ZIUA EUROPEANĂ A PROTECȚIEI DATELOR

2024

www.dataprotection.ro

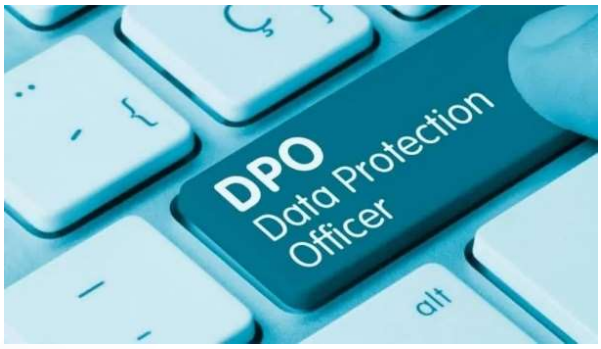
ANS PDCP

A. Semnificația Zilei Europene a Protecției Datelor

Pe data de 28 Ianuarie 2024 se sărbătorește Ziua Europeană a Protecției Datelor, care marchează împlinirea a 43 de ani de la adoptarea de către Consiliul Europei, în anul 1981, la Strasbourg, a Convenției 108 pentru protecția persoanelor referitoare la prelucrarea automatizată a datelor cu caracter personal.

Această zi reprezintă un prilej pentru a informa publicul larg cu privire la regulile de prelucrare a datelor cu caracter personal, dar și pentru a crește gradul de conștientizare a operatorilor de date în ceea ce privește importanța dreptului la viață privată a persoanelor în contextul erei digitale.

Pentru sărbătorirea Zilei Europene a Protecției Datelor, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal organizează, pe data de 26 ianuarie 2024, **Conferința on-line intitulată „Rolul și eficiența activității responsabilului cu protecția datelor”**, cu participarea reprezentanților autorităților și instituțiilor publice centrale naționale, ai forului executiv și ai celui legislativ, reprezentanților mediilor academice, organizațiilor nonguvernamentale, ai principalelor uniuni/asociații profesionale, precum și alți operatori/împuterniciți din sectorul public şi privat.



A. Semnificația Zilei Europene a Protecției Datelor

Cu acest prilej, vor fi aduse în atenția operatorilor cât și a persoanelor împuternicite aspecte specifice prelucrării datelor cu caracter personal, în special în ceea ce privește importanța rolului responsabilului cu protecția datelor.

Pentru celebrarea acestui eveniment, **pe postul național de televiziune TVR și în mijloacele de transport în comun ale Societății de Transport București, va fi difuzat clipul informativ** dedicat Regulamentului General privind Protecția Datelor.

În același timp, instituția noastră a propus Ministerului Afacerilor Interne și Ministerului Afacerilor Externe, organizarea de manifestări destinate creșterii gradului de informare cu privire la aplicarea specifică a regulilor de protecție a datelor de către personalul polițienesc, respectiv de către personalul diplomatic și consular, inclusiv cu privire la noutățile aduse prin Regulamentele (UE) 2018/1860, 2018/1861, 2018/1862, aplicabile în domeniul Schengen.

B. Responsabilul cu protecția datelor – *funcție esențială în mecanismul de prelucrare a datelor cu caracter personal*

1. Desemnarea responsabilului cu protecția datelor (art. 37 din GDPR)

Desemnarea unui responsabil cu protecția datelor **este obligatorie**:

- în cazul în care prelucrarea este efectuată de către o autoritate sau un organism public (indiferent de datele care sunt prelucrate);
- în cazul în care activitățile principale ale operatorului sau ale persoanei împuternicite de către operator constau în operațiuni de prelucrare care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;
- în cazul în care activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni.

„Activitățile principale" reprezintă operațiunile de prelucrare a datelor cu caracter personal desfășurate pentru realizarea obiectivelor operatorului sau ale persoanei împuternicite de către operator.

Exemple:

- prelucrarea datelor personale, inclusiv cele privind starea de sănătate de către un spital, cum ar fi dosarele medicale ale pacienților;
- prelucrarea datelor personale ale clienților de către o instituție financiar-bancară.

Pentru a se stabili dacă **prelucrarea este efectuată pe scară largă** trebuie să se țină cont de următorii factori:

- Numărul persoanelor vizate;
- Volumul datelor;
- Durata sau caracterul permanent al activității de prelucrare a datelor;
- Întinderea geografică a activității de prelucrare.

B. Responsabilul cu protecția datelor – *funcție esențială în mecanismul de protecție a datelor cu caracter personal*

- Exemple:

Prelucrare pe scară largă	**Prelucrare care nu constituie pe scară largă**
prelucrarea datelor privind starea de sănătate a pacienților de către un spital	prelucrarea datelor personale ale pacienților de către un cabinet medical individual
prelucrarea datelor cu caracter personal ale clienților de către o societate de asigurări sau o instituție financiar-bancară	prelucrarea datelor cu caracter personal ale clienților de către o persoană fizică autorizată care desfășoară activitate de intermediere credite sau cabinet individual de avocat

Publicarea și comunicarea datelor de contact ale responsabilului cu protecția datelor

Operatorii sau persoanele împuternicite de către operatori sunt obligați:

- să publice datele de contact ale responsabilului cu protecția datelor (exemplu: adresă poștală, număr de telefon și/sau o adresă de e-mail) și
- să comunice datele de contact ale acestuia către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Se recomandă, de asemenea, informarea angajaților operatorului sau, după caz, a angajaților persoanei împuternicite de către operator cu privire la numele și datele de contact ale responsabilului. Spre exemplu, numele și datele de contact ale acestuia ar putea fi comunicate la nivel intern, în rețeaua intranet a operatorului sau pe adresa de e-mail a angajaților.

B. Responsabilul cu protecția datelor – *funcție esențială în mecanismul de protecție a datelor cu caracter personal*

2. Funcția responsabilului cu protecția datelor (art. 38 din GDPR)

Implicarea responsabilului cu protecția datelor

Pentru a facilita conformitatea cu GDPR și pentru a promova o abordare adecvată privind protejarea vieții private, operatorul și persoana împuternicită de către operator trebuie să se asigure de faptul că responsabilul cu protecția datelor *„este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal*".

Asigurarea resurselor necesare

Pentru a permite responsabilului cu protecția datelor să își îndeplinească în mod eficient atribuțiile, operatorii și persoanele împuternicite de operatori trebuie să îi pună la dispoziție resursele necesare.

Astfel, în funcție de natura operațiunilor de prelucrare, precum și de activitățile și dimensiunea organizației, operatorul ar trebui să pună la dispoziția responsabilului cu protecția datelor următoarele resurse:

- sprijin substanțial în ceea ce privește resursele financiare, infrastructura (spații, facilități, echipamente) și personal, după caz;
- timp suficient pentru îndeplinirea sarcinilor;
- formare continuă prin participare la cursuri de perfecționare;
- comunicarea oficială cu privire la desemnarea responsabilului către toți membrii personalului;
- având în vedere dimensiunea și structura operatorului, ar putea fi necesar să se constituie o echipă a responsabilului cu protecția datelor;
- sprijin activ din partea personalului de conducere de nivel superior.

B. Responsabilul cu protecția datelor – *funcție esențială în mecanismul de protecție a datelor cu caracter personal*

Independența responsabilului cu protecția datelor

Garanții care permit responsabilului să acționeze în mod independent:

- nu primește instrucțiuni din partea operatorilor sau a persoanelor împuternicite de către operatori în ceea ce privește exercitarea de către responsabil a sarcinilor;
- nu este concediat sau sancționat de către operator în legătură cu îndeplinirea sarcinilor sale;
- răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator;
- nu există un conflicte de interese cu posibile alte sarcini și atribuții.

Conflictul de interese

Responsabilul cu protecția datelor nu poate deține o funcție în cadrul organizației, prin care să stabilească scopurile și mijloacele de prelucrare a datelor cu caracter personal.

