DECIZIA (UE) 2021/2243 A COMISIEI

din 15 decembrie 2021

de stabilire a normelor interne privind furnizarea de informații persoanelor vizate și restricționarea anumitor drepturi ale acestora în contextul prelucrării datelor cu caracter personal în scopul securității sistemelor informatice și de comunicații ale Comisiei

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 249 alineatul (1),

întrucât:

(1) În îndeplinirea sarcinilor sale, Comisia este obligată să respecte drepturile persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, recunoscute prin articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene și prin articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene. De asemenea, aceasta trebuie să respecte drepturile prevăzute în Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([1]). În același timp, Comisia trebuie să gestioneze incidentele de securitate informatică în conformitate cu normele prevăzute la articolul 15 din Decizia (UE, Euratom) 2017/46 ([2]).

(2) Pentru a asigura securitatea informatică, adică păstrarea confidențialității, integrității și disponibilității sistemelor informatice și de comunicații și a seturilor de date pe care le prelucrează, în ceea ce privește persoanele, activele și informațiile, Comisia, în special prin Direcția Generală Informatică, a luat măsurile prevăzute în Decizia (UE, Euratom) 2017/46 și în Decizia C(2017) 8841 final ([3]). Printre aceste măsuri se numără monitorizarea riscurilor de securitate informatică și a măsurilor de securitate informatică puse în aplicare, solicitarea ca proprietarii de sisteme să ia măsuri specifice de securitate informatică pentru a atenua riscurile în materie de securitate informatică la adresa sistemelor informatice și de comunicații ale Comisiei, precum și gestionarea incidentelor de securitate informatică.

(3) Direcția Generală Informatică furnizează Comisiei operațiuni și servicii de securitate informatică și trebuie să prelucreze mai multe categorii de date cu caracter personal pentru:

— a comunica alertele și avertizările legate de evenimentele și incidentele de securitate informatică;

— a răspunde la evenimentele și incidentele de securitate informatică și a le limita amploarea;

— a facilita instrumentele și operațiunile prin audituri de securitate, evaluări ale securității și gestionarea vulnerabilităților;

— a crește gradul de sensibilizare a personalului Comisiei în domeniul securității cibernetice;

— a monitoriza, detecta și preveni producerea evenimentelor și incidentelor de securitate informatică;

— a examina conturile de utilizator privilegiat.

(4) Incidentele de securitate informatică care ar putea submina securitatea sistemelor informatice și de comunicații ale Comisiei pot apărea în orice operațiune de prelucrare efectuată de Comisie. Acestea pot implica orice categorie de date cu caracter personal prelucrate de Comisie.

([1]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

([2]) Decizia (UE, Euratom) 2017/46 a Comisiei din 10 ianuarie 2017 privind securitatea sistemelor informatice și de comunicații în cadrul Comisiei Europene (JO L 6, 11.1.2017, p. 40).

([3]) Decizia C(2017) 8841 a Comisiei din 13 decembrie 2017 de stabilire a normelor de punere în aplicare pentru articolele 3, 5, 7, 8, 9, 10, 11, 12, 14 și 15 din Decizia (UE, Euratom) 2017/46 privind securitatea sistemelor informatice și de comunicații din cadrul Comisiei.

(5) În anumite circumstanțe, se poate dovedi necesar să se reconcilieze drepturile persoanelor vizate în temeiul Regulamentului (UE) 2018/1725 cu necesitatea Comisiei de a-și îndeplini în mod eficace sarcinile de asigurare a securității informatice a persoanelor, activelor și informațiilor în cadrul Comisiei în temeiul Deciziei (UE, Euratom) 2017/46 și cu respectarea deplină a drepturilor și libertăților fundamentale ale altor persoane vizate. În acest scop, articolul 25 alineatul (1) din Regulamentul (UE) 2018/1725 autorizează Comisia să restricționeze aplicarea articolelor 14-17, 19, 20 și 35 din regulamentul citat, precum și a principiului transparenței menționat la articolul său 4 alineatul (1) litera (a), în măsura în care dispozițiile sale corespund drepturilor și obligațiilor prevăzute la articolele 14-17, 19 și 20 din regulamentul respectiv.

