

Informații privind protecția datelor

Informații privind protecția datelor pentru raportarea și investigarea încălcărilor de conformitate

I. Responsabilul și scopul prelucrării datelor cu caracter personal

Noi, BSH Hausgeräte GmbH, Carl-Wery-Strasse 34, 81739 München, Germania („**BSH HQ**” sau „**Noi**”) și entitățile BSH din Uniunea Europeană, Norvegia, Elveția și Regatul Unit (denumite în continuare „**Entitate BSH**”), suntem furnizorii serviciilor descrise în prezentul document, inclusiv prelucrarea corespunzătoare a datelor cu caracter personal.

În scopul gestionării și investigării acuzațiilor de încălcări ale conformității („Gestionarea acuzațiilor și investigațiile de conformitate”), noi și entitatea BSH respectivă acționăm în calitate de operatori asociați (a se vedea art. 26 din RGPD), deoarece stabilim în comun scopurile și mijloacele de prelucrare a datelor dvs. cu caracter personal.

Noi și Entitatea BSH oferim diferite canale de raportare pentru a transmite rapoarte privind potențiale cazuri de neconformitate, atât la nivel central, cât și local:

- Sistemul de denunțare „Trust and Tell” (TnT)
- Avocat de încredere (LoT)
- Responsabilul local cu conformitatea (LCO), situat la sediul central al BSH sau la entitatea BSH respectivă.

Prezenta Informație privind protecția datelor vă informează (denumit în continuare „Dvs.”) cu privire la prelucrările relevante ale datelor cu caracter personal în cadrul gestionării acuzațiilor și al investigațiilor de conformitate.

II. Principiile noastre privind protecția datelor

În contextul furnizării serviciilor descrise în prezentul document și al funcționării site-urilor web și a altor puncte de contact, prelucrăm datele dvs. cu caracter personal în diferite moduri. Vă informăm cu privire la fiecare prelucrare a datelor cu caracter personal, precum și la temeiul juridic și principiile respective în baza cărora are loc această prelucrare.

Ne angajăm să vă protejăm datele cu caracter personal. Prin urmare, prelucrăm datele dvs. cu mare atenție și în strictă conformitate cu legile aplicabile privind protecția datelor și cu permisiunile individuale pe care ni le-ați acordat. Am luat măsuri de securitate organizaționale și tehnice pentru a proteja toate site-urile noastre web, aplicațiile și alte puncte de contact (digitale) împotriva riscurilor potențiale prezente în prelucrarea datelor cu caracter personal. Companiile din grupul nostru și partenerii care ne sprijină în furnizarea serviciilor trebuie, de asemenea, să respecte aceste reguli și principii.

Vă rugăm să utilizați informațiile de contact furnizate în această Informație privind protecția datelor pentru a ne contacta, fie în general, fie cu întrebări și/sau solicitări specifice privind protecția datelor. Există diferite legi care reglementează protecția datelor, în funcție de țara în care vă aflați. Pe baza principiilor Regulamentului general european privind protecția datelor, și anume **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, privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE („GDPR”), am definit următoarele principii de bază ca linii directoare privind modul în care prelucrăm și protejăm datele dvs. cu caracter personal atunci când vă punem la dispoziție site-urile și serviciile noastre:

1. Legalitate

Utilizăm datele cu caracter personal numai dacă această utilizare este legală, ceea ce, în cazul gestionării acuzațiilor și al investigării încălcărilor de conformitate raportate, se bazează pe următoarele temeiuri juridice:

- **Art. 6 alin. 1 lit. c) RGPD:** În Europa, implementarea unui sistem de gestionare a sesizărilor este o obligație legală care decurge din Directiva europeană privind sesizările (Regulamentul (UE) 2019/1937) și din legile naționale de transpunere privind protecția denunțătorilor. Directiva permite prelucrarea datelor cu caracter personal, care este necesară pentru gestionarea unei sesizări în conformitate cu legislația.
- **Art. 6 alin. 1 lit. f) RGPD:** Prelucrarea datelor cu caracter personal în sistemul BKMS® se bazează pe interesele legitime ale companiei noastre de a detecta și preveni abaterile și, astfel, de a evita prejudiciile aduse BSH, angajaților și clienților săi, **precum și de a urmări infracțiunile penale, de a formula pretenții civile și de a preveni încălcările normelor de reglementare.**

Pentru toate prelucrările de date cu caracter personal descrise în prezentul document, vom furniza, de asemenea, temeiul juridic al prelucrării în descrierea relației specifice de operator comun între noi și entitatea BSH respectivă, în secțiunea IV a prezentei informații privind protecția datelor.

