR</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie, de asemenea, să ofere asigurări că orice persoană vizată beneficiază de dreptul de opoziție față de prelucrarea propriilor date cu caracter personal, acesta fiind un drept acordat persoanelor vizate.</p> <p>Dreptul de opoziție poate fi exercitat de către persoanele vizate în orice moment.</p> <p>În special, orice persoană vizată beneficiază de dreptul de a se opune, la cerere și în mod gratuit, prelucrării datelor sale cu caracter personal care, conform anticipărilor operatorului, urmează să fie prelucrate în scopuri de marketing direct, de dreptul de a fi informată înainte de comunicarea datelor cu caracter personal pentru prima oară unor terți sau de utilizarea datelor în numele acestora în scopuri de marketing direct și de dreptul de li se oferi posibilitatea de a se opune în mod gratuit unor astfel de comunicări sau utilizări.</p>	<p>Elemente suplimentare necesare pentru certificarea CBPR</p> <p>N/A</p>
<p>Excepții de la dreptul de opoziție (BCR)</p> <p>N/A</p>	<p>Excepții de la dreptul de a alege (CBPR)</p> <p>Există circumstanțe în care punerea la dispoziția persoanelor, de către organizații, a unor mecanisme de exercitare a dreptului de a alege poate să nu fie necesară sau practică [120]:</p> <ul style="list-style-type: none">- caracterul evident;- colectarea de informații disponibile în mod public;

	<ul style="list-style-type: none"> - impracticabilitate tehnologică; - primirea de către terți; - comunicarea către o instituție guvernamentală care a înaintat o cerere de informații cu autoritate legală; - comunicarea către un terț în conformitate cu o formă legală de proces; - în scopuri de anchetă legitimă; - măsuri în caz de urgență.
<p>Clarificarea dreptului de opoziție (BCR)</p> <p>Persoana vizată are întotdeauna dreptul de a-și retrage consimțământul. În plus, în cazul în care există un alt temei juridic care justifică prelucrarea, persoanele vizate pot, de asemenea, să se opună.</p> <p>Mai mult, legile naționale din UE în materie de protecție a datelor menționează situațiile în care persoanele vizate, cel puțin în cazurile în care temeiul juridic al prelucrării derivă din articolul 7 litera (e) sau (f) din Directiva 95/46/CE, pot să se opună din motive întemeiate și legitime legate de situația lor specifică, cu excepția cazului în care legislația națională a statelor membre ale UE prevede altfel. În cazul în care opoziția este justificată, prelucrarea inițiată de către operator nu mai poate implica datele respective [121].</p> <p>Dreptul de opoziție nu poate fi eliminat din cauza caracterului evident, nici atunci când datele cu caracter personal supuse prelucrării sunt disponibile public, nici atunci când dreptul de opoziție este impracticabil din motive tehnologice și nici în cazul în care datele cu caracter personal au fost primite de la un terț.</p>	<p>Clarificarea dreptului de a alege (CBPR)</p> <p>Organizațiile trebuie să pună la dispoziția persoanelor mecanisme de exercitare a dreptului de a alege în ceea ce privește colectarea, utilizarea și comunicarea informațiilor lor cu caracter personal [122].</p>

Referințe

[119] UE: a se vedea Directiva 95/46, articolul 14, WP153, punctul 6.1.v, p. 10; WP108, punctul 8.2.5, p. 8; APEC: a se vedea Chestionarul de admitere, Q14-16.

[120] APEC: a se vedea Chestionarul de admitere, Calificări pentru prevederea unor mecanisme de exercitare a dreptului de a alege, pp. 11-12.

[121] UE: a se vedea Directiva 95/46, articolul 14.

[122] APEC: a se vedea Cerințele programului, Q14-16, pp. 11-13.

17. Decizii individuale automate

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

N/A

Elemente necesare pentru aprobarea BCR	Elemente necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să dea asigurări privind faptul că nicio evaluare sau o decizie privind persoana vizată care are un impact semnificativ asupra acesteia nu va fi bazată exclusiv pe prelucrarea automată a datelor sale, cu excepția cazurilor în care decizia respectivă [123]:</p> <ul style="list-style-type: none">- este luată la încheierea unui contract sau în timpul executării acestuia, cu condiția ca cererea de încheiere a contractului sau de executare a acestuia, înaintată de către persoana vizată, să fi fost aprobată, cu condiția să existe măsuri adecvate pentru protejarea intereselor sale legitime, cum ar fi acorduri care îi permit să-și exprime punctul de vedere;- este prevăzută într-o lege care stabilește și măsuri de protejare a intereselor legitime ale persoanei vizate.	N/A

Referințe

[123] UE: a se vedea WP154, punctul 9, p. 6.

