

studii și cercetări

Obligația de informare și de notificare în cazul încălcării securității datelor cu caracter personal conform art. 33, 34 GDPR

The obligation of notification and communication of a personal data breach in accordance with articles 33 and 34 of the GDPR

JÜRGEN TAEGER*

▣ Rezumat

Operatorii de date cu caracter personal (art. 4 pct. 7 GDPR) au obligațiile de informare și notificare în cazul încălcării art. 33, 34 GDPR. Conform art. 33 GDPR, încălcarea dispozițiilor privind protecția datelor cu caracter personal trebuie notificată autorității de supraveghere de îndată ce se ia cunoștință de incident. Obligația de notificare nu este aplicabilă în situația în care nu se preconizează că drepturile și libertățile persoanelor sunt expuse unui risc. Pe de altă parte, atunci când există un risc ridicat, persoanele vizate trebuie să fie informate fără întârziere. Prezentul articol tratează anumite probleme de interpretare, astfel după cum sunt ridicate în Germania.

Cuvinte-cheie: GDPR; obligația de informare; art. 33 GDPR; art. 34 GDPR; obligația de notificare.

▣ Abstract

Controllers (art. 4 par. 7 GDPR) have the obligation to inform and notify in the event of a breach of art. 33, 34 GDPR. According to art. 33 GDPR, a violation of the

* Prof. dr. prof. h.c. Jürgen Taeger este titular la catedra de drept civil, drept comercial și de afaceri, precum și director al Centrului interdisciplinar pentru drept (CRI) al Universității Carl von Ossietzky Oldenburg. Este profesor de onoare la Universitatea Babeș-Bolyai Cluj-Napoca (BBU), care i-a acordat titlul de profesor honoris causa. La BBU organizează anual împreună cu prof. dr. Med. Mihaela Drăgan și avocatul conf. univ. dr. Ciprian Păun „Conferința germano-română privind dreptul informațional european”.

De asemenea, lucrează ca Of Counsel la firma de avocatură DLA Piper UK LLP și oferă consultanță companiilor în principal în probleme de protecție a datelor.

Taeger este co-redactor al comentariului Taeger / Gabel (ed.), RPDCP LFPD, Frankfurt / M. din anul 2019.

protection of personal data must be reported to the responsible supervisory authority immediately after becoming known. The obligation to inform is not applicable in the event that the violation is not likely to endanger the rights and freedoms of individuals. On the other hand, if there is a high risk, data subjects must be informed without delay. The present article deals with some of the existing questions of interpretation, as they are discussed in Germany.

Keywords: GDPR; obligation to communicate; art. 33 GDPR; art. 34 GDPR; obligation to notify.

Persoanele responsabile (art. 4 pct. 7 GDPR) au obligațiile de informare și notificare în cazul încălcării art. 33, 34 GDPR. Conform art. 33 GDPR, încălcarea dispozițiilor privind protecția datelor cu caracter personal trebuie notificată autorității de supraveghere de îndată ce se ia cunoștință de incident. Obligația de notificare nu este aplicabilă în situația în care nu se preconizează că drepturile și libertățile persoanelor sunt expuse unui risc. Pe de altă parte, atunci când există un risc ridicat, persoanele vizate trebuie să fie informate fără întârziere. Prezentul articol tratează anumite probleme de interpretare, astfel după cum sunt ridicate în Germania.

I. Reglementarea în materia obligațiilor de informare și notificare

O prevedere similară cu cea a art. 33, 34 GDPR există încă din anul 2009, anume §42a din Legea federală privind protecția datelor (versiunea veche a LFPD), care a fost abrogată odată cu implementarea noii reglementări privind Regulamentul privind protecția datelor cu caracter personal (GDPR). Dispoziția anterioară se diferenția de actuala reglementare GDPR prin faptul că nu prevedea obligația de informare persoanelor vizate și a autorității de supraveghere în cazul încălcării protecției datelor cu caracter personal. Cu toate acestea, nu era exclusă obligația de informare cu privire la incidența unui risc scăzut pentru persoanele vizate, cum este abordat în actuala reglementare GDPR¹.