2. Corectitudine și transparență

Vă vom informa despre datele cu caracter personal pe care le colectăm și motivul pentru care le colectăm într-un mod echitabil și transparent în prezenta informare privind protecția datelor. Puteți accesa informarea privind protecția datelor direct sau printr-un link atunci când vă înregistrați și/sau la orice punct de contact în care interacționați cu noi. Utilizatorii cu vârsta sub 16 ani ar trebui să ne transmită date cu

caracter personal numai cu consimțământul părintelui sau tutorelui legal. Legislația privind protecția datelor aplicabilă în țara dumneavoastră poate prevedea limite de vârstă diferite în acest sens.

3. Limitarea scopului și minimizarea datelor

Colectăm și utilizăm numai datele cu caracter personal de care avem cu adevărat nevoie și în scopul pentru care ne-ați furnizat datele cu caracter personal. Dacă putem atinge scopul cu mai puține date cu caracter personal, vom utiliza numai datele minime necesare. Cu toate acestea, în orice moment, sunteți liber să furnizați date cu caracter personal suplimentare, dacă acest lucru ar îmbunătăți experiența dvs. cu serviciile furnizate.

4. Tipuri de prelucrare, inclusiv terțe părți

În cazurile în care nu prelucrăm datele dvs. cu caracter personal direct în calitate de operator de date (de exemplu, găzduirea site-ului web, servicii tehnice etc.), încheiem contracte cu terți care furnizează aceste servicii în numele nostru în calitate de procesatori de date. Aceste contracte îi obligă la prelucrarea datelor dvs. cu caracter personal pentru a asigura legalitatea și securitatea prelucrării. Aceasta se numește relație între operator și persoană împuternicită de operator și este definită în art. 28/29 din RGPD, unde noi suntem operatorul, iar terțul respectiv este persoana împuternicită de operator. Veți găsi o listă a persoanelor împuternicite de operator pe care le angajăm la sfârșitul acestei Informații privind protecția datelor.

Gestionarea în comun descrie situația în care mai multe părți, dintre care facem parte și noi, colaborează pentru a decide modul în care vor fi utilizate și gestionate datele (operatori comuni, a se vedea art. 26 din RGPD). Operatorii comuni trebuie să informeze în mod clar cu privire la cine prelucrează ce date cu caracter personal și ce obligații și-a asumat fiecare parte în ceea ce privește normele aplicabile de protecție a datelor. Pe măsură ce operatorii asociați se pun de acord asupra rolurilor lor și se asigură că persoanele vizate (persoanele despre care se referă datele) sunt informate cu privire la aceste roluri, vă vom informa cu privire la aceste roluri și la drepturile dvs. individuale pentru fiecare dintre situațiile de control comun descrise în prezentul document. Atunci când utilizăm un serviciu sau un partener terț, care prelucrează date cu caracter personal în calitate de operator comun, vă vom informa cu privire la drepturile și rolurile corespunzătoare în lista furnizorilor terți din secțiunea IV, la sfârșitul acestui document.

5. Securitate

Vom prelucra datele dvs. într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale, utilizând măsuri tehnice sau organizatorice adecvate. În cazul în care utilizăm terți pentru prelucrarea datelor cu caracter personal, îi obligăm pe acești terți să respecte un nivel adecvat de măsuri tehnice sau organizatorice.

6. Drepturile utilizatorului

Aveți următoarele drepturi față de noi, pe care le respectăm în timp util și în mod corespunzător, imediat după primirea cererii dumneavoastră, după cum se precizează mai jos:

- **Dreptul dumneavoastră de a solicita accesul la datele dumneavoastră cu caracter personal în conformitate cu articolul 15 din RGPD:** Vă vom informa dacă deținem date cu caracter personal despre dumneavoastră și, în caz afirmativ, vă vom oferi acces la aceste date și informații despre ele.