18. Securitate și confidențialitate

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină o cerință privind punerea în aplicare a unor măsuri tehnice și organizatorice adecvate pentru a proteja datele cu caracter personal împotriva distrugerii accidentale sau ilegale, a pierderii accidentale, a modificării, a dezvăluirii neautorizate sau a accesului autorizat și a tuturor celorlalte forme ilegale de prelucrare [124].

Măsurile respective trebuie să asigure un nivel de securitate adaptat riscurilor reprezentate de prelucrare și naturii datelor care trebuie să fie protejate [125].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, o cerință ca măsurile de securitate să fie puse în aplicare ținând seama de stadiul actual al tehnologiei și de costul punerii în aplicare a acestora [126].</p>	<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă, de asemenea, că garanțiile în materie de securitate ar trebui să facă obiectul unei revizui și reevaluări periodice [127].</p> <p>Trebuie să se pună în aplicare o politică privind securitatea informațiilor [128] și o politică de eliminare sigură a datelor cu caracter personal [129].</p> <p>Trebuie să se instituie garanții privind detectarea, prevenirea și răspunsul la atacuri, intruziuni și alte deficiențe de securitate [130].</p> <p>Angajații trebuie să fie, de asemenea, conștienți de importanța menținerii securității datelor cu caracter personal și de obligația de a respecta securitatea datelor respective, prin organizarea de cursuri de formare periodice și prin monitorizare, astfel cum este demonstrat prin proceduri [131].</p>

Referințe

[124] UE: a se vedea Directiva 95/46, articolul 17 alineatul (1); WP108, punctul 8.2.4, p. 8; APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VII, 22, p. 2; Chestionarul de admitere, Q27, p. 14.

[125] UE: a se vedea Directiva 95/46, articolul 17 alineatul (1); APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VII, 22, p. 21, Chestionarul de admitere, Q28, p. 14.

[126] UE: a se vedea Directiva 95/46, articolul 17 alineatul (1).

- [127] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul VII, 22, p. 21.
- [128] APEC: a se vedea Chestionarul de admitere, Q26, p. 14.
- [129] APEC: a se vedea Chestionarul de admitere, Q31, p. 15.
- [130] APEC: a se vedea Chestionarul de admitere, Q32 și Q33, p. 15.
- [131] APEC: a se vedea Chestionarul de admitere, Q29 și Q30-a), p. 14.

19. Programul de formare

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă formarea adecvată a personalului acesteia cu privire la regulile sale privind protecția datelor cu caracter personal și a vieții private [132].

<p>Elemente suplimentare necesare pentru aprobarea BCR</p> <p>Cerința privind formarea se referă la angajații care au acces permanent sau regulat la datele cu caracter personal, sunt implicați în colectarea de date cu caracter personal sau în elaborarea de instrumente utilizate pentru prelucrarea datelor cu caracter personal [133].</p>	<p>Elemente suplimentare necesare pentru certificarea CBPR</p> <p>Formarea trebuie să vizeze politicile și procedurile în materie de protecție a vieții private, inclusiv modul de a răspunde plângerilor referitoare la protecția vieții private [134].</p> <p>Angajații trebuie să fie, de asemenea, conștienți de importanța menținerii securității datelor cu caracter personal și de obligația de a respecta securitatea datelor respective, prin organizarea de cursuri de formare periodice și prin monitorizare, astfel cum este demonstrat prin proceduri [135].</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

[132] UE: a se vedea WP74, punctul 5.1, p. 16; APEC: a se vedea Chestionarul de admitere, Q44, p. 22.

[133] UE: a se vedea WP153, punctul 2.1, p. 5.

[134] APEC: a se vedea Cerințele programului, Q44, pp. 25-26.

[135] APEC: a se vedea Chestionarul de admitere, Q30-a), p. 14.

20. Programul de monitorizare și audit

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă monitorizarea aplicării și a respectării regulilor sale privind protecția datelor cu caracter personal și a vieții private [136].