Printre funcțiile care pot da naștere unor conflicte de interese se pot include funcțiile personalului de conducere de nivel superior, precum:

- director general
- director general administrativ
- director financiar
- medic primar
- șef al departamentului de marketing
- șef al serviciului de resurse umane
- șef al departamentelor IT

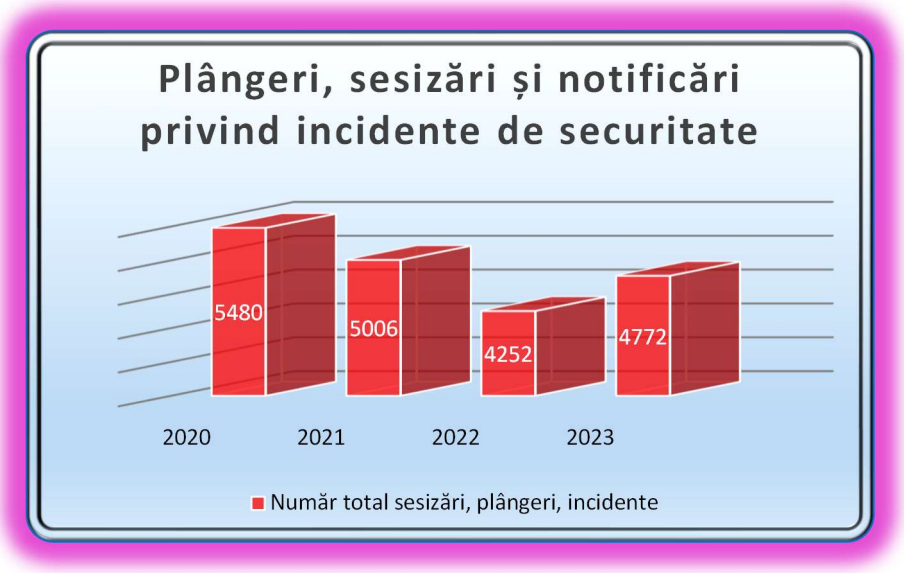
B. Responsabilul cu protecția datelor – *funcție esențială în mecanismul de protecție a datelor cu caracter personal*

Mai multe informații pot fi găsite în ”Ghidul privind responsabilul pentru protecția datelor”, emis, în anul 2017, de Comitetul european pentru protecția datelor, disponibil pe adresa de internet a autorității, www.dataprotection.ro, la secțiunea dedicată Noului Regulament General de Protecția Datelor.

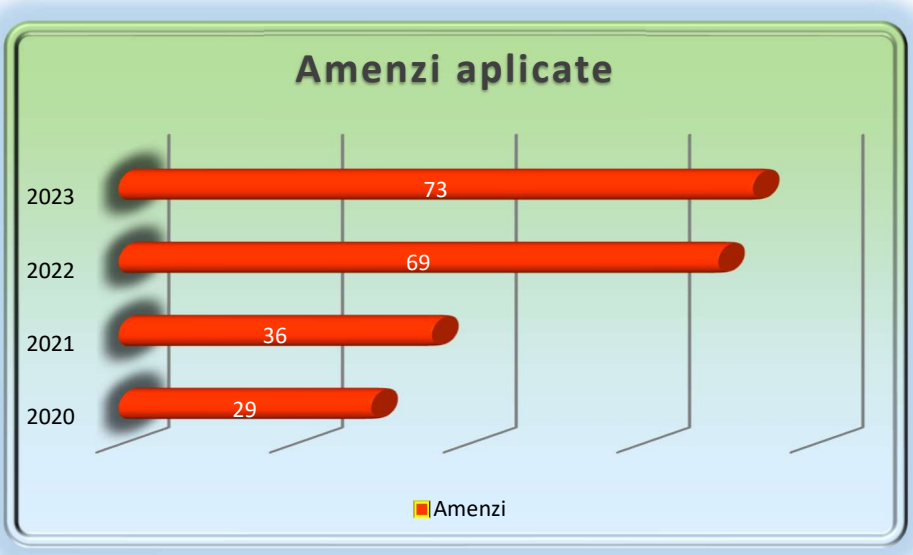
3. Sarcinile responsabilului cu protecția datelor (art. 39 din GDPR)

- informarea și consilierea operatorului, sau, după caz, a persoanei împuternicite de operator cu privire la obligațiile care le revin în temeiul GDPR;
- monitorizarea respectării GDPR;
- furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor;
- cooperarea cu autoritatea de supraveghere

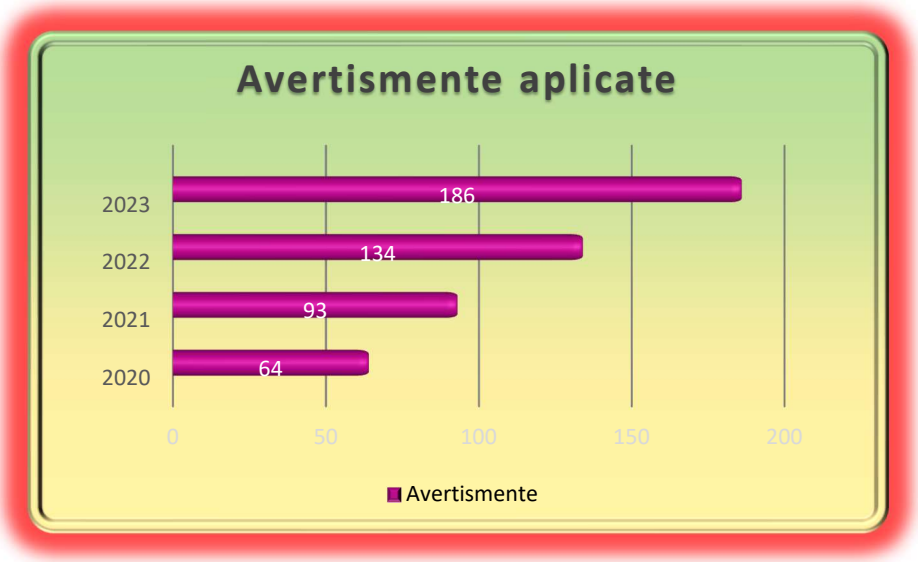
În cursul anului 2023, Autoritatea de Supraveghere a primit un număr de **4772** de plângeri, sesizări și notificări privind incidente de securitate, pe baza cărora au fost deschise **548 investigații**.



Ca urmare a investigațiilor efectuate, Autoritatea de supraveghere a aplicat, în anul 2023, în total **73 de amenzi** în cuantum **de 2.348.265 lei.** Dintre acestea, **67 de amenzi** au fost aplicate în baza GDPR (în cuantum **de 2.228.265 lei –** echivalentul sumei de 448.600 euro), **4 amenzi** au fost aplicate în baza Legii nr. 506/2004 (în cuantum de **100.000 lei)** și **2 amenzi** au fost aplicate în baza Legii nr. 190/2018 în cuantum de **20.000 lei.**

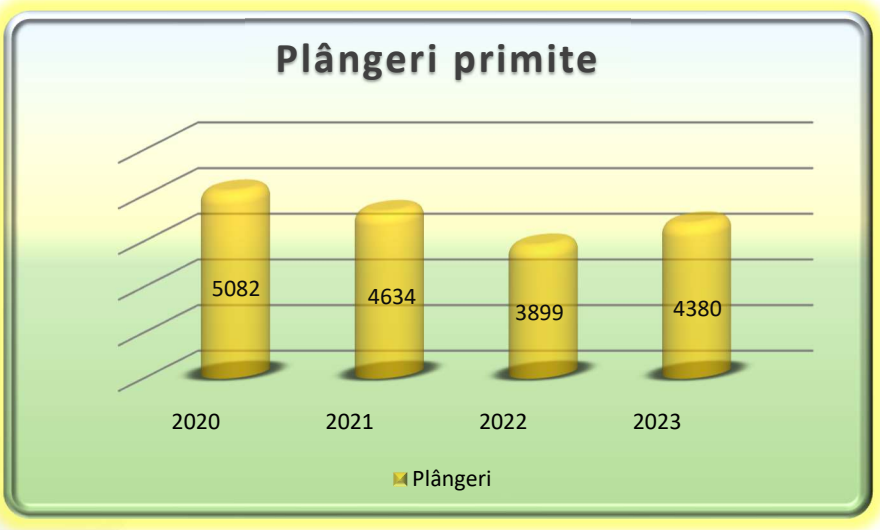


De asemenea, în anul 2023, au mai fost aplicate în total **186 de avertismente** și au fost dispuse **138 de măsuri corective.**



A. Activitatea de soluționare a plângerilor

În ceea ce privește activitatea de soluționare a plângerilor, Autoritatea de Supraveghere a primit **în anul 2023** un număr total de **4380 plângeri**, pe baza cărora au fost demarate **207 investigații**.