- **Dreptul dumneavoastră de a solicita rectificarea datelor dumneavoastră în conformitate cu art. 16 din RGPD:** Vom corecta informațiile inexacte sau vom completa datele personale incomplete, cu condiția ca aceste date să fie necesare pentru scopul prevăzut al prelucrării datelor dumneavoastră.
- **Dreptul dumneavoastră de a solicita ștergerea datelor dumneavoastră în conformitate cu art. 17 din RGPD:** Vom șterge datele personale pe care le deținem despre dumneavoastră. Cu excepția cazului în care aceste date fac obiectul unor perioade de păstrare sau drepturi de păstrare, de exemplu deoarece trebuie să păstrăm datele dumneavoastră pentru a ne îndeplini obligațiile contractuale sau conform cerințelor legii.
- **Dreptul dumneavoastră de a solicita restricționarea prelucrării datelor dumneavoastră în conformitate cu art. 18 din RGPD:** În cazurile prevăzute la art. 18 (1) din RGPD, ne puteți solicita să blocăm datele dumneavoastră. Vom prelucra datele blocate doar într-o măsură foarte limitată și dacă este necesar pentru a furniza astfel de servicii sau a îndeplini obligații, a căror executare este necesară după blocarea datelor dumneavoastră solicitată de dumneavoastră.
- **Dreptul dumneavoastră de a retrage consimțământul în conformitate cu art. 7 (3) din RGPD:** Pentru prelucrările de date care necesită consimțământul dumneavoastră, vă puteți retrage consimțământul în orice moment pentru a împiedica prelucrarea viitoare a datelor dumneavoastră. Prelucrările de date bazate pe consimțământul dumneavoastră anterior retragerii rămân valabile și legale.
- **Dreptul dumneavoastră de a vă opune prelucrării datelor dumneavoastră în conformitate cu art. 21 din RGPD:** Vă puteți opune prelucrării viitoare a datelor dumneavoastră, dacă prelucram datele dumneavoastră pe baza uneia dintre justificările legale prevăzute la articolul 6 (1e sau 1f) din RGPD. Dacă vă opuneți, vom înceta prelucrarea datelor dumneavoastră, cu excepția cazului în care avem motive legitime și imperioase pentru continuarea prelucrării care prevalează asupra intereselor și drepturilor dumneavoastră sau pentru constatarea, exercitarea sau apărarea unor drepturi în instanță. Prelucrarea datelor dumneavoastră în scopul marketingului direct nu constituie niciodată un motiv legitim și imperios pentru noi.
- **Dreptul dumneavoastră la portabilitatea datelor în conformitate cu art. 20 din RGPD:** În cazul în care prelucrarea datelor se efectuează prin mijloace automatizate și se bazează pe consimțământ sau contract, vă putem furniza datele pe care ni le-ați furnizat într-un format structurat, utilizat în mod obișnuit și care poate fi citit automat.
- **Dreptul dumneavoastră de a depune o plângere la o autoritate de reglementare:** Puteți depune o plângere referitoare la protecția datelor la o autoritate de protecție a datelor. Pentru a face acest lucru, contactați autoritatea de protecție a datelor relevantă care este responsabilă pentru locul dumneavoastră de reședință sau autoritatea de protecție a datelor sub a cărei jurisdicție ne aflăm (menționată mai jos în Lista autorităților de protecție a datelor).

7. Principii de ștergere

În principiu, stocăm datele dvs. atât timp cât este necesar pentru a investiga incidentul de conformitate la care se referă raportul dvs. După finalizarea investigației și expirarea perioadei de păstrare aplicabile, vom șterge datele dvs. cu caracter personal, cu excepția datelor a căror stocare ulterioară este necesară pentru stabilirea, exercitarea sau apărarea drepturilor legale. Ștergerea acestor date este reglementată de termenele maxime de prescripție prevăzute de legile aplicabile.