(6) Prezenta decizie trebuie să se aplice tuturor operațiunilor de prelucrare efectuate de Comisie în calitate de operator de date în îndeplinirea sarcinilor sale de asigurare a securității informatice a persoanelor, activelor și informațiilor în cadrul Comisiei în temeiul Deciziei (UE, Euratom) 2017/46. Prin urmare, aceasta trebuie să se refere la persoanele vizate din categoriile de date cu caracter personal acoperite de toate aceste operațiuni de prelucrare, și anume la persoanele care interacționează cu oricare dintre sistemele informatice și de comunicații ale Comisiei.

(7) Datele cu caracter personal sunt stocate într-un mediu electronic securizat, pentru a preveni accesarea ilegală de către persoane din afara Comisiei. Diferitelor operațiuni de prelucrare li se aplică diferite perioade de păstrare a datelor, în funcție de tipul de date cu caracter personal implicate. Păstrarea dosarelor în cadrul Comisiei este reglementată de Lista comună de păstrare a dosarelor la nivelul Comisiei [SEC(2019) 900], un document de reglementare sub forma unui calendar de păstrare care stabilește perioadele de păstrare pentru diferite tipuri de dosare ale Comisiei pentru a limita păstrarea datelor la ceea ce este necesar.

(8) Comisia ar putea fi nevoită să restricționeze aplicarea drepturilor persoanelor vizate pentru a-și proteja securitatea internă în temeiul articolului 25 alineatul (1) litera (d) din Regulamentul (UE) 2018/1725 (și anume, pentru a păstra confidențialitatea, integritatea și disponibilitatea sistemelor sale informatice și de comunicații și a seturilor de date pe care le prelucrează, a activelor și a informațiilor aferente). În particular, Comisia ar putea fi nevoită să facă acest lucru atunci când:

— comunică alertele și avertizările legate de evenimentele și incidentele de securitate informatică;

— răspunde la evenimentele și incidentele de securitate informatică și le limitează amploarea; facilitează instrumentele și operațiunile prin audituri de securitate, evaluări ale securității și gestionarea vulnerabilităților;

— crește gradul de sensibilizare a personalului Comisiei în domeniul securității cibernetice;

— monitorizează, detectează și previne producerea evenimentelor și incidentelor de securitate informatică;

— examinează conturile de utilizator privilegiat.

(9) În scopul gestionării incidentelor de securitate informatică, astfel cum se menționează la articolul 15 din Decizia (UE, Euratom) 2017/46, Direcția Generală Informatică poate face schimb de informații cu Centrul de răspuns la incidente de securitate cibernetică din cadrul Direcției Generale Resurse Umane și Securitate.

(10) Pentru a respecta dispozițiile articolelor 14, 15 și 16 din Regulamentul (UE) 2018/1725, Comisia trebuie să informeze toate persoanele fizice cu privire la activitățile care implică prelucrarea datelor lor cu caracter personal și care le afectează drepturile. Comisia trebuie să facă acest lucru într-un mod transparent și coerent, prin publicarea unei comunicări privind protecția datelor pe site-ul web al Comisiei. După caz, aceasta trebuie să aplice garanții suplimentare pentru a informa persoanele vizate în mod individual, într-un format adecvat.

(11) Respectarea dispozițiilor articolelor 14, 15 și 16 din Regulamentul (UE) 2018/1725 ar putea dezvălui existența unor măsuri de securitate, a unor vulnerabilități sau a unor incidente de natură informatică care intră sub incidența articolului 15 din Decizia (UE, Euratom) 2017/46. Dezvăluirea acestor măsuri de securitate, vulnerabilități și incidente de natură informatică sporește riscul ca măsura de securitate informatică expusă să fie apoi eludată, ca vulnerabilitatea expusă să fie utilizată în mod abuziv și ca o analiză continuă a incidentelor de securitate informatică să fie subminată deoarece artefactele ar putea fi manipulate accidental sau intenționat de un utilizator sau de un actor rău intenționat. Acest lucru ar putea afecta grav capacitatea Comisiei de a-și asigura securitatea informatică și, în special, de a gestiona în mod eficace incidentele de securitate informatică în viitor.