Plângerile primite de Autoritatea de Supraveghere în anul 2023 au vizat, în principal, următoarele domenii:

- prelucrarea datelor cu caracter personal cu încălcarea prevederilor art. 5 și 6 din GDPR;
- încălcarea drepturilor persoanelor vizate, în special, a dreptului de acces al persoanei vizate și a dreptului la ștergerea datelor acesteia;
- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date cu caracter personal.

Urmare a **investigațiilor efectuate pe baza plângerilor**, au fost aplicate următoarele **sancțiuni contravenționale** :

- **36 de amenzi** în baza GDPR în cuantum total de 687.102,38 lei (echivalentul sumei de 138.700 euro);
- **2 amenzi în** baza Legii nr. 506/2004, în cuantum total de 20.000 lei;
- **1 amendă** în baza legii 190/2018, în cuantum total de 10.000 lei;
- **120 de avertismente**;
- **80 măsuri corective** în baza dispozițiilor art. 58 alin. (2) lit. c), d) și e) din Regulamentul (UE) 2016/679.

B. Activitatea de control ca urmare a primirii de notificări privind încălcarea securității datelor și sesizări

În ceea ce privește incidentele de securitate, operatorii de date au transmis **în anul 2023**, un număr de **181 de notificări privind încălcarea securității datelor** (180 încălcări ale GDPR și 1 încălcare a Legii nr. 506/2004), iar sesizările privind posibile neconformități cu dispozițiile Regulamentul (UE) 2016/679 s-au ridicat la un număr de **211**.

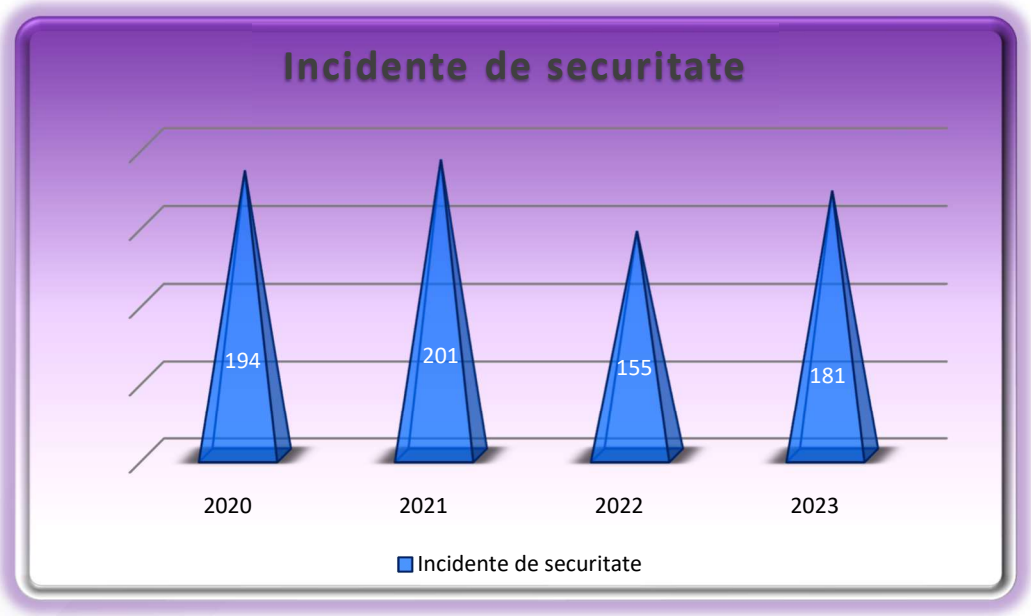
Încălcările de securitate au vizat, în principal, următoarele aspecte:

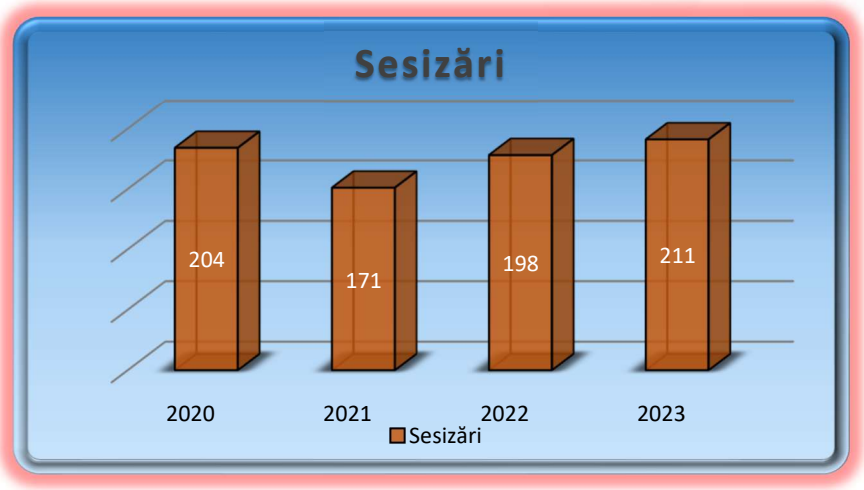
- Confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare a dezvăluirilor neautorizate ori ca urmare a unui incident informatic de tip atac ransomware;
- Confidențialitatea datelor cu caracter personal în mediul online ca urmare a configurării deficitare a site-urilor/aplicațiilor informatice utilizate de operatori;
- Prelucrarea datelor cu caracter personal ale clienților din sistemul bancar;
- Dezvăluirea datelor cu caracter personal în mediul online, în special pe rețelele sociale;
- Accesul neautorizat la sistemele de supraveghere video cu circuit închis;
- Dezvăluirea datelor cu caracter personal în sistemul medical.

Sesizările primite au vizat, în principal, următoarele aspecte:

- Încălcarea principiilor de prelucrare a datelor prevăzute de GDPR;
- Dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;
- Confidențialitatea datelor cu caracter personal în mediul on-line ca urmare a configurării deficitare a site-urilor/aplicațiilor informatice utilizate de operatori;
- Dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele sociale;
- Prelucrarea datelor cu caracter personal prin intermediul sistemelor de supraveghere video, inclusiv prin utilizarea unor mijloace de supraveghere video mobilă (body-cam);
- Încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale prin neadoptarea de către operatori a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor.

Evoluția incidentelor de securitate și a sesizărilor în 2023 poate fi observată în graficul de mai jos, astfel:





Ca urmare a **sesizărilor** primite **și încălcărilor de securitate** notificate de către operatorii de date cu caracter personal, la nivelul Autorității de Supraveghere au fost demarate, pe parcursul anului 2023, un număr de **341 de investigații din oficiu**.

Urmare a **investigațiilor efectuate,** în anul 2023, au fost aplicate:

- **31 de amenzi** în baza GDPR în cuantum total de 1.541,163 lei (echivalentul sumei de 309.900 euro);
- **2 amenzi** în baza Legii nr. 506/2004, în cuantum total de 80.000 lei;
- **1 amendă** în baza Legii nr. 190/2018, în cuantum total de 10.000 lei;
- **66 de avertismente**;
- **58 măsuri corective** în baza dispozițiilor art. 58 alin. (2) lit. c), d) și e) din GDPR;
- **3 avertizări.**

Măsurile corective dispuse în urma plângerilor și a investigațiilor din oficiu au constat, în special, în următoarele:

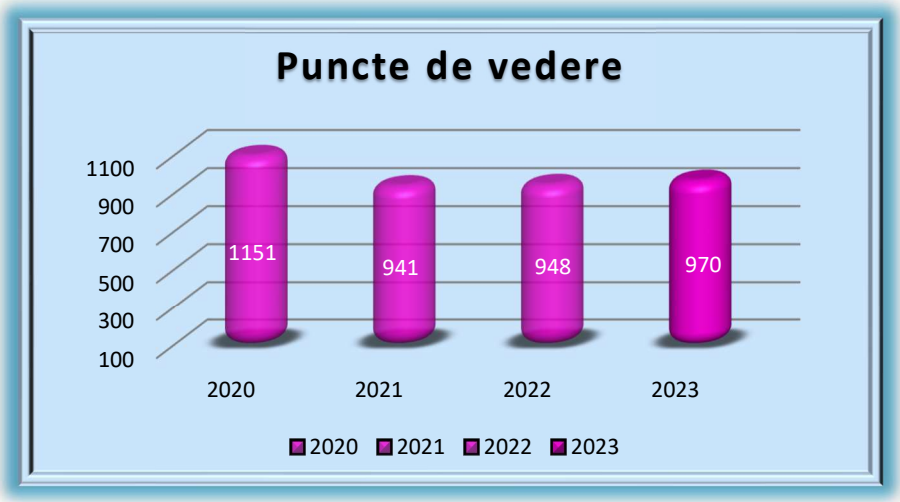
- asigurarea unei informări complete a persoanelor vizate pe site-ul operatorului, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, pe fiecare secțiune din site unde pot fi colectate/prelucrate date personale, prin raportare la dispozițiile art. 12-14 din GDPR, informarea urmând să fie, în principal, în limba română;