8. Responsabilul cu protecția datelor

Dacă aveți întrebări cu privire la protecția datelor sau dacă doriți să vă exercitați drepturile, responsabilul nostru cu protecția datelor (DPO) vă stă la dispoziție pentru a vă ajuta. Puteți lua legătura cu DPO-ul nostru direct, trimițând o scrisoare sau un e-mail folosind datele de contact furnizate mai jos:

- **Dacă sunteți rezident într-un stat membru al UE/SEE, vă rugăm să contactați:**
BSH Hausgeräte GmbH, Responsabilul cu protecția datelor, Carl-Wery-Str. 34, 81739 München, Germania, Data-Protection-DE@bshg.com
- **Dacă sunteți rezident în Regatul Unit, vă rugăm să contactați:**
BSH Home Appliances Limited, Responsabilul cu protecția datelor, Grand Union House, Old Wolverton Road, Wolverton, Milton Keynes, MK12 5PT, Data-Protection-UK@bshg.com
- **Dacă sunteți rezident în Elveția, vă rugăm să contactați:**
BSH Hausgeräte AG, Reprezentant pentru Home Connect GmbH, BSH Hausgeräte AG, Fahrweidstrasse 80, CH-8954 Geroldswil, Data-Protection-CH@bshg.com

9. Modificări ale prezentei Informații privind protecția datelor

Prezenta Informație privind protecția datelor reflectă starea actuală a prelucrării datelor pe site-ul nostru web și în alte puncte de interacțiune. În cazul modificărilor aduse prelucrării datelor, prezenta Informație privind protecția datelor va fi actualizată în consecință. Punem întotdeauna la dispoziție cea mai recentă versiune a prezentei Informații privind protecția datelor pe site-ul nostru web, astfel încât să puteți fi informat cu privire la domeniul de aplicare al prelucrării datelor prin intermediul acestui site web.

III. Gestionarea reclamațiilor și investigarea conformității

1. Prelucrarea datelor

a. Gestionarea plângerilor și investigațiile de conformitate

Partea care primește sesizările („**Partea destinatară**”) poate fi fie noi, fie entitatea BSH respectivă și este responsabilă de primirea inițială și documentarea sesizărilor, asigurând confidențialitatea și trimiterea unei confirmări de primire către denunțator, acolo unde este posibil, precum și de determinarea responsabilului pentru subiectul respectiv și a oportunității desfășurării unei investigații, protejând în același timp drepturile denunțătorilor și ale persoanelor acuzate. Partea care efectuează investigațiile („**Partea care investighează**”) poate fi fie noi, fie entitatea BSH respectivă și este responsabilă de investigațiile aprofundate, inclusiv de abordarea sau punerea în aplicare a măsurilor ulterioare, de documentarea corespunzătoare și de raportarea finală. Ambele părți își vor coordona acțiunile pentru a asigura transparența și respectarea cerințelor privind protecția datelor.

În cadrul controlului comun, părțile sunt responsabile de prelucrarea datelor cu caracter personal după cum urmează:

- **Acțiunea A (Partea primitoare):** Această parte gestionează primirea inițială a rapoartelor de denunțare, inclusiv comunicarea cu denunțatorul, efectuarea verificărilor inițiale de plauzibilitate și clasificarea obiectului, precum și documentarea cazului în vederea predării.
- **Acțiunea B (Partea care investighează):** Această parte efectuează investigația aprofundată a abaterilor plauzibile, inclusiv verificări suplimentare și documentarea tuturor datelor și constatărilor anchetei.

b. Coordonare, documentare finală și analiză

În cadrul controlului comun, părțile sunt responsabile de prelucrarea datelor cu caracter personal pentru coordonarea, închiderea și analizarea rapoartelor primite și a investigațiilor de conformitate efectuate, după cum urmează:

- **Acțiunea C:** Coordonăm procesul general oferind îndrumări privind investigațiile și creând rapoarte analitice finale pentru părțile interesate interne și externe.

- **Acțiunea D:** Entitatea BSH respectivă este responsabilă de gestionarea centralizată a ciclului de viață al tuturor datelor, inclusiv pregătirea, stocarea și ștergerea rapoartelor de denunțare și a datelor privind investigațiile de conformitate din sistemele IT centrale.

