CUPRINS

OPINII

SECTORIAL

STUDII DE CAZ

MONITORUL PROTECŢIEI DATELOR

Obligaţia de informare şi de notificare în cazul încălcării securităţii 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 obligaţiile de informare şi notificare în cazul încălcării art. 33, 34 GDPR. Conform art. 33 GDPR, încălcarea dispoziţiilor privind protecţia datelor cu caracter personal trebuie notificată autorităţii de supraveghere de îndată ce se ia cunoştinţă de incident. Obligaţia de notificare nu este aplicabilă în situaţia în care nu se preconizează că drepturile şi libertăţile 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; obligaţia de informare; art. 33 GDPR; art. 34 GDPR; obligaţia 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 şi de afaceri, precum şi director al Centrului interdisciplinar pentru drept (CRI) al Universităţii Carl von Ossietzky Oldenburg. Este profesor de onoare la Universitatea Babeş-Bolyai Cluj-Napoca (BBU), care i-a acordat titlul de profesor honoris causa. La BBU organizează anual împreună cu prof. dr. Med. Mihaela Drăgan şi avocatul conf. univ. dr. Ciprian Păun „Conferinţa germano-română privind dreptul informaţional european".

De asemenea, lucrează ca Of Counsel la firma de avocatură DLA Piper UK LLP şi oferă consultanţă companiilor în principal în probleme de protecţie 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 obligaţiile de informare şi notificare în cazul încălcării art. 33, 34 GDPR. Conform art. 33 GDPR, încălcarea dispoziţiilor privind protecţia datelor cu caracter personal trebuie notificată autorităţii de supraveghere de îndată ce se ia cunoştinţă de incident. Obligaţia de notificare nu este aplicabilă în situaţia în care nu se preconizează că drepturile şi libertăţile 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 obligaţiilor de informare şi notificare

O prevedere similară cu cea a art. 33, 34 GDPR există încă din anul 2009, anume §42a din Legea federală privind protecţia datelor (versiunea veche a LFPD), care a fost abrogată odată cu implementarea noii reglementări privind Regulamentul privind protecţia datelor cu caracter personal (GDPR). Dispoziţia anterioară se diferenţia de actuala reglementare GDPR prin faptul că nu prevedea obligaţia de informare persoanelor vizate şi a autorităţii de supraveghere în cazul încălcării protecţiei datelor cu caracter personal. Cu toate acestea, nu era exclusă obligaţia de informare cu privire la incidenţa unui risc scăzut pentru persoanele vizate, cum este abordat în actuala reglementare GDPR[1].

Dispoziţia are ca model Data Breach Laws din dreptul Statelor Unite[2] şi art. 4 alin. (3) pct. 1 din Directiva UE ePrivacy[3]. De asemenea, reglementările privind încălcarea protecţiei datelor au fost cunoscute în Irlanda[4] şi Italia[5].

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

---

[1] A se vedea *Gabel*, în: Taeger/Gabel, LFPD, ediţia 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 consecinţele pozitive din SUA *Dix*, în: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, art. 33 alin. (1).

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

[5] https://www.garanteprivacy.it/documents/10160/0/All+B+al+Provv.+513+del+12+novembre+2014+Mod.+segnalazione+data+breach.pdf.

În cazul accesului neautorizat la sistemele de telecomunicaţii şi ale procesării datelor utilizatorilor există obligaţii de notificare către Agenţia Federală a Reţelelor ca autoritate de supraveghere care incumba furnizorilor de servicii de telecomunicaţii.

În situaţia în care există alte obligaţii de notificare a încălcărilor care deservesc alte scopuri, de exemplu securitatea datelor, cum ar fi cf. § 8b alin. (4) din Actului federal privind securitatea în tehnologia informaţiei (AFSIT), acestea sunt suplimentare obligaţiei de notificare conform art. 33 GDPR[6].

Notificările către autorităţile de supraveghere în baza obligaţiei de informare prevăzute în § 42 teza 1 din reglementarea veche a LFPD erau foarte rare. Acest caz nu este cauzat numai de faptul că obligaţia de notificare se aplica numai în condiţiile unui risc ridicat, rezultat dintr-o descoperire nelegală cu privire la diverse date cu caracter sensibil. De asemenea, este esenţial ca sensibilitatea autorităţilor competente să fie evident subdezvoltată cu privire la sancţiuni 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 – sfârşitul lunii ianuarie 2019 s-au înregistrat 12600 de notificări către autorităţile de supraveghere germane, cu 59000 mai multe decât în UE în primele opt luni de la intrarea în vigoare a GDPR[7].