Dispoziția are ca model Data Breach Laws din dreptul Statelor Unite² și art. 4 alin. (3) pct. 1 din Directiva UE ePrivacy³. De asemenea, reglementările privind încălcarea protecției datelor au fost cunoscute în Irlanda⁴ și Italia⁵.

O obligație de informare a autorităților de prevenire și de aplicare a legii este cuprinsă în art. 30 JIRL, în Germania, în § 65 din noua Lege privind protecția datelor. Suplimentar există reglementări specific referitoare la încălcarea secretului fiscal în Codul fiscal (CF) și a celui social în Codul social (CS X).

¹ A se vedea *Gabel*, în: Taeger/Gabel, LFPD, ediția a doua., 2019, § 4a alin. (7) urm.; *Hanloser*, CCZ 2010, 25; *Conrad*, în: Auer-Reinsdorff/Conrad, Handbuch IT – und Datenschutzrecht, ed. a treia, 2019, § 34 alin. (697).

² <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

³ *Spies*, MMR 2008, H. 5, XIX; similare cu consecințele pozitive din SUA *Dix*, în: *Simitis/Hornung/Spiecker* gen. *Döhm*, *Datenschutzrecht*, 2019, art. 33 alin. (1).

⁴ https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.

⁵ <https://www.garantepriacy.it/documents/10160/0/All+B+al+Prov.+513+del+12+novem+bre+2014+Mod.+segnalazione+data+breach.pdf>.

În cazul accesului neautorizat la sistemele de telecomunicații și ale procesării datelor utilizatorilor există obligații de notificare către Agenția Federală a Rețelelor ca autoritate de supraveghere care incumba furnizorilor de servicii de telecomunicații.

În situația în care există alte obligații de notificare a încălcărilor care deservește alte scopuri, de exemplu securitatea datelor, cum ar fi cf. § 8b alin. (4) din Actului federal privind securitatea în tehnologia informației (AFSIT), acestea sunt suplimentare obligației de notificare conform art. 33 GDPR⁶.

Notificările către autoritățile de supraveghere în baza obligației de informare prevăzute în § 42 teza 1 din reglementarea veche a LFPD erau foarte rare. Acest caz nu este cauzat numai de faptul că obligația de notificare se aplica numai în condițiile unui risc ridicat, rezultat dintr-o descoperire nelegală cu privire la diverse date cu caracter sensibil. De asemenea, este esențial ca sensibilitatea autorităților competente să fie evident subdezvoltată cu privire la sancțiuni pecuniare scăzute. Altfel este dificil de explicat de ce numărul notificărilor a crescut odată cu intrarea în vigoare a GDPR. În perioada 25 mai 2018 – sfârșitul lunii ianuarie 2019 s-au înregistrat 12600 de notificări către autoritățile de supraveghere germane, cu 59000 mai multe decât în UE în primele opt luni de la intrarea în vigoare a GDPR⁷.

În regiunea Nordrhein-Westfalen numărul notificărilor a crescut de 20 de ori⁸. Comisarul de state pentru protecția datelor și libertatea de informare a primit pe tot parcursul anului 2017 numai 60 de notificări în baza § 42a LFPD (reglementarea veche); din ianuarie până în mai au fost, de asemenea, numai 61 de notificări. Dar după acestea notificările privind incidentele de date și atacurile specifice au crescut semnificativ: din mai până în decembrie 2018 au fost mai mult de 1200⁹. Statistici similare sunt întâlnite și cu referire la celelalte landuri. Un motiv pentru această creștere ar putea fi constituit de obligația de notificare extinsă comparativ cu LFPD (variantea veche), dar, în mod special, efectul sensibilizant al amenințărilor cu amenzi ridicate.

Numai în Regatul Țărilor de Jos s-au înregistrat în aceeași perioadă cu 15400 mai multe notificări, în ciuda populației semnificativ de reduse. Cu toate acestea, în Spania au fost raportate numai 670 de cazuri, în România numai 260, iar în Grecia doar 70 de cazuri¹⁰. Cauza pentru aceste discrepanțe majore dintre statele membre nu a fost investigată pe deplin nici până în prezent.