2. Tratarea confidențială a sesizărilor și transferul de date

Rapoartele primite sunt preluate de un grup restrâns de angajați autorizați în mod expres și special instruiți și sunt întotdeauna tratate în mod confidențial. În cadrul procesării unui raport, poate fi necesar să îl redirecționăm către angajații responsabili de la sediul central al BSH sau către entitatea BSH respectivă. Informațiile dvs. vor fi accesibile numai acelor angajați care au nevoie de ele pentru a procesa raportul dvs. și numai în măsura permisă de legile privind protecția denunțătorilor. Toate persoanele care au acces la raportul dvs. sunt obligate să păstreze confidențialitatea. Datele pot fi, de asemenea, transferate către alte organisme responsabile (de exemplu, autorități publice) dacă suntem obligați legal să facem acest lucru și în măsura permisă de legile privind protecția denunțătorilor.

3. Utilizarea sistemului de denunțare „Trust and Tell”

a. Punerea la dispoziție a site-ului web.

Serviciul „Trust and Tell” este furnizat prin intermediul unui site web operat de un furnizor de servicii extern specializat, EQS Group GmbH, în numele nostru. Comunicarea dintre computerul dumneavoastră și sistemul BKMS® pentru raportarea conformității are loc printr-o conexiune criptată (TLS).

b. Despre serviciu

Sistemul de raportare „Trust and Tell” are scopul de a primi, procesa și gestiona în mod sigur și confidențial rapoartele privind încălcările de conformitate din cadrul sau legate de noi și/sau de entitatea BSH respectivă.

Utilizarea sistemului de raportare se face pe bază de voluntariat. Este posibilă configurarea unei căsuțe poștale în cadrul sistemului de raportare, securizată cu un pseudonim/nume de utilizator și o parolă alese individual. Acest lucru vă permite să trimiteți rapoarte către angajatul responsabil din cadrul companiei noastre sau al entității BSH respective, fie pe nume, fie în mod anonim și sigur. Acest sistem stochează date numai în interiorul sistemului de raportare, ceea ce îl face deosebit de sigur. Nu este o formă de comunicare obișnuită prin e-mail.

Atunci când trimiteți o sesizare sau o completare, puteți trimite simultan atașamente către angajatul responsabil din cadrul companiei noastre sau al entității BSH respective. Dacă doriți să trimiteți o sesizare anonimă, vă rugăm să luați în considerare următoarele recomandări de securitate: fișierele pot conține date personale ascunse care ar putea compromite anonimatul dumneavoastră. Ștergeți aceste date înainte de a le trimite. Dacă nu puteți șterge aceste date sau nu sunteți sigur cum să procedați, copiați textul atașamentului în textul sesizării.

c. Adresa IP, cookie-uri etc.

Sistemul de raportare nu înregistrează date privind adresa IP, marcaje de timp sau metadate referitoare la utilizarea sa de către denunțători.

În timpul utilizării BKMS® Incident Reporting, serverul nu este capabil să identifice în mod unic clientul (computerul utilizatorului). Pentru a putea identifica în mod clar clientul în timpul unei

sesiuni, aplicația transmite un cookie de sesiune către computerul utilizatorului. Acest cookie de sesiune este utilizat numai pentru conexiunea curentă și are doar un număr de identificare pentru sesiunea în curs. Acest cookie este șters odată ce browserul este închis. Acest număr de sesiune nu are nicio legătură cu denunțatorul sau cu datele transmise și este necesar doar din motive tehnice.

IV. Lista furnizorilor terți și a operatorilor asociați, precum și utilizarea acestora

Partea care primește rapoartele poate fi fie noi, fie entitatea BSH respectivă și este responsabilă de primirea inițială și documentarea rapoartelor, asigurând confidențialitatea și trimiterea unei confirmări de primire către denunțator, acolo unde este posibil, precum și de determinarea responsabilului pentru subiectul respectiv și de oportunitatea desfășurării unei investigații, protejând în același timp drepturile denunțatorilor și ale celor acuzați. Partea care efectuează investigațiile poate fi fie noi, fie entitatea BSH respectivă și este responsabilă de investigațiile aprofundate, inclusiv de abordarea sau punerea în aplicare a măsurilor ulterioare, de documentarea corespunzătoare și de raportarea finală. Ambele părți își vor coordona acțiunile pentru a asigura transparența și respectarea cerințelor privind protecția datelor.