În regiunea Nordrhein-Westfalen numărul notificărilor a crescut de 20 de ori[8]. Comisarul de state pentru protecţia datelor şi 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 şi atacurile specifice au crescut semnificativ: din mai până în decembrie 2018 au fost mai mult de 1200[9]. Statistici similare sunt întâlnite şi cu referire la celelalte landuri. Un motiv pentru această creştere ar putea fi constituit de obligaţia de notificare extinsă comparativ cu LFPD (varianta veche), dar, în mod special, efectul sensibilizant al ameninţărilor cu amenzi ridicate.

Numai în Regatul Ţărilor de Jos s-au înregistrat în aceeaşi perioadă cu 15400 mai multe notificări, în ciuda populaţiei 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 cazuri[10]. Cauza pentru aceste discrepanţe majore dintre statele membre nu a fost investigată pe deplin nici până în prezent.

---

[6] *Schultze-Melling*, în: Taeger/Gabel, RPDCP LFPD, ediţia 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 Infomationssystemen în 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. Obligaţia de a notifica autoritatea de supraveghere şi excepţia de la aceasta

Responsabilul cu protecţia datelor trebuie să raporteze fiecare „încălcare a protecţiei datelor cu caracter personal". Prin aceasta se înţelege conform definiţiei legale din art. 4 pct. 12 GDPR „încălcare a securităţii 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 obligaţiilor din cadrul RPDCP sau ale altor legi privind protecţia datelor cum ar fi prelucrarea datelor cu caracter personal fără o bază legală sau nerespectarea obligaţiilor de informare[12].

Obligaţia de notificare se naşte odată cu încălcarea protecţiei datelor. Termenul de notificare curge de la momentul cunoaşterii incidentului privind încălcarea protecţiei datelor. De îndată ce operatorul are informaţii reale că există o probabilitate foarte ridicată ca încălcarea să se fi petrecut, trebuie efectuată notificarea. În ceea ce priveşte detaliile despre încălcarea protecţiei datelor, aplicarea măsurilor suplimentare de limitare a riscurilor, care pot influenţa măsurile autorităţii de supraveghere, acestea pot fi raportate ulterior [alin. (4)].

1. Condiţia efectuării notificării: riscul suficient de concret

Cerinţa pentru efectuarea notificării nu constituie ca încălcarea să fie cauzată de operatorul cu intenţie, fără temei juridic sau din culpă[13]. Sunt adresate incidentele de Securitate, mai concret o încălcare a confidenţialităţii, a disponibilităţii şi a integrităţii datelor. Scopul notificării încălcării securităţii datelor cu caracter personal este „să se flancheze cerinţele legale de fond la nivel de securitate IT"[14] şi să se asigure gradul necesar de securitate IT[15]. Un incident de securitate se poate produce chiar dacă sunt luate cele mai înalte măsuri de precauţie în materie de securitate şi în tratarea datelor cu caracter personal[16]; însă şi din cauza încălcării măsurilor tehnice şi organizatorice necesare în temeiul art. 32 GDPR pentru asigurarea securităţii datelor. Astfel, rămâne încă de discutat interzicerea utilizării informaţiilor de importanţă obţinute de către o autoritate de supraveghere în urma notificării.

Obligaţia de a raporta o încălcare a securităţii datelor din cauza unei „incident" sau a unui atac extern reprezintă acum regula indiferent de natura datelor, deşi există o excepţie semnificativă („prag material de notificare"[17]). În consecinţă, 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/Kugelmann, 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/Kugelmann, 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) şi urm.

[16] A se vedea etwa *Schreibauer/Spittka*, în: Wybitul, Handbuch EU-Datenschutzgrun dverordnung, 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. Döhmann, Datenschutzrecht, art. 33 alin. (6).

necesară dacă încălcarea „este puţin probabil să genereze un risc pentru drepturile şi libertăţile persoanelor fizice" (excepţie de rezervă[18]). 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 reputaţională, pierderea confidenţialităţii datelor cu caracter personal supuse secretului profesional, eliminarea neautorizată a pseudonimizării sau alte dezavantaje economice sau sociale semnificative. Prin stabilirea cerinţelor de protecţie şi analiza riscurilor[19], trebuie să se evalueze gradul de apariţie şi probabilitatea apariţiei riscului unei încălcări a criteriilor de securitate a confidenţialităţii, integrităţii şi disponibilităţii datelor ca obiective de protecţie conform art. 32 GDPR[20]. Evaluarea riscurilor trebuie să fie realistă şi poate exclude riscurile rare[21]. Dacă datele sunt pierdute iremediabil, nu există nicio obligaţie de a notifica dacă datele au avut relevanţă numai pentru persoana responsabilă, iar persoana vizată nu îşi riscă drepturile şi libertăţile personale[22].