(12) În temeiul articolului 25 alineatul (1) litera (h) din Regulamentul (UE) 2018/1725, Comisia este, de asemenea, autorizată să restricționeze aplicarea drepturilor persoanelor vizate pentru a proteja drepturile și libertățile altor persoane fizice în legătură cu incidente de securitate informatică care ar putea submina operațiunile de securitate informatică.

(13) Comisia poate fi nevoită să restricționeze furnizarea de informații persoanelor vizate și aplicarea altor drepturi ale acestora în ceea ce privește datele cu caracter personal primite din partea țărilor din afara UE sau a organizațiilor internaționale, pentru a-și îndeplini obligația de cooperare cu respectivele țări sau organizații. Acest lucru face parte din datoria Comisiei de a salvgarda un obiectiv important de interes public general al UE, astfel cum se menționează la articolul 25 alineatul (1) litera (c) din Regulamentul (UE) 2018/1725. Cu toate acestea, în anumite circumstanțe, interesul drepturilor fundamentale ale persoanei vizate poate prevala asupra interesului cooperării internaționale.

(14) Prin urmare, Comisia a identificat motivele enumerate la articolul 25 alineatul (1) literele (c), (d) și (h) din Regulamentul (UE) 2018/1725 ca fiind motive pentru restricții pe care ar putea fi necesar să le aplice operațiunilor de prelucrare a datelor efectuate de Direcția Generală Informatică în legătură cu furnizarea de operațiuni și servicii de securitate informatică Comisiei.

(15) Este oportun ca orice restricție aplicată în temeiul prezentei decizii să fie necesară și proporționată, ținând seama de riscurile la adresa drepturilor și libertăților persoanelor vizate.

(16) Comisia trebuie să gestioneze toate restricțiile într-un mod transparent și să înregistreze fiecare aplicare a unei restricții în sistemul de evidență corespunzător.

(17) În temeiul articolului 25 alineatul (8) din Regulamentul (UE) 2018/1725, operatorii de date pot să amâne, să omită sau să refuze furnizarea de informații pe baza justificării aplicării unei restricții persoanei vizate în cazul în care furnizarea informațiilor respective ar submina în orice mod efectul restricției. În particular, acest lucru se aplică restricțiilor privind obligațiile prevăzute la articolele 16 și 35 din Regulamentul (UE) 2018/1725. Comisia trebuie să examineze în mod regulat restricțiile impuse pentru a se asigura că drepturile persoanei vizate de a fi informată în conformitate cu articolele 16 și 35 din Regulamentul (UE) 2018/1725 sunt restricționate numai atâta timp cât astfel de restricții sunt necesare pentru a permite Comisiei să își asigure securitatea informatică și, în particular, să rezolve incidentele de securitate informatică.

(18) Atunci când Comisia restricționează aplicarea drepturilor unor persoane vizate, altele decât cele menționate la articolele 16 și 35 din Regulamentul (UE) 2018/1725, operatorul de date trebuie să evalueze, de la caz la caz, măsura în care comunicarea restricției i-ar submina scopul.

(19) Este necesar ca responsabilul cu protecția datelor din cadrul Comisiei să efectueze o examinare independentă a aplicării restricțiilor, pentru a asigura respectarea prezentei decizii.

(20) Pentru a permite Comisiei să restricționeze imediat aplicarea anumitor drepturi și obligații în conformitate cu articolul 25 din Regulamentul (UE) 2018/1725, prezenta decizie trebuie să intre în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

(21) Autoritatea Europeană pentru Protecția Datelor a emis un aviz la 16 septembrie 2021,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Obiect și domeniu de aplicare

(1) Prezenta decizie stabilește normele pe care Comisia trebuie să le respecte pentru a informa persoanele vizate cu privire la prelucrarea datelor lor cu caracter personal în conformitate cu articolele 14, 15 și 16 din Regulamentul (UE) 2018/1725, atunci când își îndeplinește sarcinile care îi revin în temeiul Deciziei (UE, Euratom) 2017/46.

Aceasta stabilește, de asemenea, condițiile în care Comisia poate restricționa aplicarea articolelor 4, 14-17, 19, 20 și 35 din Regulamentul (UE) 2018/1725, în conformitate cu articolul 25 alineatul (1) literele (c), (d) și (h) din regulamentul menționat, atunci când își îndeplinește sarcinile în temeiul Deciziei (UE, Euratom) 2017/46.