<p>Elemente suplimentare necesare pentru aprobarea BCR</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, obligația de a verifica respectarea de către grup a regulilor privind protecția datelor cu caracter personal și a vieții private și, în special, următoarele aspecte [137]:</p> <ul style="list-style-type: none">- programul de audit acoperă toate aspectele legate de protecția datelor cu caracter personal și a vieții private, inclusiv metode de a se asigura faptul că se vor întreprinde acțiuni corective;- astfel de acțiuni de audit trebuie să fie efectuate în mod regulat (trebuie să se specifice intervalul) de către echipa de audit acreditată internă sau externă sau la cererea specifică a inspectorului/funției responsabile de protecția vieții private (sau orice altă funcție competentă din cadrul organizației);- rezultatele tuturor auditurilor ar trebui să fie comunicate inspectorului/funției responsabile de protecția vieții private (sau orice altă funcție competentă din cadrul organizației) și consiliului de administrație;- APD din UE pot primi, la cerere, o copie a auditurilor;- planul de audit ar trebui să permită APD din UE să aibă autoritatea de a realiza un audit în materie de protecție a datelor, dacă este necesar;- fiecare membru al grupului trebuie să	<p>Elemente suplimentare necesare pentru certificarea CBPR</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, cerința ca operatorul să ateste anual continuarea aderării la cerințele programului CBPR [138].</p> <p>Agenții APEC cu responsabilități în materie de CBPR trebuie să realizeze revizuri detaliate periodice pentru a asigura integritatea recertificării [139].</p> <p>Operatorul trebuie să efectueze periodic verificări la fața locului sau monitorizări vizând persoanele împuternicite de acesta în vederea prelucrării de date cu caracter personal, agenții, contractanții sau alți prestatori de servicii, pentru a asigura conformitatea cu instrucțiunile sale și cu acordurile/contractele pe care le-a încheiat [140].</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

accepte că poate fi auditat de către APD din UE și că va respecta recomandările APD din UE cu privire la orice aspect legat de regulile în cauză.	
---------------------------------------------------------------------------------------------------------------------------------------------------	--

Referințe

[136] UE: a se vedea WP74, punctul 5.2, p. 16; APEC: a se vedea Cererea de recunoaștere, anexa A, 6-8, p. 6.

[137] UE: a se vedea WP153, punctul 2.3, p. 7.

[138] APEC: a se vedea Cererea de recunoaștere, anexa A, 8, p. 6.

[139] APEC: a se vedea Cererea de recunoaștere, anexa A, 8, p. 6.

[140] APEC: a se vedea Chestionarul de admitere, Q49, p. 23.

21. Conformitatea și monitorizarea conformității

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă numirea unor angajați adecvați (cum ar fi o rețea de inspectori privind protecția vieții private) care să supravegheze și să asigure conformitatea cu regulile organizației privind protecția datelor cu caracter personal și a vieții private [141].

<p>Elemente suplimentare necesare pentru aprobarea BCR [142]</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, o scurtă descriere a structurii interne, a rolului și a responsabilităților rețelei sau a inspectorilor privind protecția vieții private sau a funcției similare create pentru a asigura conformitatea cu regulile organizației privind protecția datelor cu caracter personal și a vieții private.</p> <p>Personalul corespunzător numit trebuie să fie susținut de către conducerea superioară.</p> <p>Exemplu de structură internă, rol și responsabilități ale rețelei sau ale inspectorilor privind protecția vieții private sau ale funcției similare create pentru a asigura conformitatea cu regulile organizației privind protecția datelor cu caracter personal și a vieții private: inspectorul-șef privind protecția vieții private informează consiliul de administrație, se ocupă de anchetele ADP naționale din UE, întocmește rapoarte anuale privind conformitatea, asigură conformitatea la nivel global și faptul că inspectorii privind protecția vieții private pot fi responsabili cu soluționarea la nivel local a plângerilor persoanelor vizate, raportarea problemelor majore privind protecția vieții private inspectorului-șef privind protecția vieții private și asigurarea conformității la nivel local.</p>	<p>Elemente suplimentare necesare pentru certificarea CBPR</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă, de asemenea, că persoana (persoanele) numită (numite) trebuie să introducă proceduri oportune pentru primirea, investigarea și soluționarea plângerilor referitoare la protecția vieții private, explicând acțiunile corective întreprinse, atunci când este cazul [143].</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

[141] UE: a se vedea WP74, punctul 5.1, p. 16; APEC: a se vedea Chestionarul de admitere, Q40, p. 21.