- punerea în aplicare a măsurilor tehnice și organizatorice adecvate pentru a demonstra că prelucrările de date pe care le efectuează sunt în conformitate cu GDPR, ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, inclusiv să revizuiască și să actualizeze aceste măsuri;
- reevaluarea măsurilor tehnice și organizatorice implementate, atât cu privire la gestionarea petițiilor transmise prin intermediul formularului de contact disponibil pe pagina de internet a operatorului, în cadrul sistemului informatic de petiții, cât și actualizarea procedurii operaționale privind activitatea de gestionare a petițiilor;
- realizarea instruirii angajaților cu privire la riscurile și consecințele pe care le implică dezvăluirea datelor personale, pentru evitarea unor incidente de securitate similare;
- asigurarea conformității cu prevederile GDPR a operațiunilor de colectare și prelucrare ulterioară a datelor personale, astfel încât să se evite dezvăluirea ilegală a datelor personale prelucrate; în acest sens, se va avea în vedere inclusiv aplicarea unor măsuri adecvate de securitate și confidențialitate (inclusiv pseudonimizarea, dacă este cazul), prin stabilirea unor proceduri clare privind transmiterea datelor personale către instanțele judecătorești și/sau justițiabili, instruirea regulată a persoanelor care prelucrează date sub autoritatea operatorului și implicarea corespunzătoare în aceste activități a responsabilului cu protecția datelor personale potrivit art. 37-39 din GDPR;
- implementarea unui mecanism procedurat și aplicat la intervale regulate de timp, privind testarea, evaluarea și aprecierea periodică a eficacității măsurilor adoptate, având în vedere riscul prezentat de prelucrare, în vederea asigurării unui nivel de securitate corespunzător și evitării pe viitor a unor incidente de securitate similare;

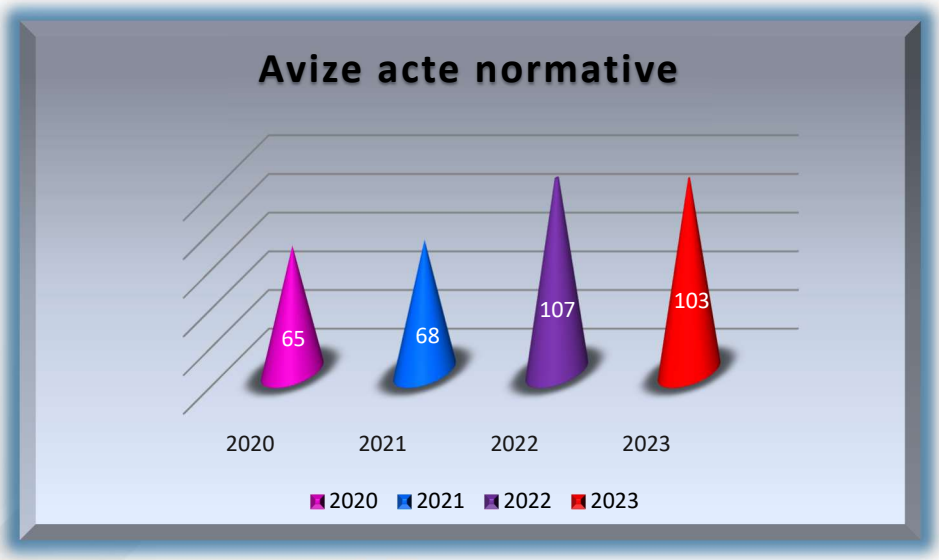
- adoptarea măsurilor tehnice și organizatorice adecvate, astfel încât operatorul să faciliteze exercitarea drepturilor persoanelor vizate, în special a dreptului de acces la o copie a datelor personale ce fac obiectul prelucrării, inclusiv prin utilizarea unor programe informatice care să permită editarea informațiilor de natură a aduce atingere drepturilor și libertăților altora (subl. ns. – in contextul utilizării sistemelor de supraveghere video de către operator);
- eliminarea utilizării camerelor de supraveghere video instalate în birouri și sala de mese pentru care nu există un temei legal expres de prelucrare a datelor personale ale angajaților săi conform art. 6 din GDPR.

C. Activitatea juridică, de consultare şi informare publică

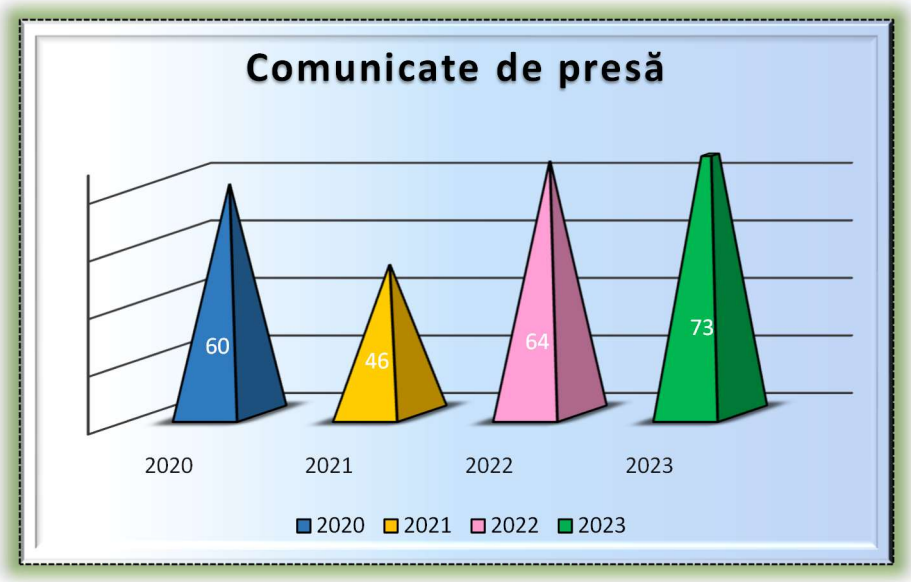
Pe parcursul **anului 2023** a fost adresat Autorității de Supraveghere un număr de **970 solicitări de emitere puncte de vedere** privind diverse aspecte referitoare la modalitatea de interpretare și aplicare a GDPR, de către operatori și împuterniciții acestora, din domeniul public și privat, de către alte entități, precum și de către persoane fizice.



De asemenea, în anul 2023, Autoritatea națională de supraveghere a emis **avize asupra unui număr de 103 proiecte de acte normative,** elaborate de instituții și autorități publice, care implicau aspecte complexe privind prelucrarea datelor cu caracter personal, în temeiul art. 57 alin. (1) lit. c) din GDPR.



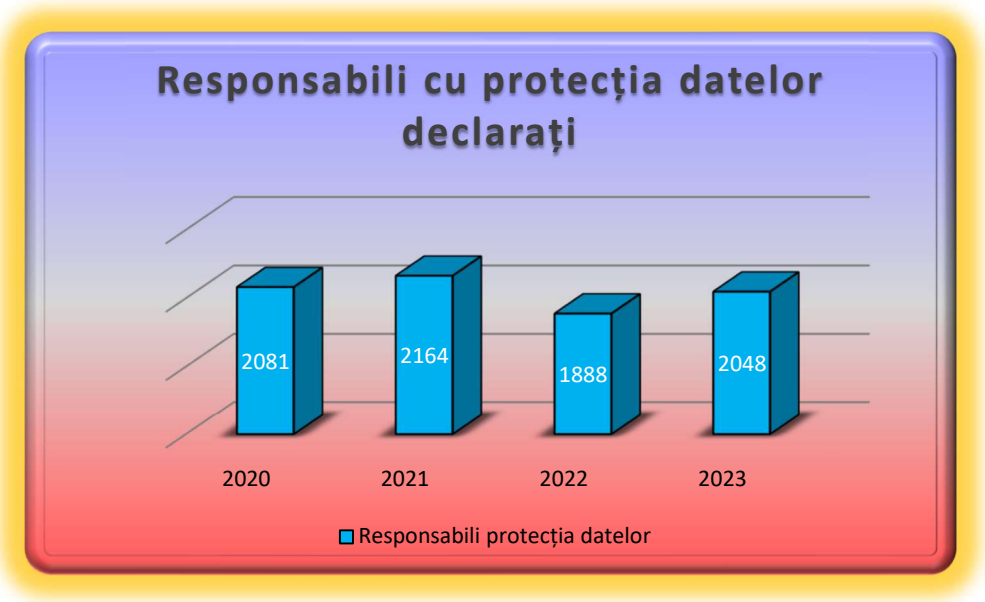
Autoritatea de supraveghere a realizat și în cursul anului 2023 o informare promptă şi eficientă cu privire la activitatea desfășurată, atât prin prisma celor **73 de comunicate de presă** postate pe site-ul instituției noastre la secțiunea „Știri”, cât și a informațiilor de la secțiunea specială dedicată GDPR.