(2) Prezenta decizie se aplică prelucrării datelor cu caracter personal, fie de către Comisie, fie în numele acesteia, în scopul sau în legătură cu activitățile desfășurate pentru a asigura securitatea informatică a persoanelor, a activelor și a informațiilor în cadrul Comisiei în temeiul Deciziei (UE, Euratom) 2017/46.

Articolul 2

Excepții și restricții aplicabile

(1) Atunci când își exercită atribuțiile cu privire la drepturile persoanelor vizate în temeiul Regulamentului (UE) 2018/1725, Comisia analizează dacă se aplică vreuna dintre excepțiile prevăzute în regulamentul menționat.

(2) Sub rezerva articolelor 3-7 din prezenta decizie, atunci când exercitarea drepturilor și a obligațiilor prevăzute la articolele 14-17, 19, 20 și 35 din Regulamentul (UE) 2018/1725 în ceea ce privește date cu caracter personal prelucrate de Comisie ar submina scopul de a furniza operațiuni și servicii de securitate informatică, printre altele prin dezvăluirea instrumentelor de investigare, a vulnerabilităților și a metodelor Comisiei, sau ar afecta drepturile și libertățile și securitatea altor persoane vizate, în particular în ceea ce privește prelucrarea datelor cu caracter personal pentru:

— a comunica alertele și avertizările legate de evenimentele și incidentele de securitate informatică;

— a răspunde la evenimentele și incidentele de securitate informatică și a le limita amploarea;

— a facilita instrumentele și operațiunile prin audituri de securitate, evaluări ale securității și gestionarea vulnerabilităților;

— a crește gradul de sensibilizare a personalului Comisiei în domeniul securității cibernetice;

— a monitoriza, detecta și preveni producerea evenimentelor și incidentelor de securitate informatică;

— a examina conturile de utilizator privilegiat,

Comisia poate restricționa aplicarea:

(a) articolelor 14-17, 19, 20 și 35 din Regulamentul (UE) 2018/1725;

(b) principiului transparenței menționat la articolul 4 alineatul (1) litera (a) din Regulamentul (UE) 2018/1725, în măsura în care dispozițiile sale corespund drepturilor și obligațiilor prevăzute la articolele 14-17, 19 și 20 din Regulamentul (UE) 2018/1725.

Comisia poate face acest lucru în conformitate cu articolul 25 alineatul (1) literele (c), (d) și (h) din Regulamentul (UE) 2018/1725.

(3) Sub rezerva articolelor 3-7, Comisia poate restricționa drepturile și obligațiile menționate la alineatul (2) de la prezentul articol:

(a) dacă exercitarea drepturilor și obligațiilor respective în ceea ce privește datele cu caracter personal obținute de la o altă instituție, un alt organ, o altă agenție sau un alt oficiu al UE ar putea fi restricționată de instituția, organul, agenția sau oficiul respectiv al UE pe baza unor acte juridice prevăzute la articolul 25 din Regulamentul (UE) 2018/1725 sau în temeiul capitolului IX din respectivul regulament, în conformitate cu Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului ([4]) sau în conformitate cu Regulamentul (UE) 2017/1939 al Consiliului ([5]);

(b) dacă exercitarea drepturilor și obligațiilor respective în privința datelor cu caracter personal obținute de la autoritatea competentă a unui stat membru ar putea fi restricționată de autoritățile competente ale respectivului stat membru pe baza măsurilor legislative menționate la articolul 23 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([6]) sau în temeiul măsurilor naționale de transpunere a articolului 13 alineatul (3), a articolului 15 alineatul (3) sau a articolului 16 alineatul (3) din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([7]);

([4]) Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53).

([5]) Regulamentul (UE) 2017/1939 al Consiliului din 12 octombrie 2017 de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO) (JO L 283, 31.10.2017, p. 1).

([6]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([7]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

(c) atunci când exercitarea acestor drepturi și obligații ar submina cooperarea Comisiei cu țări terțe sau cu organizații internaționale în ceea ce privește amenințările comune la adresa securității cibernetice.