[142] UE: a se vedea WP153, punctul 2.4, p. 8.

[143] APEC: a se vedea Cerințele programului, Q40, pp. 24-25.

22. Mecanisme interne de soluționare a plângerilor

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să instituie o procedură de soluționare a plângerilor, prin care [144]:

- orice persoană vizată poate depune o plângere în care să sesizeze că orice membru al grupului nu respectă regulile organizației privind protecția datelor cu caracter personal și a vieții private.
- plângerile sunt soluționate de un departament/o persoană specificat(ă) în mod clar.

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
Departamentul/persoana care se ocupă cu soluționarea plângerilor trebuie să beneficieze de un nivel adecvat de independență în exercitarea funcțiilor sale [145].	Atunci când se răspunde persoanelor vizate în legătură cu plângerile înaintate de acestea, răspunsul trebuie să includă explicații cu privire la acțiunile corective întreprinse ca urmare a plângerii lor [146].

Referințe

[144] UE: a se vedea WP74, punctul 5.3, p. 17; APEC: a se vedea Chestionarul de admitere, Q41-42, p.21.

[145] UE: a se vedea WP74, punctul 5.3, p. 17.

[146] APEC: a se vedea Chestionarul de admitere, Q43, p. 21.

23. Actualizarea regulilor unei organizații privind protecția datelor cu caracter personal și a vieții private

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă raportarea oricăror modificări semnificative aduse regulilor sale privind protecția datelor cu caracter personal și a vieții private sau listei membrilor către toți membrii grupului, precum și APD din UE și agenților APEC cu responsabilități în materie de CBPR, pentru a ține seama de modificările cadrului de reglementare și ale structurii întreprinderii, și anume de faptul că unele modificări pot necesita o nouă aprobare din partea APD naționale din UE și/sau pot necesita o revizuire de către agenții APEC cu responsabilități în materie de CBPR [147].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, o prevedere conform căreia modificările substanțiale aduse regulilor organizației privind protecția datelor cu caracter personal și a vieții private vor fi comunicate, de asemenea, persoanelor vizate [148].</p> <p>Actualizarea regulilor unei organizații privind protecția datelor cu caracter personal și a vieții private sau a listei membrilor grupului care trebuie să respecte regulile respective se poate realiza fără a fi necesar să se solicite din nou autorizarea în următoarele condiții [149]:</p> <ul style="list-style-type: none">(i) o persoană identificată păstrează o listă actualizată integral a membrilor grupului, ține evidența și înregistrează orice modificări aduse regulilor privind protecția datelor cu caracter personal și a vieții private și furnizează informațiile necesare persoanelor vizate și APD naționale din UE, la cerere.(ii) nu are loc un transfer către un nou membru înainte ca respectivul nou membru să fie obligat în mod efectiv să respecte regulile organizației privind protecția datelor cu caracter personal și a vieții private și să fie în măsură să	<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină, de asemenea, o cerință privind faptul că, în cazul în care s-a adus o modificare de fond regulilor organizației privind protecția datelor cu caracter personal și a vieții private (astfel cum a stabilit în mod rezonabil și cu bună credință agentul APEC cu responsabilități în materie de CBPR), agentul va întreprinde fără întârziere un proces de revizuire [150].</p> <p>Organizațiile ar trebui să furnizeze o declarație actualizată privind practicile și politicile lor referitoare la informațiile cu caracter personal [151].</p> <p>De asemenea, organizațiile trebuie să ofere persoanelor mecanisme de exercitare a dreptului de a alege în ceea ce privește colectarea, utilizarea și comunicarea informațiilor lor cu caracter personal [152].</p>

<p>asigure conformitatea.</p> <p>(iii) orice modificări aduse regulilor organizației privind protecția datelor cu caracter personal și a vieții private sau listei membrilor ar trebui să fie raportate o dată pe an către APD naționale din UE responsabile de autorizare, împreună cu o scurtă explicație a motivului actualizării.</p>	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Referințe

[147] UE: a se vedea WP74, punctul 4.2, p. 15; APEC: a se vedea Cererea de recunoaștere, anexa A, 8, p. 6.