⁶ *Schultze-Melling*, în: Taeger/Gabel, RPDCP LFPD, ediția a treia, 2019, art. 33 alin. (5); *Reif*, în: Gola, RP-DCP, art. 33 alin. (15); *Brink*, în: Wolff/Brink, BeckOK Datenschutzrecht, art. 33 alin. (18). A se vedea art. 14 pct. 3 NIS-RL, Directiva (UE) 2016/1148 des Europ. Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. EU 2016, L 194/1, für Betreiber wesentlicher Dienste.

⁷ DLA Piper GDPR Data Breach Survey, Februar 2019, <https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/>.

⁸ *Brink/Kranig*, PinG 2019, 104.

⁹ 24. Datenschutzbericht des LDI NRW, 13.

¹⁰ Alle Angaben aus DLA Piper GDPR Data Breach Survey vom Februar 2019, <https://www.dlapiper.com/~media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf>.

II. Obligația de a notifica autoritatea de supraveghere și excepția de la aceasta

Responsabilul cu protecția datelor trebuie să raporteze fiecare „încălcare a protecției datelor cu caracter personal”. Prin aceasta se înțelege conform definiției legale din art. 4 pct. 12 GDPR „încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod”¹¹. Nu trebuie notificate alte încălcări ale obligațiilor din cadrul RPDCP sau ale altor legi privind protecția datelor cum ar fi prelucrarea datelor cu caracter personal fără o bază legală sau nerespectarea obligațiilor de informare¹².

Obligația de notificare se naște odată cu încălcarea protecției datelor. Termenul de notificare curge de la momentul cunoașterii incidentului privind încălcarea protecției datelor. De îndată ce operatorul are informații reale că există o probabilitate foarte ridicată ca încălcarea să se fi petrecut, trebuie efectuată notificarea. În ceea ce privește detaliile despre încălcarea protecției datelor, aplicarea măsurilor suplimentare de limitare a riscurilor, care pot influența măsurile autorității de supraveghere, acestea pot fi raportate ulterior [alin. (4)].

1. Condiția efectuării notificării: riscul suficient de concret

Cerința pentru efectuarea notificării nu constituie ca încălcarea să fie cauzată de operatorul cu intenție, fără temei juridic sau din culpă¹³. Sunt adresate incidentele de Securitate, mai concret o încălcare a confidențialității, a disponibilității și a integrității datelor. Scopul notificării încălcării securității datelor cu caracter personal este „să se flancheze cerințele legale de fond la nivel de securitate IT”¹⁴ și să se asigure gradul necesar de securitate IT¹⁵. Un incident de securitate se poate produce chiar dacă sunt luate cele mai înalte măsuri de precauție în materie de securitate și în tratarea datelor cu caracter personal¹⁶; însă și din cauza încălcării măsurilor tehnice și organizatorice necesare în temeiul art. 32 GDPR pentru asigurarea securității datelor. Astfel, rămâne încă de discutat interzicerea utilizării informațiilor de importanță obținute de către o autoritate de supraveghere în urma notificării.

Obligația de a raporta o încălcare a securității datelor din cauza unei „incident” sau a unui atac extern reprezintă acum regula indiferent de natura datelor, deși există o excepție semnificativă („prag material de notificare”¹⁷). În consecință, aceasta nu este

¹¹ Informativ *Jandt*, în: Kühling/Buchner, RP-DCP /LFPD, 2. Aufl., 2018, art. 33 alin. (6) urm.

¹² Vgl. *Franck*, în: Schwartmann/Jaspers/Thüsing/Kugelman, RP-DCP /LFPD, art. 33 alin. (89), (97). Unklar *Weichert*, în: Däubler/Wedde/Weichert/Sommer, EU-RP-DCP und LFPD-neu, 2018, art. 33 alin. (18).

¹³ *Reif*, în: Gola, RP-DCP, 2018, art. 33 alin. (23); *Marschall*, DuD 2015, 183 (184).

¹⁴ *Marschall*, DuD 2015, 183 (184), unter Hinweis auf *Hanloser*, MMR 2010, 300 (301).