Înainte de a aplica restricții în circumstanțele menționate la primul paragraf literele (a) și (b), Comisia consultă instituțiile, organele, agențiile și oficiile relevante ale UE sau autoritățile competente ale statelor membre în ceea ce privește motivele potențiale pentru impunerea de restricții, precum și necesitatea și proporționalitatea restricțiilor în cauză, cu excepția cazului în care acest lucru ar submina activitățile Comisiei și cu excepția cazului în care Comisia are certitudinea că aplicarea unei restricții este prevăzută de unul dintre actele menționate la literele respective sau că o consultare ar pune în pericol scopul activităților sale în temeiul Deciziei (UE, Euratom) 2017/46.

Primul paragraf litera (c) nu se aplică în cazul în care interesele sau drepturile și libertățile fundamentale ale persoanei vizate prevalează asupra interesului Comisiei de a coopera cu țări din afara UE sau cu organizații internaționale.

(4) Alineatele (1), (2) și (3) nu aduc atingere aplicării altor decizii ale Comisiei de stabilire a unor norme interne de reglementare a furnizării de informații persoanelor vizate și de restricționare a anumitor drepturi în temeiul articolului 25 din Regulamentul (UE) 2018/1725.

(5) Orice restricționare a drepturilor și obligațiilor menționată la alineatul (2) trebuie să fie necesară și proporțională cu riscurile la adresa drepturilor și libertăților persoanelor vizate.

(6) Înainte de aplicarea restricțiilor, trebuie să se efectueze un test de necesitate și proporționalitate, de la caz la caz, iar restricțiile trebuie să se limiteze la ceea ce este strict necesar pentru atingerea scopului preconizat.

Articolul 3

Furnizarea de informații persoanelor vizate

(1) Comisia publică pe site-ul său web un anunț privind protecția datelor prin care informează toate persoanele vizate în legătură cu activitățile sale care implică prelucrarea datelor lor cu caracter personal, pe care le desfășoară cu scopul de a-și îndeplini sarcinile prevăzute în Decizia (UE, Euratom) 2017/46, inclusiv o descriere a categoriilor de date cu caracter personal implicate. Atunci când este posibil să se procedeze astfel fără a se compromite securitatea informatică, Comisia asigură faptul că persoanele vizate sunt informate în mod individual într-un format adecvat.

(2) Atunci când restricționează, integral sau parțial, furnizarea de informații persoanelor vizate ale căror date cu caracter personal le prelucrează în scopul îndeplinirii sarcinilor care îi revin în temeiul Deciziei (UE, Euratom) 2017/46, Comisia înscrie în evidențe și înregistrează motivele restricției în conformitate cu articolul 6 din prezenta decizie.

Articolul 4

Dreptul de acces al persoanei vizate, dreptul la ștergerea datelor și dreptul la restricționarea prelucrării

(1) Atunci când Comisia restricționează, integral sau parțial, dreptul de acces la datele cu caracter personal al persoanelor vizate, dreptul la ștergerea datelor sau dreptul de a restricționa prelucrarea datelor, astfel cum se menționează la articolele 17, 19 și 20 din Regulamentul (UE) 2018/1725, ea informează persoana vizată în cauză, în răspunsul ei la cererea de acces, de ștergere a datelor sau de restricționare a prelucrării datelor:

(a) cu privire la restricția aplicată și la motivele principale pentru care a făcut acest lucru;

(b) cu privire la modalitatea de a depune o plângere la Autoritatea Europeană pentru Protecția Datelor sau de a introduce o cale de atac la Curtea de Justiție a Uniunii Europene.

(2) Comisia poate amâna, omite sau refuza furnizarea de informații privind motivele restricției menționate la alineatul (1) atât timp cât acest lucru ar submina scopul restricției.

(3) Comisia înscrie în evidențe și înregistrează motivele restricției în conformitate cu articolul 6.

(4) Atunci când dreptul de acces este restricționat, integral sau parțial, persoanele vizate își pot exercita dreptul de acces prin contactarea Autorității Europene pentru Protecția Datelor, în conformitate cu articolul 25 alineatele (6), (7) și (8) din Regulamentul (UE) 2018/1725.