[148] UE: a se vedea WP154, punctul 21, pp. 9-10.

[149] UE: a se vedea WP74, punctul 4.2, p. 15.

[150] APEC: a se vedea Cererea de recunoaștere, anexa A, 8, p. 6.

[151] APEC: a se vedea Cadrul privind protecția vieții private, partea iii, principiul II, 15; Chestionarul de admitere, Q1, p. 4.

[152] APEC: a se vedea Cerințele programului, Q14-16, pp. 11-13.

24. Acțiuni în situația în care legislația locală riscă să împiedice respectarea regulilor organizației privind protecția datelor cu caracter personal și a vieții private și în cazul cererilor de acces formulate de autoritățile de aplicare a legii

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

N/A

<p>Elemente necesare pentru aprobarea BCR [153]</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină o prevedere clară care să indice faptul că, în cazul în care un membru al grupului are motive să considere că legislația care i se aplică îl împiedică să-și îndeplinească obligațiile izvorâte din regulile organizației privind protecția datelor cu caracter personal și a vieții private și are un efect considerabil asupra garanțiilor oferite în regulile în cauză, membrul respectiv informează fără întârziere sediul din UE sau membrul din UE căruia i s-au delegat responsabilități în materie de protecție a datelor ori cealaltă persoană cu funcție relevantă privind protecția vieții private (cu excepția cazului în care acest lucru este interzis de o autoritate de aplicare a legii, cum ar fi interdicția din dreptul penal menită să păstreze confidențialitatea unei anchete a autorităților de aplicare a legii).</p> <p>De asemenea, regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să prevadă faptul că, în cazul în care există un conflict între legislația națională și obligațiile, cerințele și angajamentele prevăzute în regulile organizației privind protecția datelor cu caracter personal și a vieții private ale sediului din UE, membrul din UE căruia i s-au delegat responsabilități în materie de protecție a datelor sau cealaltă persoană cu funcție relevantă privind protecția vieții private</p>	<p>Elemente necesare pentru certificarea CBPR</p> <p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină o cerință privind existența unei proceduri în situația unor citații, mandate sau ordine judiciare sau guvernamentale, inclusiv cele care solicită comunicarea de date cu caracter personal [154].</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>trebuie să consulte APD naționale competente din UE și să ia o decizie responsabilă cu privire la măsurile pe care trebuie să le întreprindă.</p>	
------------------------------------------------------------------------------------------------------------------------------------------------------	--

<p>Orice incidente referitoare la acest aspect din regulile organizației privind protecția datelor cu caracter personal și a vieții private trebuie să fie detaliat și analizat în cadrul auditurilor periodice menționate în secțiunea 20.</p>	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Referințe

[153] UE: a se vedea WP74, punctul 3.3.3, pp. 13-14 și WP154, punctul 16, p. 8.

[154] APEC: a se vedea Chestionarul de admitere, Q45, p. 22.

25. Asistența reciprocă și cooperarea cu APD naționale din UE/PEA ale APEC

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

N/A

Elemente necesare pentru aprobarea BCR	Elementele necesare pentru certificarea CBPR
<p>Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să conțină următoarele obligații:</p> <ul style="list-style-type: none">- membrii grupului trebuie să coopereze și să se ajute reciproc să proceseze o cerere sau o plângere înaintată de o persoană ori o anchetă sau cercetare efectuată de APD din UE;- entitățile trebuie să se conformeze recomandărilor făcute de APD naționale din UE cu privire la orice aspecte legate de interpretarea regulilor organizației privind protecția datelor cu caracter personal și a vieții private.	<p>Organizațiile din economiile participante pot beneficia de certificarea CBPR. Economiiile membre pot să participe la sistemul CBPR numai dacă autoritatea lor de asigurare a aplicării normelor privind protecția vieții private (PEA) participă la Acordul APEC privind asigurarea aplicării transfrontaliere a normelor privind protecția vieții private (CPEA) [156].</p>

Referințe

[155] UE: a se vedea WP74, punctul 5.4, p. 17.

[156] APEC: a se vedea Carta JOP , punctul 2.2i, p. 15.