¹⁵ Ausführl. mit Beispielen *Franck*, în: Schwartmann/Jaspers/Thüsing/Kugelman, RP-DCP /LFPD, 2018, art. 33 alin. (30); *Schreibauer/Spittka*, în: Wybitul, Handbuch EU-Datenschutz grundverordnung, art. 33 alin. (13) urm.; *Hladjk*, în: Ehmann/Selmayr, RP-DCP, art. 33 alin. (5) și urm.

¹⁶ A se vedea etwa *Schreibauer/Spittka*, în: Wybitul, Handbuch EU-Datenschutzgrundverordnung, 2017, art. 33 alin. (12). Unklar *Gierschmann*, în: Gierschmann et al., RP-DCP, art. 33 alin. (23), nach der eine Meldepflicht ausgelöst wird, wenn „Maßnahmen ... verletzt wurden”.

¹⁷ *Dix*, în: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, art. 33 alin. (6).

necesară dacă încălcarea „este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice” (excepție de rezervă¹⁸). Considerentul 85 clarifică faptul că trebuie puse în prim plan, în conformitate cu scopul regulamentului, riscurile pentru interesele persoanei vizate în caz de discriminare, furt de identitate sau fraudă, pierderi financiare, vătămare reputațională, pierderea confidențialității datelor cu caracter personal supuse secretului profesional, eliminarea neautorizată a pseudonimizării sau alte dezavantaje economice sau sociale semnificative. Prin stabilirea cerințelor de protecție și analiza riscurilor¹⁹, trebuie să se evalueze gradul de apariție și probabilitatea apariției riscului unei încălcări a criteriilor de securitate a confidențialității, integrității și disponibilității datelor ca obiective de protecție conform art. 32 GDPR²⁰. Evaluarea riscurilor trebuie să fie realistă și poate exclude riscurile rare²¹. Dacă datele sunt pierdute iremediabil, nu există nicio obligație de a notifica dacă datele au avut relevanță numai pentru persoana responsabilă, iar persoana vizată nu își riscă drepturile și libertățile personale²².

În ceea ce privește gradul de dificultate (calitatea riscului), *Schultze-Melling*²³ reliefează că „un risc suficient de concret pentru drepturile și libertățile persoanelor fizice există atunci dacă, pe baza unei opinii pe cât posibil de obiective, dezavantajele menționate sunt amenințate, de fapt, cu o consecință echivalentă și adecvată raportată la evenimentele care au avut loc și că o asemenea considerație poate fi menținută chiar și în contextul obiectivului de protecție”. Prin urmare, obligația de notificare este declanșată numai dacă, dincolo de suspiciuni, există și dovezi reale ale unui prejudiciu iminent²⁴. Din acest moment începe să curgă termenul care este încă discutabil.

Obligația de notificare a unui risc în curs de declanșare poate să se nască, dacă un laptop cu informații personale este pierdut, ale cărui date stocate sunt însă criptate, astfel încât evenimentul pierderii informațiilor persoanei vizate este puțin probabil dacă există o copie de rezervă datelor²⁵. Cu toate acestea, această abordare este controversată: potrivit unei alte opinii, dar neconvingătoare, există obligația de a notifica în ciuda criptării datelor²⁶. Perspectiva art. 34 alin. (3) lit. a) GDPR este mai degrabă de luat

¹⁸ *Martini*, în: Paal/Pauly, RP-DCP, 2. Aufl., 2018, art. 33 alin. (21).

¹⁹ Dazu ausführlich *Conrad*, în: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 33 alin. (180) și urm.

²⁰ A se vedea Considerentele 46 și 47 RPDCP, precum și ghidul Bayer. LB für den Datenschutz, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen (öffentlicher Stellen), Erläuterungen zu Art. 33 und 34 Datenschutz-Grundverordnung Orientierungshilfe, v. 1.6.2019. Vgl. auch *Martini*, în: Paal/Pauly, RP-DCP, art. 33 alin. (22) f.

²¹ Ähnlich *Martini*, în: Paal/Pauly, RP-DCP, art. 33 alin. (27).

²² *Gierschmann*, în: Gierschmann et al., RP-DCP, art. 33 alin. (30).

²³ *Schultze-Melling*, în: Taeger/Gabel, RPDCP LFPD, art. 33 alin. (21).