În cursul anului 2023, au fost înregistrate pe rolul instanțelor de judecată un număr de **47 de cereri noi de chemare în judecată** întemeiate pe GDPR, pe Legea nr. 506/2004 sau pe Legea nr. 554/2004 a contenciosului administrativ.

D. Responsabilii cu protecția datelor

Operatorii au continuat să declare și în anul 2023, **responsabilii cu protecția datelor**, înregistrându-se la Autoritatea de Supraveghere un număr de **2048** responsabili numiți de către operatorii din domeniul public și privat.



A. Activitatea în domeniul relațiilor internaționale

În anul 2023, Autoritatea de Supraveghere a primit și a analizat cereri de aprobare a **BCRs transmise de 14 de companii multinaționale**. Instituția noastră a acționat în calitate de autoritate principală pentru **2 seturi** de reguli corporatiste obligatorii și a asistat alte autorități de supraveghere, acționând în calitate de co-revizor la cererile de aprobare a BCRs transmise **de 3 companii** în această perioadă.

De asemenea, Autoritatea de Supraveghere a avut calitatea de raportor principal pentru cerințele de acreditare a unui organism de monitorizare a codurilor de conduita in temeiul art. 41 din GDPR, iar de 3 ori a fost raportor pentru cerințele de acreditare a unui organism de monitorizare a codurilor de conduita in temeiul art. 41 din GDPR si pentru cerințele suplimentare pentru acreditarea organismelor de certificare in temeiul art. 43 din GDPR.

B. Orientări adoptate de Comitetul European pentru Protecția Datelor în cursul anului 2023

- Recomandările 1/2022 privind solicitarea de aprobare și la elementele și principiile ce trebuie conținute în Regulile Corporatiste Obligatorii pentru operator (art. 47 din GDPR);
- Orientările 4/2022 privind calcularea amenzilor administrative în temeiul GDPR;
- Orientările 3/2021 privind aplicarea art. 65 alin. (1) litera a) din GDPR;
- Orientările 5/2022 privind utilizarea tehnologiei de recunoaștere facială în domeniul asigurării respectării legii;
- Orientările 8/2022 pentru identificarea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator;
- Orientările 1/2022 privind drepturile persoanelor vizate – Dreptul de acces;
- Orientările 9/2022 notificarea încălcărilor de securitate in temeiul GDPR;
- Orientările 7/2022 privind certificarea ca instrument pentru transferuri;
- Orientările 5/2021 privind interacțiunea dintre aplicarea articolului 3 si dispozițiile referitoare la transferurile internaționale în conformitate cu capitolul V din GDPR;

- Orientările 3/2022 privind tipare nerecomandate în folosirea rețelelor de socializare: cum să le recunoști și să le eviți.

C. Avize comune ale Comitetul European pentru Protecția Datelor (CEPD) – Autoritatea Europeană pentru Protecția Datelor (AEPD) adoptate în cursul anului 2022

- Aviz comun EDPB-EDPS 1/2023 privind Propunerea de Regulament al Parlamentului European si al Consiliului de stabilire a unor norme procedurale suplimentare referitoare la asigurarea respectării GDPR;
- Aviz comun EDPB-EDPS 2/2023 referitor la propunerea de Regulament privind moneda euro digitală,

Mai multe informații referitoare la activitatea Autorității Naționale de Supraveghere și a Comitetului European pentru Protecția Datelor pot fi obținute accesând adresele de internet:

https://www.dataprotection.ro/

https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

A. The meaning of the European Data Protection Day

The European Data Protection Day is celebrated on the 28th of January 2024, which marks the 43rd anniversary of the adoption, in 1981, in Strasbourg, of Convention 108 for the protection of individuals with regard to automatic data processing of personal data.

This day represents an occasion to inform the large public on the personal data processing rules, but also to increase the degree of awareness of the data controllers in relation to the importance of the right to private life of the persons in the context of the digital era.

For the celebration of the European Data Protection Day, the National Supervisory Authority for the Processing of Personal Data organises, on the 26th of January 2024, the online conference with the theme "**The role and efficiency of the data protection officer's activity"**, with the participation of the representatives of national central public authorities and institutions, of the executive and legislative forum, of the academic representatives, non-governmental organisations, of the main professional unions/associations, as well as of other controllers/processors from the private and public sector.

A. The meaning of the European Data Protection Day

With this occasion, specific aspects regarding the processing of personal data, specifically in relation to the importance of the role of the data protection officer, will be brought to the attention of both the controllers and processors.

For the celebration of this event, **the informative video** dedicated to the General Data Protection Regulation will be broadcasted **on the national television TVR and in the means of public transport of the Bucharest Transport Company**.

At the same time, our institution proposed to the Ministry of Internal Affairs and to the Ministry of Foreign Affairs the organisation of events dedicated to the increase of the degree of information regarding the specific application of the data protection rules by the police personnel, respectively by the diplomatic and consular personnel, including in relation to the novelties brought by Regulations (EU) 2018/1860, 2018/1861, 2018/1862, applicable in the Schengen field.

B. The Data protection officer – essential role within the personal data processing mechanism

1. The designation of the data protection officer (Article 37 of the GDPR)

The designation of a data protection officer is **mandatory** when:

- the processing is carried out by a public authority or body (irrespective of the data that are processed);
- the core activities of the controller or the processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale;
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

"Core activities" represent the personal data protection processing operations performed for achieving the objectives of the controller of processor.

Examples:

- the processing of personal data, inclusively those on the health status, by an hospital, such as the medical records of the patients;
- the processing of personal data of the clients by a financial-banking institution.

In order to establish if **the processing is performed on a large scale**, the following aspects shall be taken into consideration:

- The number of data subjects;
- The volume of data;
- The duration or permanence of the data processing activity;
- Geographical surface of the processing activity.

B. The Data protection officer – essential role within the personal data processing mechanism

- Examples:

Large scale processing	Processing that is not on a large scale
processing of health data of the patients by a hospital	processing of personal data of the patients by an individual medical unit
the processing of personal data of the clients by an insurance company of a financial-banking company	the processing of personal data of the clients by an authorised natural person that performs an activity of intermediation of loans or an individual lawyer office

Publication and communication of the contact data of the data protection officer

The controllers or processors shall:

- publish the contact data of the data protection officer (for example: mail address, telephone number and/or e-mail address) and
- to communicate the contact data of the latter to the National Supervisory Authority for Personal Data Processing.

It is also recommended to inform the employees of the controller or, as the case may be, of the employees of the processor regarding the name and contact details of the officer. For example, the name and contact data could be communicated internally, within the intranet network of the controller or on the e-mail address of the employees.

B. The Data protection officer – essential role within the personal data processing mechanism

2. The role of the data protection officer (Article 38 of the GDPR)

The involvement of the data protection officer

In order to ease the compliance with the GDPR and to promote an adequate approach regarding the protection of the private life, the controller and processor shall ensure the fact that the data protection officer "is involved properly and in a timely manner in all issues which relate to the protection of personal data."

Ensuring the necessary resources

In order to allow to the data protection officer to efficiently fulfil his/her tasks, the controllers and processors shall provide the necessary resources.

Thus, depending on the nature of the processing operations, as well as on the activities and dimension of the organisation, the controller shall make available to the data protection officer the following resources:

- substantial support regarding the financial resources, the infrastructure (spaces, facilities, equipment) and personnel, as the case may be;
- sufficient time for fulfilling the tasks;
- continuous training by participating to training courses;
- the official communication regarding the designation of the officer to all the members of the personnel;
- considering the dimension and structure of the controller, it could be necessary to form a data protection officer team;
- active support from the high-level management personnel.