26. Relația dintre legislația locală și regulile unei organizații privind protecția datelor cu caracter personal și a vieții private

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

N/A

<p>Elemente necesare pentru aprobarea BCR</p> <p>În cazul în care datele cu caracter personal sunt prelucrate în UE, se aplică legile privind protecția datelor din UE. Prin urmare, regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să confirme că [157]:</p> <ul style="list-style-type: none">- în cazul în care legislația locală, de exemplu legislația UE, prevede un nivel mai ridicat de protecție a datelor cu caracter personal, aceasta va avea întâietate față de regulile organizației privind protecția datelor cu caracter personal și a vieții private;- în orice caz, datele vor fi prelucrate în conformitate cu legislația statului membru în cauză, în conformitate cu articolul 4 din Directiva 95/46/CE.	<p>Elementele necesare pentru certificarea CBPR</p> <p>N/A</p>
<p>Clarificarea relației dintre legislația locală și BCR</p> <p>N/A</p>	<p>Clarificarea relației dintre legislația locală și CBPR [158]</p> <p>Participarea la sistemul CBPR nu înlocuiește obligațiile legale interne ale organizației participante.</p> <p>În cazul în care nu există cerințe naționale aplicabile privind protecția vieții private într-o economie, regulile organizației privind protecția datelor cu caracter personal și a vieții private sunt menite să asigure un nivel minim de protecție.</p> <p>În cazul în care cerințele legale interne depășesc ceea ce este prevăzut în regulile organizației privind protecția datelor cu caracter personal și a vieții private, se vor</p>

	<p>aplica în continuare integral legile și reglementările interne în acest domeniu.</p> <p>În cazul în care cerințele din regulile organizației privind protecția datelor cu caracter personal și a vieții private depășesc cerințele din legile și reglementările interne, organizația va trebui să îndeplinească cerințele suplimentare pentru a putea participa.</p> <p>Cu toate acestea, autoritățile de asigurare a aplicării normelor privind protecția vieții private din economia respectivă ar trebui să aibă capacitatea de a lua măsuri de aplicare a legii, în temeiul legilor și reglementărilor interne aplicabile, care să aibă ca efect protecția informațiilor cu caracter personal în concordanță cu cerințele CBPR.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

[157] UE: a se vedea WP74, punctul 3.3.3, pp. 13-14.

[158] APEC: a se vedea Politici, norme și orientări, punctele 43 și 44, pp. 10-11.

27. Dispoziții finale

Elemente comune necesare atât pentru aprobarea BCR, cât și pentru certificarea CBPR

Regulile unei organizații privind protecția datelor cu caracter personal și a vieții private trebuie să specifice data la care acestea intră în vigoare [159].

Referințe

[159] UE: a se vedea WP154, punctul 23, p. 10; APEC: a se vedea Cerințele programului, Q1, p. 2.

Adoptat la Bruxelles, 27 februarie 2014

*Pentru grupul de lucru,
Președintele
Jacob KOHNSTAMM*

Apendice

Apendicele 1: Documentația care trebuie furnizată de o organizație care dorește aprobarea BCR proprii de către APD naționale din UE și de o organizație care dorește certificarea CBPR proprii de către agenții APEC cu responsabilități în materie de CBPR

Apendicele 1: Documentația care trebuie furnizată de o organizație care dorește aprobarea BCR proprii de către APD naționale din UE și de o organizație care dorește certificarea CBPR proprii de către agenții APEC cu responsabilități în materie de CBPR

O organizație care solicită aprobarea BCR și certificarea CBPR proprii trebuie să furnizeze APD naționale din UE și agentului APEC cu responsabilități în materie de CBPR orice documente care arată că obligațiile, cerințele și angajamentele din regulile organizației privind protecția datelor cu caracter personal și a vieții private sunt respectate, de exemplu [160]:

- politici în materie de protecție a vieții private (de exemplu, politica de protecție a vieții private privind clienții, politica de protecție a vieții private privind resursele umane) pentru a informa persoanele vizate (de exemplu, clienții, angajații) cu privire la modul în care întreprinderea protejează datele lor cu caracter personal [161];
- orientări pentru angajații care au acces la datele cu caracter personal, astfel încât aceștia să poată să înțeleagă și să aplice ușor normele incluse în regulile privind protecția vieții private (de exemplu, orientări privind modul de a răspunde la o plângere de la o persoană vizată, de a oferi informații persoanelor vizate, privind măsurile corespunzătoare de securitate/confidențialitate care trebuie să fie respectate) [162];
- exemple și/sau explicații cu privire la programul de formare [163];
- descrierea sistemului intern de soluționare a plângerilor [164];
- politica de securitate pentru sistemele informatice care prelucrează datele cu caracter personal din APEC și UE [165];
- orice contract standard care trebuie să fie utilizat cu persoanele împuternicite de către operatorii de date (care sunt sau nu membre ale grupului) care prelucrează date cu caracter personal din UE și APEC, după caz [166].