²⁴ *Jandt*, în: Kühling/Buchner, RP-DCP LFPD, art. 33 alin. (15); *Gierschmann*, în: Gierschmann et al., RP-DCP, art. 33 alin. (24); *Dix*, în: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, art. 33 alin. (7) („hinreichende Kenntnis”).

²⁵ So auch *Laue*, în: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl., 2019, § 7 alin. (45), și cu exemplele următoare *Schultze-Melling*, în: Taeger/Gabel, RPDCP LFPD, art. 33 alin. (24) f., art. 29-Datenschutzgruppe, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250rev.01, 8 urm., și *EDPS*, Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten für die Organe und Einrichtungen der Europäischen Union, 11, 18-12-14_edps_guidelines_data_breach_de.

²⁶ A se vedea etwa *Franck*, în: Schwartmann/Jaspers/Thüsing, RP-DCP /LFPD, art. 33 RP-DCP, alin. (38); *Dix*, în: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, art. 33 alin. (12).

în considerare, conform căreia „operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea”; pentru că, dacă obligația de a anunța persoanele vizate poate fi deja eliminată în cazul în care incidentul poate fi asociat unui risc ridicat, astfel în mod corect ar trebui să se aplice și în cazul unui risc mai puțin grav. În consecință, în ceea ce privește pierderea de date suficient de criptate conform stadiului tehnicii anterioare, nu există nicio obligație de notificare²⁷ dacă datele sunt încă disponibile în altă parte, cum ar fi într-un sistem de arhivă²⁸.

2. Abordarea bazată pe risc și marja de apreciere

Conform abordării GDPR bazată pe riscuri, responsabilitatea operatorului este de a efectua această evaluare²⁹, Chiar dacă rezultatul evaluării relevă că nu există niciun risc, anume certitudine absența unui risc³⁰ și, prin urmare, notificarea nu este necesară, evenimentul și evaluarea riscului trebuie totuși investigate³¹, dacă este posibil și cu un aviz din partea ofițerului responsabil cu protecția datelor, care, în contextul atribuțiilor sale în temeiul art. 39 GDPR, urmărește să supravegheze respectarea GDPR și să îi sfătuiască pe cei responsabili. Aceasta corespunde principiului răspunderii din art. 5 GDPR.

În situații-limită există o marjă de apreciere conform căreia autoritatea de supraveghere trebuie să respecte și să se abțină de la o amendă în orice altă evaluare sau cel puțin să stabilească cuantumul amenzii foarte scăzut dacă consideră că ar fi trebuit să se facă o notificare. Din acestea rezultă că, atunci când operatorii evaluează cu precauție riscurile, ei sunt mai susceptibili să raporteze un incident, decât ca autoritatea de supraveghere să cunoască pe altă cale incidentul și să decidă că ar fi trebuit să se efectueze notificarea și apoi să se aplice o amendă pentru încălcarea acestei obligații. Ar fi de dorit ca autoritățile naționale de supraveghere și Consiliul european pentru protecția datelor (CEPD) să furnizeze criteriile de evaluare a riscurilor pentru a-i ajuta pe operatori să identifice atunci când este necesară notificarea.

Poziția autorităților de supraveghere, dintre care 17 din sistemul federal al Germaniei, nu este uniformă cu privire la aplicarea obligației de notificare. Ar trebui să fie o practică bună să i se ofere operatorilor o comunicare a situației inițiale și finale. În funcție de relevanța incidentului, pot fi efectuate alte controale de către autoritățile de supraveghere prin anchete sau audituri la fața locului pentru a determina eliminarea riscurilor.

²⁷ Altă perspectivă *Eusani*, DS 2019, 18 (29).

²⁸ So die h. M. in der Literatur und bei den Aufsichtsbehörden, vgl. *Pohl*, PinG 2019, 100 (101); *Kasner*, PinG 2019, 111 (113); *Bergt*, DuD 2017, 555 (560); *Reif*, în: Gola, RP-DCP, 2018, art. 33 alin. (29); *Grages*, în: Plath, RP-DCP /LFPD, 3. Aufl., 2018, art. 33 alin. (6); *Gierschmann*, în: *Gierschmann u. a.*, RP-DCP, art. 33 alin. (32); *Wilhelm*, în: *Sydow*, EU-RPDCP, 2018, art. 33 alin. (8), (9); *Brink/Kranig*, PinG 2019, 104 (105); *EDSA*, DL 250 rev.01, 22; *HH DSB*, Data-Breach-Meldungen nach Art. 33 RP-DCP, 4.