B. The Data protection officer – essential role within the personal data processing mechanism

The independence of the data protection officer

Safeguards that allow the officer to act independently:

- does not receive instruction from the controllers or processors in relation to the exercise of the tasks by the officer;
- is not dismissed or sanctioned by the controller in relation to the fulfillment of his/her tasks;
- shall directly report to the highest management level of the controller or the processor;
- there is no conflict of interest with other possible tasks and duties.

Conflict of interests

The data protection officer cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data.

Among the positions that can lead to some conflicts of interest can be included the positions of the high-level management personnel, such as:

- chief executive officer
- chief operating officer
- chief financial officer
- chief medical officer
- head of marketing department
- head of Human Resources o
- head of IT departments

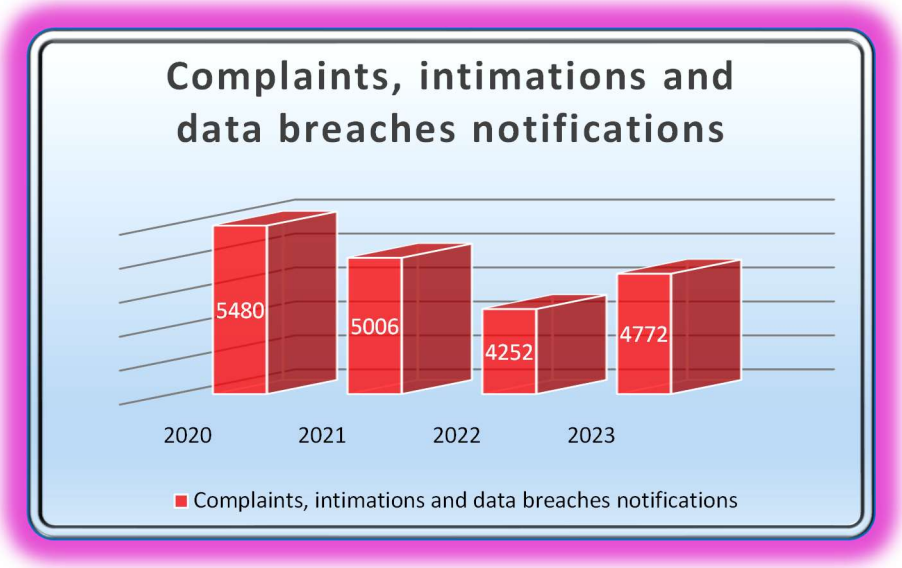
B. The Data protection officer – essential role within the personal data processing mechanism

More information is available within the "Guidelines on Data Protection Officer" issued by the European Data Protection Board in 2017, available on the Internet address of the authority, www.dataprotection.ro, under the section dedicated to the New Data Protection Regulation.

4. The tasks of the data protection officer (Article 39 of the GDPR)

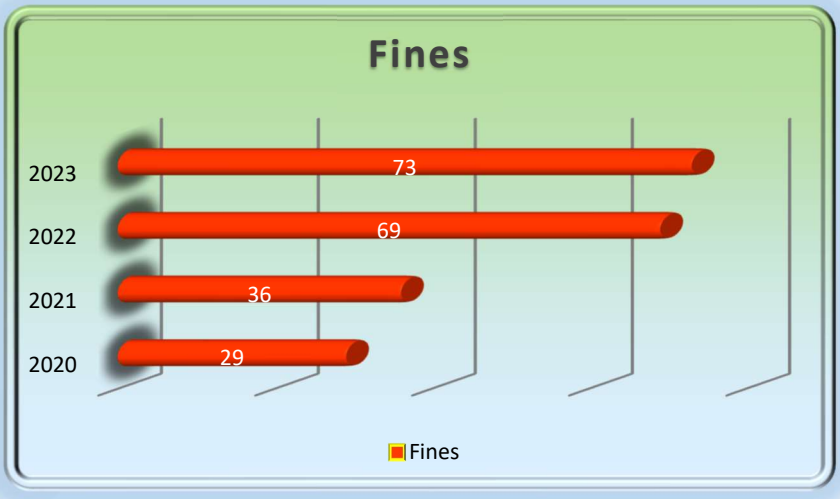
- to inform and advise the controller or, as the case may be, the processor in relation to their obligations pursuant to the GDPR;
- to monitor the compliance with the GDPR;
- to provide advice where requested as regards the data protection impact assessment;
- to cooperate with the supervisory authority.

During 2023, the National Supervisory Authority received a number of **4772** complaints, intimations and notifications of personal data breaches, based on which **548 investigations** were opened.

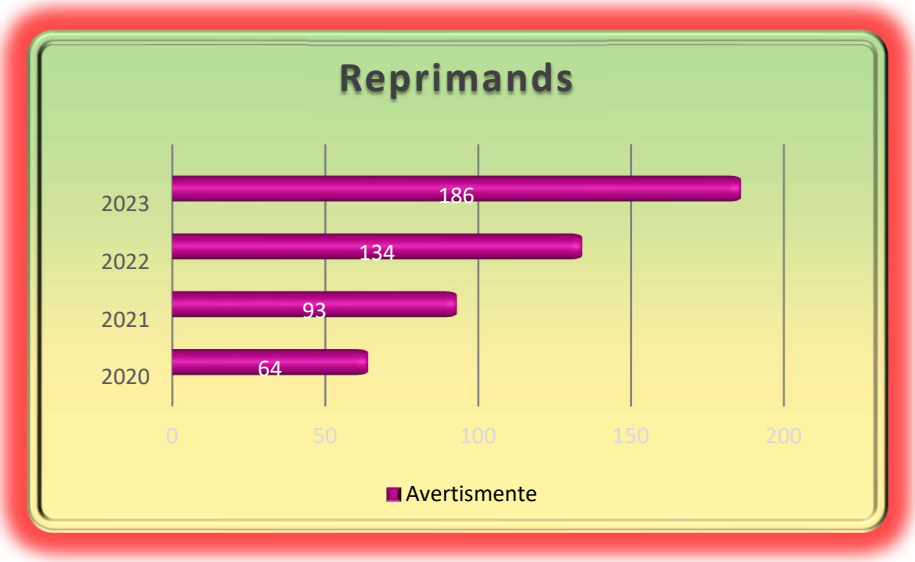


Following the investigations performed, the Supervisory Authority applied, during 2023, a total of **73 fines** with a total amount of **Lei 2,348,265.**

Out of these, **67 fines** were imposed based on the GDPR (in amount of **Lei 2,228,265 –** the equivalent of EUR 448,600), **4 fines** were imposed based on Law no. 506/2004 (in amount of **Lei 100,000)** and **2 fines** were imposed based on Law no. 190/2018 in amount of **Lei 20,000.**

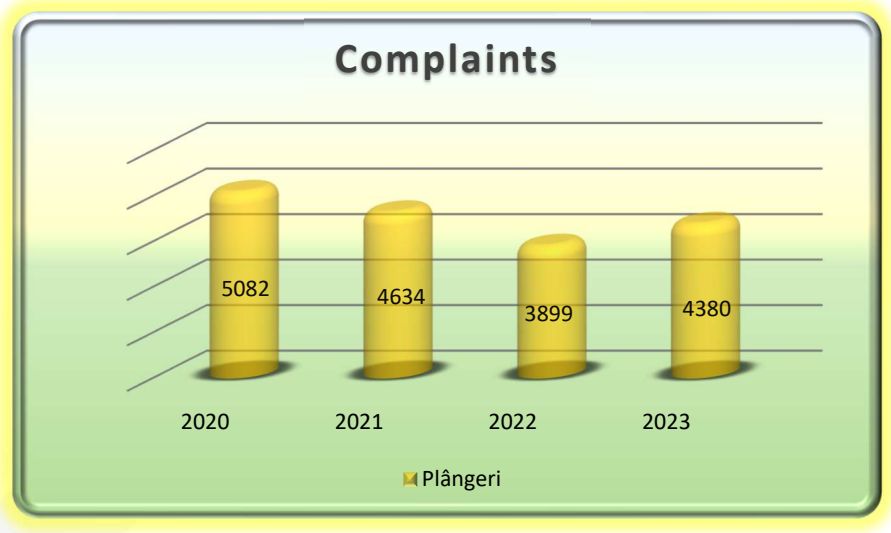


Also, during 2023, **186 reprimands** were applied and **138 corrective measures** were ordered.