În ceea ce priveşte gradul de dificultate (calitatea riscului), *Schultze-Melling*[23] reliefează că „un risc suficient de concret pentru drepturile şi libertăţile persoanelor fizice există atunci dacă, pe baza unei opinii pe cât posibil de obiective, dezavantajele menţionate sunt ameninţate, de fapt, cu o consecinţă echivalentă şi adecvată raportată la evenimentele care au avut loc şi că o asemenea consideraţie poate fi menţinută chiar şi în contextul obiectivului de protecţie". Prin urmare, obligaţia de notificare este declanşată numai dacă, dincolo de suspiciuni, există şi dovezi reale ale unui prejudiciu iminent[24]. Din acest moment începe să curgă termenul care este încă discutabil.

Obligaţia de notificare a unui risc în curs de declanşare poate să se nască, dacă un laptop cu informaţii personale este pierdut, ale cărui date stocate sunt însă criptate, astfel încât evenimentul pierderii informaţiilor persoanei vizate este puţin probabil dacă există o copie de rezervă datelor[25]. Cu toate acestea, această abordare este controversată: potrivit unei alte opinii, dar neconvingătoare, există obligaţia de a notifica în ciuda criptării datelor[26]. 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) şi urm.

[20] A se vedea Considerentele 46 şi 47 RPDCP, precum şi 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), şi 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., şi *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 protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii 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 obligaţia de a anunţa 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 şi în cazul unui risc mai puţin grav. În consecinţă, în ceea ce priveşte pierderea de date suficient de criptate conform stadiului tehnicii anterioare, nu există nicio obligaţie de notificare[27] dacă datele sunt încă disponibile în altă parte, cum ar fi într-un sistem de arhivă[28].

2. Abordarea bazată pe risc şi marja de apreciere

Conform abordării GDPR bazată pe riscuri, responsabilitatea operatorului este de a efectua această evaluare[29], Chiar dacă rezultatul evaluării relevă că nu există niciun risc, anume certitudine absenţa unui risc[30] şi, prin urmare, notificarea nu este necesară, evenimentul şi evaluarea riscului trebuie totuşi investigate[31], dacă este posibil şi cu un aviz din partea ofiţerului responsabil cu protecţia datelor, care, în contextul atribuţiilor sale în temeiul art. 39 GDPR, urmăreşte să supravegheze respectarea GDPR şi să îi sfătuiască pe cei responsabili. Aceasta corespunde principiului răspunderii din art. 5 GDPR.

În situaţii-limită există o marjă de apreciere conform căreia autoritatea de supraveghere trebuie să respecte şi să se abţină de la o amendă în orice altă evaluare sau cel puţin 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 precauţie riscurile, ei sunt mai susceptibili să raporteze un incident, decât ca autoritatea de supraveghere să cunoască pe altă cale incidentul şi să decidă că ar fi trebuit să se efectueze notificarea şi apoi să se aplice o amendă pentru încălcarea acestei obligaţii. Ar fi de dorit ca autorităţile naţionale de supraveghere şi Consiliul european pentru protecţia datelor (CEPD) să furnizeze criterii de evaluare a riscurilor pentru a-i ajuta pe operatori să identifice atunci când este necesară notificarea.

Poziţia autorităţilor de supraveghere, dintre care 17 din sistemul federal al Germaniei, nu este uniformă cu privire la aplicarea obligaţiei de notificare. Ar trebui să fie o practică bună să i se ofere operatorilor o comunicare a situaţiei iniţiale şi finale. În funcţie de relevanţa incidentului, pot fi efectuate alte controale de către autorităţile de supraveghere prin anchete sau audituri la faţa locului pentru a determina eliminarea riscurilor.

---

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

[28] So die h. M. în 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) şi 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 obligaţiile de documentare după *Dix*, în: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, art. 33 alin. (23).

III. Comunicarea către persoanele vizate

Depinde de rezultatul analizei de evaluare a riscului dacă, pe lângă notificarea autorităţii de supraveghere, trebuie informată şi persoana vizată. Operatorul trebuie să o informeze şi pe aceasta doar dacă încălcarea protecţiei datelor cu caracter personal „poate implica un risc ridicat pentru drepturile şi libertăţile personale ale persoanelor fizice" [art. 34 alin. (1) GDPR]. Cu cât este mai ridicat potenţialul prejudiciu, cu atât scade pragul privind probabilitatea de apariţie. Evaluarea se poate baza pe standardele de evaluare prevăzute de Directiva UE ePrivacy[32].