²⁹ *Schultze-Melling*, în: *Taeger/Gabel*, RPDCP LFPD, art. 33 alin. (19); *Gierschmann*, în: *Gierschmann et al.*, RP-DCP, art. 33 alin. (32), § 42 LFPD alin. (19) și urm.; *Veil*, ZD 2015, 347.

³⁰ *Zu der Prognoseentscheidung Martini*, în: *Paal/Pauly*, RP-DCP, art. 33 alin. (26), und *Brink*, în: *Wolff/Brink*, art. 33 alin. (38).

³¹ Pentru obligațiile de documentare după *Dix*, în: *Simitis/Hornung/Spiecker gen. Döhmman*, Datenschutzrecht, art. 33 alin. (23).

III. Comunicarea către persoanele vizate

Depinde de rezultatul analizei de evaluare a riscului dacă, pe lângă notificarea autorității de supraveghere, trebuie informată și persoana vizată. Operatorul trebuie să o informeze și pe aceasta doar dacă încălcarea protecției datelor cu caracter personal „poate implica un risc ridicat pentru drepturile și libertățile personale ale persoanelor fizice” [art. 34 alin. (1) GDPR]. Cu cât este mai ridicat potențialul prejudiciu, cu atât scade pragul privind probabilitatea de apariție. Evaluarea se poate baza pe standardele de evaluare prevăzute de Directiva UE ePrivacy³².

Cu toate acestea art. 34 GDPR prevede o comunicare „imediată”. Cu toate acestea, referințele din considerentul 86 arată că trebuie să existe alte elemente de control pentru a determina „imparțialitatea” față de art. 33 GDPR. Conform considerentului 86, comunicările trebuie făcute „în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorități competente, cum ar fi autoritățile de aplicare a legii”. Conform considerentului 86 teza 3, trebuie menționat că persoanele vizate trebuie informate imediat pentru a putea reduce riscul unui prejudiciu direct. Cu toate acestea, o perioadă mai lungă până la comunicare poate fi justificată dacă în primul rând „trebuie luate măsuri adecvate împotriva încălcărilor continue sau comparabile ale protecției datelor cu caracter personal”. Există așteptarea ca comunicarea să se realizeze pe cât posibil de rapid.

Notificarea ar trebui să fie făcută într-un limbaj clar și simplu [art. 34 alin. (2) GDPR], astfel încât persoana în cauză să poată evalua corect orice risc și să ia măsuri adecvate pentru a preveni prejudiciul. Cu toate acestea, în conformitate cu alin. (3), există trei excepții, potrivit cărora nu trebuie făcută o comunicare. În primul rând, cf. lit. a) obligația de a informa persoanele vizate dacă au fost luate măsuri tehnice și organizatorice adecvate pentru a împiedica accesul terților la date. Conform lit. b) operatorul poate renunța la comunicare dacă, ulterior, ia măsuri prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate *nu mai este* susceptibil să se materializeze. Chiar dacă operatorul este în principiu obligat să informeze toate persoanele vizate în mod individual cu privire la risc, informarea individuală conform lit. c) este înlocuită de un anunț public sau o altă difuzare efectivă a informațiilor dacă informarea individuală este disproporționată din cauza numărului foarte mare de persoane afectate sau a lipsei informației cu privire la adresă.

IV. Beneficiarul obligației de notificare

Notificarea intră în sarcina operatorului în sensul art. 4 pct. 7 GDPR. Pentru operatorii asociați [art. 26 alin. (1) GDPR], este evident că operatorul cărui îi incumbă obligația de notificare este cel în a cărui arie de responsabilitate a avut loc incidentul. Deoarece, în caz de incertitudine, un alt operator poate fi considerat de autoritatea de supraveghere ca fiind responsabilă pentru raportarea încălcării datelor, acordul care va fi încheiat în conformitate cu art. 26 trebuie să reglementeze în mod explicit responsabilitățile, obligațiile, termenele și sancțiunile și să distribuie riscul între părțile

³² A se vedea catalogul de criterii al art. 29-Grupa privind protecția datelor în DL 250 Rev.01.

responsabile³³. Fără un acord în acest sens, ei răspund în solidar pentru îndeplinirea obligației de notificare³⁴.