A. The activity of handling complaints

With regards to the activity of handling complaints, the Supervisory Authority received **in 2023** a total number of **4380** complaints, based on which **207 investigations** were initiated.



II. The monitoring and control activity

The complaints received by the Supervisory Authority in 2023 were referring, in particular, to the following:

- the processing of personal data by infringing the provisions of Articles 5 and 6 of the GDPR;
- the infringement of the data subjects' rights, in particular of the right of access of the data subject and the right to erasure of his/her data;
- the infringement of security and confidentiality measures for the processing of personal data.

Following the **investigations performed based on the complaints,** the following **sanctions** were imposed:

- **36 fines** based on the GDPR in total amount of Lei 687,102.38 lei (the equivalent EUR 138,700);
- **2 fines** based on Law no. 506/2004, in total amount of Lei 20,000;
- **1 fine** based on Law no. 190/2018, in total amount of Lei 10,000;
- **120 reprimands**;
- **80 corrective measures** based on the provisions of Article 58 paragraph (2) letters c) and d) and e) of Regulation (EU) 2016/679.

B. The control activity following the receipt of notifications of personal data breach and intimations

With regard to the security breaches, the controllers submitted, in **2023,** a number of **181 notifications for the breach of the data security** (180 breaches of the GDPR and 1 breach of Law no. 506/2004) and the intimations regarding possible non-compliance with the provisions of Regulation (EU) 2016/679 were in amount of **211.**

The security breaches referred, in particular, to the following aspects:

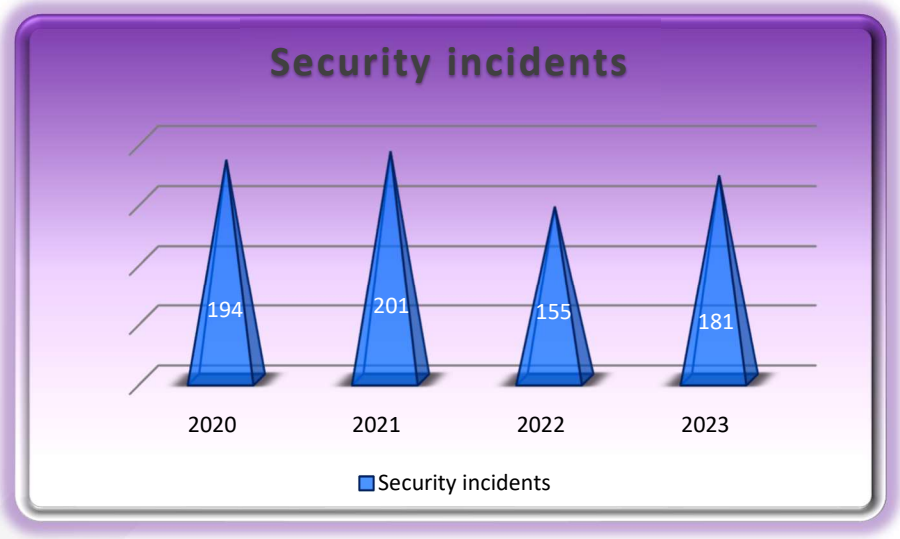
- confidentiality/availability/integrity of the personal data affected especially following the unauthorised disclosure or following a ransomware informatic attack incident;
- confidentiality of personal data in the online environment following the poor configuration of the websites/computer applications used by the controllers;
- the processing of personal data of the clients from the banking sector;
- the disclosure of personal data in the online environment, specifically on social media;
- unauthorised access to the video surveillance systems with closed circuit (CCTV);
- disclosure of personal data processed within the medical system.

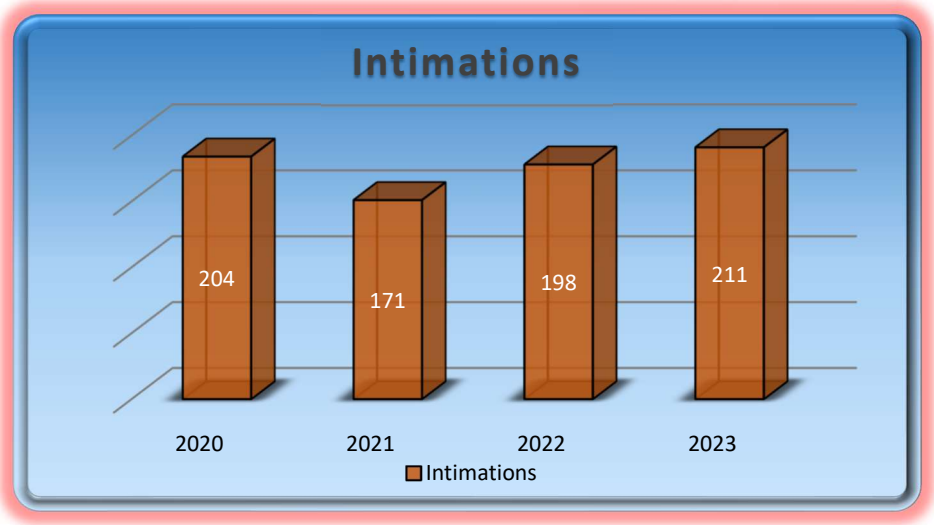
B. The control activity following the receipt of notifications of personal data breach and intimations

The intimations received were referring, in particular, to the following aspects:

- the infringement of the data processing principles provided by the GDPR;
- the disclosure of personal data without the consent of the data subjects;
- the confidentiality of personal data in the online environment, following the poor configuration of the websites/informatic applications used by the controllers;
- the publication/disclosure of personal data in the online environment, especially on social platforms;
- the processing of images through the video surveillance systems, inclusively though mobile video surveillance means (body-cam);
- the infringement of security and confidentiality measures for the processing of personal data, given that the controllers did not adopt the appropriate technical and organisational measures regarding the security of the processing.

The evolution of the security incidents and intimations in 2023 can be noted in the graphics presented below, as follows:





Based on the **intimations** received and **the security breaches** notified by the personal data controllers, during 2023, the Supervisory Authority initiated a number of **341 ex officio investigations.**

Following the **investigations performed,** during 2023, were applied:

- **31 fines** based on the GDPR in total amount of Lei 1,541,163 lei (the equivalent of EUR 309,900);
- **2 fines** based on Law no. 506/2004, in total amount of Lei 80,000;
- **1 fine** based on Law no. 190/2018, in amount of Lei 10,000;
- **66 reprimands**;
- **58 corrective measures** based on the provisions of Article 58 paragraph (2) letters c), d) and e) of the GDPR;
- **3 warnings.**

The corrective measures imposed following the complaints and ex officio investigations have addressed, in particular, the following:

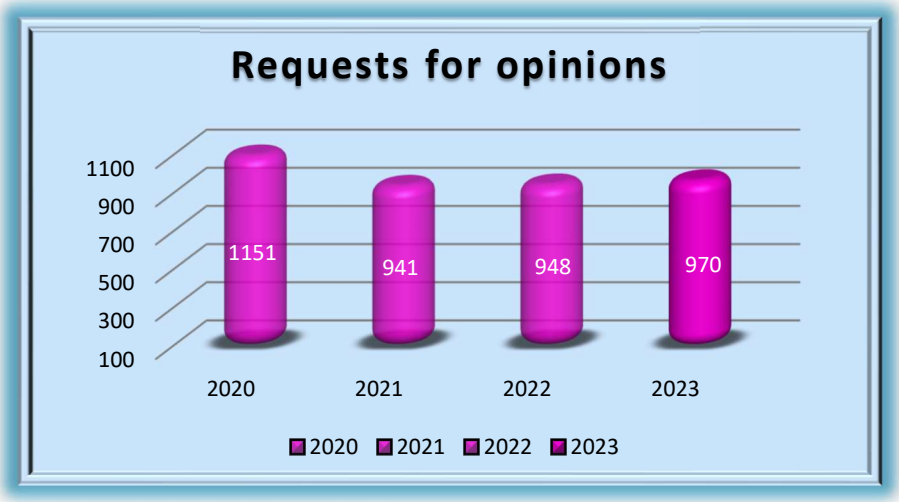
- ensuring a complete information of the data subjects on the website of the controller, in a concise, transparent, intelligible and easily accessible language, on each section from the website where personal data can be collected/processed, by reference to the provisions of Articles 12-14 of the GDPR, the information following to be, mainly, in Romanian;