Elemente suplimentare necesare pentru aprobarea BCR	Elemente suplimentare necesare pentru certificarea CBPR
<p>Organizația solicitantă furnizează, de asemenea, APD din UE:</p> <ul style="list-style-type: none"> - o fișă a postului pentru inspectorii însărcinați cu protecția datelor sau pentru alte persoane însărcinate cu protecția datelor în cadrul întreprinderii; - cererea-tip WP133 [167]; - planul și programul de audit al protecției datelor, stabilit împreună cu 	<p>Organizația solicitantă furnizează, de asemenea, agenților APEC cu responsabilități în materie de CBPR:</p> <ul style="list-style-type: none"> - chestionarul de admitere; - exemple de documente suplimentare care pot fi necesare pentru ca agenții APEC cu responsabilități în materie de CBPR să își efectueze analiza cu privire la regulile organizației privind protecția

<p>persoanele competente (auditori acreditați interni/externi ai întreprinderii);</p> <p>- o documentație care arată că membrul aflat la originea transferului de date în afara UE și sediul din UE sau membrul din UE căruia i s-au delegat responsabilități dețin suficiente active pentru a putea plăti despăgubirile rezultate din încălcarea regulilor organizației privind protecția datelor cu caracter personal și a vieții private.</p>	<p>datelor cu caracter personal și a vieții private:</p> <ul style="list-style-type: none"> - exemple de notificări furnizate persoanelor vizate [168]; - o documentație care arată respectarea limitelor privind colectarea de date, identificând [169]: <ul style="list-style-type: none"> (i) fiecare tip de date colectate; (ii) scopul corespunzător declarat pentru colectarea fiecărui tip de date și (iii) toate utilizările care se aplică pentru fiecare tip de date; (iv) o explicație a gradului de compatibilitate sau de conexiune a fiecărei utilizări identificate cu scopul declarat al colectării; - o documentație care arată că datele cu caracter personal sunt colectate, utilizate și comunicate în scopurile identificate sau în alte scopuri compatibile sau conexe, cu excepția cazului în care există derogări în anumite circumstanțe [170]; - o documentație care prezintă mecanismele puse la dispoziția persoanelor vizate pentru ca acestea să își poată exercita dreptul de a alege în ceea ce privește colectarea, utilizarea și comunicarea datelor lor cu caracter personal și care arată că mecanismele respective există și funcționează și că scopul colectării este declarat în mod clar [171]; - procedurile implementate pentru a verifica și a asigura faptul că datele cu caracter personal sunt actualizate, exacte și complete, în măsura necesară pentru scopurile în care acestea sunt utilizate [172]; - o documentație care arată existența
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	acordurilor cu persoanele împuternicite de către operatori, agenți, contractanți sau alți prestatori de servicii pentru a asigura că obligațiile operatorului față de persoanele vizate vor fi respectate [173].
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Referințe

[160] UE: a se vedea WP154, documentația care trebuie furnizată APD, pp. 10-11.

[161] APEC: a se vedea Cerințele programului, Q1, pp. 2-4.

[162] APEC: a se vedea Cerințele programului, Q29, p. 18; Q44, pp. 25-26.

[163] APEC: a se vedea Cerințele programului, Q44, pp. 25-26.

[164] APEC: a se vedea Cerințele programului, Q41-43, p. 25.

[165] APEC: a se vedea Cerințele programului, Q26, p. 17; Q31, p. 19.

[166] APEC: a se vedea Cerințele programului, Q46, pp. 26-27.

[167] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc.

[168] APEC: a se vedea Cerințele programului, Q2, p. 4.

[169] APEC: a se vedea Cerințele programului, Q6, p. 6.

[170] APEC: a se vedea Cerințele programului, Q8, p. 8.

[171] APEC: a se vedea Cerințele programului, Q14-17, pp. 11-13.

[172] APEC: a se vedea Cerințele programului, Q21, p. 15.