Dacă un împuternicit cu prelucrarea datelor a dobândit deja cunoștințe despre o încălcare a protecției datelor cu caracter personal din aria sa, acesta trebuie să informeze imediat clientul fără nici o investigație sau evaluare³⁵, deoarece evaluarea riscurilor și notificarea sunt întră în sarcina clientului. Cu informațiile primite de la împuternicitul cu prelucrarea datelor, operatorul a luat cunoștință de incidentul produs la procesator, care este atribuit operatorului de atunci și, ca urmare, trebuie să fie raportat de acesta autorității de supraveghere. La notificarea unui incident, se urmărește consultarea strânsă cu împuternicitul cu prelucrarea datelor pentru a lua măsuri pentru a evita prejudiciul.

În cazul activităților transfrontaliere ale operatorului cu sucursale în diferite state membre ale UE, dacă notificarea este transmisă către o autoritate de supraveghere, alta decât cea prevăzută de art. 55 GDPR, se prezumă ca și când nu ar fi avut loc. Este responsabilitatea operatorului să constate sau să se intereseze despre aria de competență³⁶. Cu toate acestea, autoritatea de supraveghere lipsită de competență ar trebui să facă o trimitere la autoritatea competentă sau să o transmită imediat autorității competente. Procedura ar trebui să fie coordonată de autoritățile de supraveghere, cu excepția cazului în care CEPD oferă îndrumări³⁷.

V. Conținutul și forma notificării și a comunicării

Informațiile care trebuie furnizate autorității de supraveghere rezultă din art. 33 alin. (3) GDPR. Autoritățile de supraveghere din Germania și România³⁸ au la dispoziție formulare electronice pe site-urile lor web, cu ajutorul cărora conținutul esențial poate fi specificat și completat cu text nepredefinit. Dacă, așa cum s-a întâmplat, situl web al autorității de supraveghere este perturbat și notificarea formularului disponibil nu este posibil în altă modalitate, informațiile cerute de art. 33 RPDCP trebuie să fie comunicate informal, dacă este necesar prin telefon. Mesajele prin e-mail trebuie criptate.

În practică, este comună furnizarea de informații suplimentare într-o scrisoare de întâmpinare, anume referitoare la nașterea și desfășurarea incidentului raportabil ca urmare a investigațiilor și măsurile care au fost luate pentru a preveni prejudicierea celor afectați și pentru a preveni repetarea acestora.

Art. 34 alin. (2) GDPR îi ține pe operatori să comunice persoanelor vizate „într-un limbaj clar și simplu natura încălcării protecției datelor cu caracter personal”, cel puțin informații și recomandări dispuse prin prevederile art. 33 alin. (3) lit. b), lit. c) și lit. d). Această cerință este justificată în plus de considerentul 86. Acesta prevede că notificarea ar trebui să conțină „o descriere a naturii încălcării datelor cu caracter personal și recomandări adresate persoanei fizice în cauză pentru a diminua efectele adverse ale acestei încălcări”.

³³ Zutreffend *Schultze-Melling*, în: Taeger/Gabel, RPDCP LFPD, art. 33 alin. (40).

³⁴ Ebenso *Martini*, în: Paal/Pauly, RPDCP LFPD, art. 33 alin. (14).

³⁵ DL 250 rev.01, 15.

³⁶ *Franck*, în: Schwartmann/Jaspers/Thüsing/Kugelmann, RP-DCP /LFPD, art. 33 alin. (56).

³⁷ A se vedea *Jandt*, în: Kühling/Buchner, RP-DCP /LFPD, art. 33 alin. (17).

³⁸ https://www.dataprotection.ro/formulare/formularBresaGdpr.do?action=view_action&newFormular=tru.