- implementing the adequate technical and organisational measures in order to prove that the data processing operations performed are in compliance with the GDPR, considering the nature, scope, context and purposes of the processing, inclusively to review and update these measures;
- re-evaluating the technical and organisational measures implemented, both in relation to the handling of the requests provided through the contact form available on the internet page of the controller, within the informatic system for requests and the update of the operational procedure for the complaints handling activity;
- performing the training of the employees in relation to the risks and consequences that the disclosure of personal data implies, in order to avoid some similar security incidents;
- ensuring the compliance with the GDPR provisions of the onward collection and processing of personal data, so as to avoid the illegal disclosure of the personal data processed; in this respect, the implementation of some adequate security and confidentiality measures will be also taken into consideration (inclusively the pseudonymisation, as the case may be), by establishing clear procedures for the submission of personal data to the judicial courts and/or justice seekers, the regular training of the persons processing data under the authority of the controller and the corresponding involvement in these activities of the data protection officer according to Articles 37-39 of the GDPR;
- implementing a procedure mechanism and applied at regular time intervals, regarding the testing, evaluation and periodical assessment of the efficiency of the measures adopted, considering the risk presented by the processing, in order to ensure a corresponding level of security and to further avoid some similar security incidents;

- adopting adequate technical and organisational measures, in order for the controller to facilitate the exercise of the data subjects' rights, specifically of the right of access to a copy of the personal data that are subject to the processing, inclusively by using some informatic systems that allow the editing of the information able to infringe the rights and freedoms of others (our highlight - in the context of the use of the video surveillance systems by the controller);
- removing the video surveillance cameras installed in the offices and dining room for which there is no specific legal basis for the processing of the personal data of the employees according to Article 6 of the GDPR.

C. The legal, advisory and public information activity

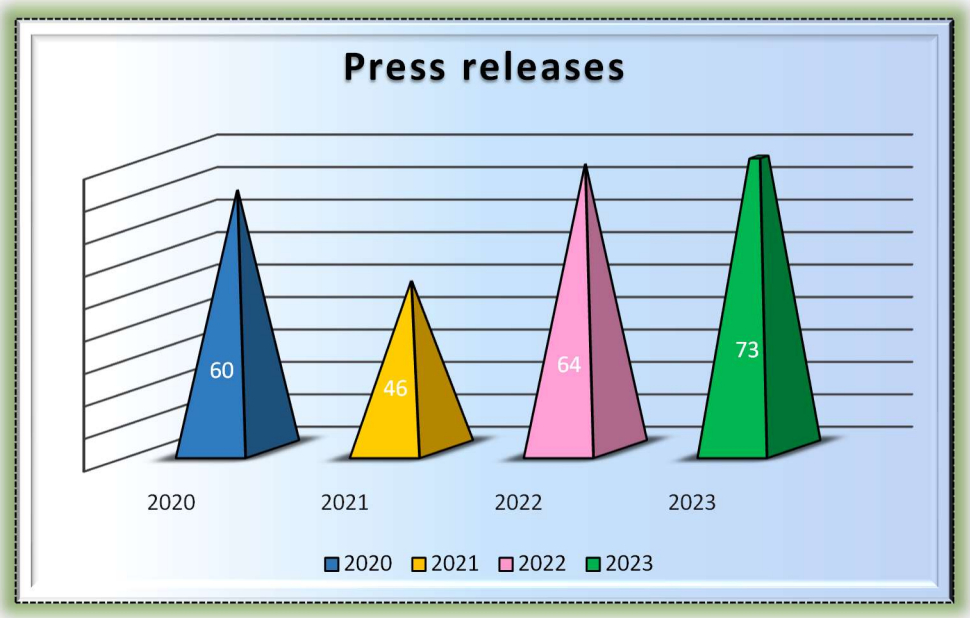
During **2023,** the Supervisory Authority received a number of **970 requests for opinions** in relation to various aspects regarding the interpretation and application of the GDPR, from the controllers and processors of public and private sector, from other entities, as well as from natural persons.



Also, in 2023, the Supervisory Authority issued **opinions on a number of 103 proposal of legal acts,** drafted by public institutions and authorities, which involved complex aspects regarding the processing of personal data, pursuant to Article 57 paragraph (1) letter c) of the GDPR.

II. The monitoring and control activity

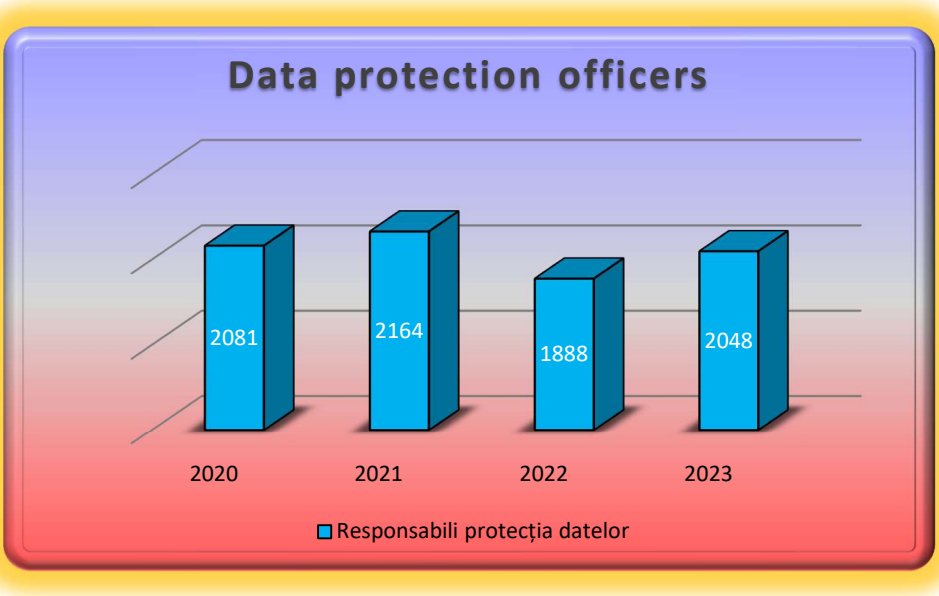
During 2023, the Supervisory Authority also provided prompt and efficient information regarding the activity carried out, both through the **73 press releases** posted on the website of our institution under section "News", as well as through the information from the section dedicated to the GDPR.



In the course of 2023, **47 new summons applications** based on the GDPR, on Law no. 506/2004 or on Law no. 554/2004 of the administrative litigation were received.

D. Data protection officers

The controllers continued to notify the **data protection officers** in 2023 as well, thus, a number of **2048** officers appointed by the public and private controllers being registered at the Supervisory Authority.



A. Foreign affairs activity

In 2023, the Supervisory Authority received and assessed the application forms for approval of the **Binding Corporate Rules submitted by 14 multinational companies**. Our institution acted as lead authority for **2 sets** of binding corporate rules and assisted other supervisory authorities by acting as co-reviewer of the BCRs approval requests submitted, during this period, by **3 companies**.

Also, the Supervisory Authority acted as lead rapporteur for the criteria for accreditation of a monitoring body for the codes of conduct based on Article 41 of the GDPR, and 3 times was rapporteur for the criteria for accreditation of a monitoring body for the codes of conduct based on Article 41 of the GDPR and for the additional criteria for the accreditation of the certification bodies based on Article 43 of the GDPR.

B. Guidelines adopted by the European Data Protection Board during 2023

- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)
- Guidelines 04/2022 on the calculation of administrative fines under the GDPR
- Guidelines 03/2021 on the application of Article 65(1)(a) GDPR
- Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement
- Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority
- Guidelines 01/2022 on data subject rights - Right of access
- Guidelines 9/2022 on personal data breach notification under GDPR
- Guidelines 07/2022 on certification as a tool for transfers
- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

- Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them

C. Joint opinions of the European Data Protection Board (EDPB) – European Data Protection Supervisor (EDPS) adopted during 2023

- EDPB-EDPS Joint Opinion 01/2023 on the Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of the GDPR
- EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro

More information on the activity of the National Supervisory Authority and of the European Data Protection Board can be obtained by accessing the following link:

https://www.dataprotection.ro/

https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
Bulevardul G-ral. Gheorghe Magheru 28 -30, sector 1, București
Tel. +40.318.059.211
Email: anspdcp@dataprotection.ro

www.dataprotection.ro