Articolul 5

Informarea persoanelor vizate cu privire la încălcarea securității datelor cu caracter personal

Atunci când Comisia restricționează informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal, astfel cum se menționează la articolul 35 din Regulamentul (UE) 2018/1725, ea înscrie în evidențe și înregistrează motivele restricției în conformitate cu articolul 6 al prezentei decizii. Comisia comunică AEPD înscrierea în evidențe în momentul notificării încălcării securității datelor cu caracter personal.

Articolul 6

Înscrierea în evidențe și înregistrarea restricțiilor

(1) Comisia înscrie în evidențe motivele oricărei restricții aplicate în temeiul prezentei decizii, inclusiv o trimitere la temeiul (temeiurile) juridic(e) aplicate pentru restricție și o evaluare a necesității și a proporționalității restricției, ținând seama de elementele relevante prevăzute la articolul 25 alineatul (2) din Regulamentul (UE) 2018/1725.

(2) Înscrierea în evidențe trebuie să precizeze modul în care exercitarea unui drept de către persoana vizată ar submina scopul de a furniza Comisiei operațiuni și servicii de securitate informatică în conformitate cu Decizia (UE, Euratom) 2017/46, sau al restricțiilor aplicate în temeiul articolului 2 alineatul (2) sau (3) din prezenta decizie, sau ar afecta drepturile și libertățile altor persoane vizate.

(3) Comisia înregistrează aceste evidențe și orice documente care conțin elemente de fapt și de drept justificative. La cerere, acestea se pun la dispoziția Autorității Europene pentru Protecția Datelor.

Articolul 7

Durata restricțiilor

(1) Restricțiile menționate la articolele 3, 4 și 5 continuă să se aplice atât timp cât motivele care stau la baza lor rămân valabile.

(2) Atunci când motivele care stau la baza unei restricții menționate la articolele 3, 4 și 5 nu mai sunt valabile, Comisia:

(a) ridică restricția;

(b) informează persoana vizată cu privire la principalele motive care au stat la baza restricției;

(c) informează persoana vizată cu privire la modul în care poate depune o plângere la Autoritatea Europeană pentru Protecția Datelor în orice moment sau poate introduce o cale de atac la Curtea de Justiție a Uniunii Europene.

Articolul 8

Garanții și perioade de stocare

(1) Comisia reexaminează aplicarea restricțiilor menționate la articolele 3, 4 și 5 la șase luni de la adoptarea acestora, precum și la închiderea operațiunii de securitate informatică în cauză. Ulterior, Comisia examinează și monitorizează anual necesitatea de a menține orice restricție.

Reexaminarea trebuie să includă evaluarea necesității și a proporționalității restricției, ținând seama de elementele relevante menționate la articolul 25 alineatul (2) din Regulamentul (UE) 2018/1725.

(2) Comisia a adoptat măsuri tehnice și organizatorice pentru a evita orice distrugere accidentală sau ilegală, pierdere, modificare, divulgare neautorizată sau acces neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, cum ar fi gestionarea drepturilor de acces, politica privind copia de rezervă și orice altă măsură luată în conformitate cu Decizia (UE, Euratom) 2017/46.

(3) Comisia înregistrează perioadele de păstrare aplicabile în conformitate cu Lista comună de păstrare a dosarelor la nivelul Comisiei și pune la dispoziția persoanelor vizate perioadele de păstrare relevante pentru aceste activități de prelucrare în avizul său privind protecția datelor.

Articolul 9

Reexaminarea de către responsabilul cu protecția datelor al Comisiei

(1) Responsabilul cu protecția datelor al Comisiei trebuie să fie informat, fără întârzieri nejustificate, ori de câte ori drepturile persoanelor vizate sunt restricționate în conformitate cu prezenta decizie. La cerere, responsabilului cu protecția datelor i se acordă accesul la evidențe și la orice documente care conțin elemente de fapt și de drept justificative.

(2) Responsabilul cu protecția datelor poate solicita o reexaminare a restricțiilor și trebuie să fie informat cu privire la rezultatul reexaminării solicitate.

(3) Comisia documentează implicarea responsabilului cu protecția datelor ori de câte ori drepturile persoanelor vizate sunt restricționate în conformitate cu prezenta decizie.

Articolul 10

Intrarea în vigoare

Prezenta decizie intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 15 decembrie 2021.

Pentru Comisie
Președintele
Ursula VON DER LEYEN