În cadrul controlului comun, părțile sunt responsabile de prelucrarea datelor cu caracter personal pentru gestionarea acuzațiilor și investigarea conformității, după cum urmează:

Obligații în temeiul RGPD al UE, RGPD al Regatului Unit și FADP elvețian) <i>Partea responsabilă bifează în tabelul de mai jos responsabilitatea care îi revine</i>	Domeniul de aplicare al acțiunii A, B, C (Sediul central al BSH)	Domeniul de aplicare al acțiunilor A, B, D (Entitate BSH)
Cerința privind temeiul juridic pentru prelucrarea în comun (articolul 6 din RGPD al UE și RGPD al Regatului Unit, articolul 6 din FADP elvețian),	[x] în ceea ce privește propriile sale prelucrări	[x] în ceea ce privește propriile prelucrări
Furnizarea de informații privind prelucrarea în comun a datelor cu caracter personal (Articolele 13 și 14 din RGPD al UE și RGPD al Regatului Unit, articolul 19 din FADP elvețian)	[x] privind propriile sale prelucrări	[x] privind propriile prelucrări
Punerea la dispoziție a esenței prezentului JCA (articolul 26 alineatul (2) din RGPD al UE și RGPD al Regatului Unit)	[x] în ceea ce privește propriile sale prelucrări	[x] în ceea ce privește propriile sale prelucrări
Drepturile persoanei vizate cu privire la datele cu caracter personal stocate de părți după prelucrarea în comun (articolele 15-20 din RGPD UE și RGPD Marea Britanie, articolele 25-29 din FADP elvețian)	[x] în calitate de coordonator central și pentru entitatea BSH respectivă	

Obligații în temeiul RGPD al UE, RGPD al Regatului Unit și FADP elvețian) <i>Partea responsabilă bifează în tabelul de mai jos responsabilitatea care îi revine</i>	Domeniul de aplicare al acțiunii A, B, C (Sediul central al BSH)	Domeniul de aplicare al acțiunilor A, B, D (Entitate BSH)
Dreptul de a se opune în măsura în care prelucrarea în comun se bazează pe un interes legitim (articolul 21 din RGPD al UE și RGPD al Regatului Unit)	[x] în calitate de coordonator central și pentru entitatea BSH respectivă	
Securitatea prelucrării în comun (Articolul 32: RGPD UE și RGPD Regatului Unit, articolul 8 FADP elvețian)	[x] pentru sistemele IT gestionate de noi	[x] pentru sistemele informatice gestionate de entitatea BSH
Încălcări ale securității datelor cu caracter personal privind prelucrarea în comun (articolele 33, 34 din RGPD UE și RGPD Marea Britanie, articolul 24 din FADP elvețian)	[x] pentru sistemele informatice gestionate de noi	[x] pentru sistemele IT gestionate de entitatea BSH

În plus, datele cu caracter personal pot fi transferate către aceste părți terțe în următoarele scopuri:

- Sistemul de raportare „Trust and Tell” este gestionat de un furnizor extern specializat, EQS Group GmbH, Karlstraße 47, D-80333 München, Germania, care acționează în calitate de procesator pentru BSH. Datele sunt stocate într-o bază de date gestionată de EQS Group GmbH într-un centru de date de înaltă securitate situat în Uniunea Europeană. Furnizorul de servicii nu are acces la date. Acest lucru este asigurat printr-o procedură certificată și prin măsuri tehnice și organizatorice cuprinzătoare.
- Ombudsmanul Dr. Karl Sidhu (SvS Attorneys at Law), Widenmayerstr. 36, 80538 München, Germania, acționează în calitate de avocat de încredere, fiind unul dintre canalele de contact pentru denunțatori.
- Consilier juridic extern pentru a sprijini investigația și remedierea.
- Transfer către Robert Bosch GmbH (societatea noastră-mamă), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, pentru prelucrarea tehnică a datelor pe sistemele IT operate în numele nostru și al entității BSH respective.
- Transfer către Robert Bosch GmbH (societatea noastră-mamă), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, pentru furnizarea de servicii de e-discovery (în special operarea de instrumente pentru revizuirea și analiza e-mailurilor într-un mod structurat) în numele nostru și al entității BSH respective.