Cu toate acestea art. 34 GDPR prevede o comunicare „imediată". Cu toate acestea, referinţele din considerentul 86 arată că trebuie să existe alte elemente de control pentru a determina „imparţialitatea" faţă de art. 33 GDPR. Conform considerentului 86, comunicările trebuie făcute „în cel mai scurt timp posibil în mod rezonabil şi în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorităţi competente, cum ar fi autorităţile de aplicare a legii". Conform considerentului 86 teza 3, trebuie menţionat 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 protecţiei datelor cu caracter personal". Există aşteptarea ca comunicarea să se realizeze pe cât posibil de rapid.

Notificarea ar trebui să fie făcută într-un limbaj clar şi simplu [art. 34 alin. (2) GDPR], astfel încât persoana în cauză să poată evalua corect orice risc şi să ia măsuri adecvate pentru a preveni prejudiciul. Cu toate acestea, în conformitate cu alin. (3), există trei excepţii, potrivit cărora nu trebuie făcută o comunicare. În primul rând, cf. lit. a) obligaţia de a informa persoanele vizate dacă au fost luate măsuri tehnice şi organizatorice adecvate pentru a împiedica accesul terţilor la date. Conform lit. b) operatorul poate renunţa la comunicare dacă, ulterior, ia măsuri prin care se asigură că riscul ridicat pentru drepturile şi libertăţile 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 anunţ public sau o altă difuzare efectivă a informaţiilor dacă informarea individuală este disproporţionată din cauza numărului foarte mare de persoane afectate sau a lipsei informaţiei cu privire la adresă.

IV. Beneficiarul obligaţiei de notificare

Notificarea intră în sarcina operatorului în sensul art. 4 pct. 7 GDPR. Pentru operatorii asociaţi [art. 26 alin. (1) GDPR], este evident că operatorul căruia îi incumbă obligaţia 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 responsabilităţile, obligaţiile, termenele şi sancţiunile şi să distribuie riscul între părţile

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

responsabile[33]. Fără un acord în acest sens, ei răspund în solidar pentru îndeplinirea obligaţiei de notificare[34].

Dacă un împuternicit cu prelucrarea datelor a dobândit deja cunoştinţe despre o încălcare a protecţiei datelor cu caracter personal din aria sa, acesta trebuie să informeze imediat clientul fără nici o investigaţie sau evaluare[35], deoarece evaluarea riscurilor şi notificarea sunt intră în sarcina clientului. Cu informaţiile primite de la împuternicitul cu prelucrarea datelor, operatorul a luat cunoştinţă de incidentul produs la procesator, care este atribuit operatorului de atunci şi, ca urmare, trebuie să fie raportat de acesta autorităţii de supraveghere. La notificarea unui incident, se urmăreşte consultarea strânsă cu împuternicitul cu prelucrarea datelor pentru a lua măsuri pentru a evita prejudiciul.

În cazul activităţilor 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 şi când nu ar fi avut loc. Este responsabilitatea operatorului să constate sau să se intereseze despre aria de competenţă[36]. Cu toate acestea, autoritatea de supraveghere lipsită de competenţă ar trebui să facă o trimitere la autoritatea competentă sau să o transmită imediat autorităţii competente. Procedura ar trebui să fie coordonată de autorităţile de supraveghere, cu excepţia cazului în care CEPD oferă îndrumări[37].

V. Conţinutul şi forma notificării şi a comunicării

Informaţiile care trebuie furnizate autorităţii de supraveghere rezultă din art. 33 alin. (3) GDPR. Autorităţile de supraveghere din Germania şi România[38] au la dispoziţie formulare electronice pe site-urile lor web, cu ajutorul cărora conţinutul esenţial poate fi specificat şi completat cu text nepredefinit. Dacă, aşa cum s-a întâmplat, situl web al autorităţii de supraveghere este perturbat şi notificarea formularului disponibil nu este posibil în altă modalitate, informaţiile 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 informaţii suplimentare într-o scrisoare de întâmpinare, anume referitoare la naşterea şi desfăşurarea incidentului raportabil ca urmare a investigaţiilor şi măsurile care au fost luate pentru a preveni prejudicierea celor afectaţi şi pentru a preveni repetarea acestora.

Art. 34 alin. (2) GDPR îi ţine pe operatori să comunice persoanelor vizate „într-un limbaj clar şi simplu natura încălcării protecţiei datelor cu caracter personal", cel puţin informaţii şi recomandări dispuse prin prevederile art. 33 alin. (3) lit. b), lit. c) şi lit. d). Această cerinţă este justificată în plus de considerentul 86. Acesta prevede că notificarea ar trebui să conţină „o descriere a naturii încălcării datelor cu caracter personal şi 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.