V. Lista autorităților de protecție a datelor în conformitate cu RGPD

În conformitate cu Regulamentul general privind protecția datelor (GDPR), persoanele fizice au dreptul de a-și proteja datele cu caracter personal și pot solicita asistență din partea autorităților relevante de protecție a datelor (DPA). Lista de mai jos are scopul de a vă oferi o listă a DPA din regiunea GDPR. Este important de reținut că persoanele vizate au opțiunea de a contacta fie DPA din locul lor de reședință, fie DPA responsabilă pentru furnizorul site-ului web, în funcție de locația furnizorului. Vă rugăm să rețineți că

această listă nu este exhaustivă și că pot exista alte DPA în regiunea GDPR sau, dacă nu vă aflați în regiunea GDPR, în țara dumneavoastră.

- **Austria:** Österreichische Datenschutzbehörde, <http://www.dsb.gv.at/>
- **Belgia:** Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA), <https://www.autoriteprotectiondonnees.be> <https://www.gegevensbeschermingsautoriteit.be>
- **Bulgaria:** Comisia pentru protecția datelor cu caracter personal, <https://www.cdpd.bg/>
- **Croația:** Agenția croată pentru protecția datelor cu caracter personal, <http://www.azop.hr/>
- **Cipru:** Comisarul pentru protecția datelor cu caracter personal, <http://www.dataprotection.gov.cy/>
- **Republica Cehă:** Oficiul pentru Protecția Datelor cu Caracter Personal, <http://www.uouu.cz/>
- **Danemarca:** Datatilsynet, <http://www.datatilsynet.dk/>
- **Estonia:** Inspectoratul estonian pentru protecția datelor (Andmekaitse Inspeksioon), <http://www.aki.ee/>
- **Finlanda:** Biroul Ombudsmanului pentru Protecția Datelor, <http://www.tietosuoja.fi/en/>
- **Franța:** Comisia Națională pentru Informatică și Libertăți – CNIL, <http://www.cnil.fr/> <https://www.cnil.fr/en/contact-cnil>
- **Germania/Bavaria:** Autoritatea bavareză pentru protecția datelor (BayLDA), <http://www.baylda.de>
- **Grecia:** Autoritatea elenă pentru protecția datelor, <http://www.dpa.gr/>
- **Ungaria:** Autoritatea Națională Maghiară pentru Protecția Datelor și Libertatea Informației, <http://www.naih.hu/>
- **Islanda:** Persónuvernd, <https://www.personuvernd.is> , <https://www.dpa.is>
- **Irlanda:** Comisia pentru protecția datelor, <http://www.dataprotection.ie/>
- **Italia:** Garante per la protezione dei dati personali, <http://www.garanteprivacy.it/>
- **Letonia:** Inspectoratul de Stat pentru Protecția Datelor, <https://www.dvi.gov.lv/>
- **Liechtenstein:** Autoritatea pentru protecția datelor, Principatul Liechtenstein, <https://www.datenschutzstelle.li>
- **Lituania:** Inspectoratul de Stat pentru Protecția Datelor, <https://vdai.lrv.lt/>
- **Luxemburg:** Comisia Națională pentru Protecția Datelor, <http://www.cnpd.lu/>
- **Malta:** Oficiul Comisarului pentru Informații și Protecția Datelor, <http://www.idpc.org.mt/>
- **Țările de Jos:** Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>
- **Norvegia:** Datatilsynet, <https://www.datatilsynet.no>
- **Polonia:** Urząd Ochrony Danych Osobowych (Oficiul pentru Protecția Datelor cu Caracter Personal), <https://uodo.gov.pl/>
- **Portugalia:** Comissão Nacional de Proteção de Dados – CNPD, <http://www.cnpd.pt/>
- **România:** Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, <http://www.dataprotection.ro/>
- **Slovacia:** Oficiul pentru Protecția Datelor cu Caracter Personal al Republicii Slovace, <http://www.dataprotection.gov.sk/>
- **Slovenia:** Comisarul pentru informații al Republicii Slovenia, <https://www.ip-rs.si/>
- **Spania:** Agencia Española de Protección de Datos (AEPD), <https://www.aepd.es/>
- **Suedia:** Integritetsskyddsmyndigheten, <http://www.imy.se/>

Valabil din: iunie 2026