

Информация за защита на личните данни

Информация за защита на личните данни във връзка със сигнализиране и разследване на нарушения на правилата

I. Отговорник и цел на обработката на лични данни

Ние, BSH Hausgeräte GmbH, Carl-Wery-Strasse 34, 81739 Мюнхен, Германия („**BSH HQ**“ или „**Ние**“) и дружествата на BSH в Европейския съюз, Норвегия, Швейцария и Обединеното кралство (наричани по-нататък „**юридически лица на BSH**“), сме доставчиците на услугите, описани в настоящия документ, включително съответното обработване на лични данни.

За целите на управлението и разследването на твърдения за нарушения на съответствието („Управление на твърденията и разследвания за съответствие“), ние и съответното дружество на BSH действат като съвместни администратори (вж. чл. 26 от GDPR), тъй като съвместно определяме целите и средствата за обработване на Вашите лични данни.

Ние и съответното юридическо лице на BSH предлагаме различни канали за подаване на сигнали за потенциално несъответствие, както на централно, така и на местно ниво:

- Системата за подаване на сигнали „Trust and Tell“ (TnT)
- Адвокат на доверието (LoT)
- Местен служител по съответствието (LCO), намиращ се в централата на BSH или в съответното юридическо лице на BSH.

Настоящата информация за защита на данните Ви информира (наричан по-нататък „**Вие**“) за съответните обработки на лични данни в рамките на управлението на твърденията и разследванията за съответствие.

II. Нашите принципи за защита на данните

В контекста на предоставянето на описаните тук услуги и функционирането на уебсайтове и други точки на контакт, ние обработваме Вашите лични данни по различни начини. Ние Ви информираме за всяка обработка на лични данни, както и за съответното правно основание и принципите, съгласно които се извършва тази обработка.

Ние се ангажираме да защитаваме Вашите лични данни. Ето защо обработваме Вашите данни с голямо внимание и в строго съответствие с приложимите закони за защита на данните и индивидуалните разрешения, които може да сте ни дали. Взели сме организационни и технически мерки за сигурност, за да защитим всички наши уебсайтове, приложения и други (цифрови) точки на контакт срещу потенциалните рискове, свързани с обработката на лични данни. Компаниите от нашата група и партньорите, които ни подпомагат при предоставянето на услугите, също трябва да спазват тези правила и принципи.

Моля, използвайте контактната информация, предоставена в настоящата Информация за защита на данните, за да се свържете с нас по общи въпроси или с конкретни въпроси и/или запитвания относно защитата на данните. Съществуват различни закони, които регулират защитата на данните в зависимост от държавата, в която се намирате. Въз основа на принципите на Общия регламент за защита на данните на ЕС, т.е. РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 г. относно защитата на физическите лица при обработването на лични данни, относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО („GDPR“), ние определихме следните основни принципи като наши насоки за това как обработваме и защитаваме Вашите лични данни при предоставянето на нашите уебсайтове и услуги:

1. Законосъобразност

Ние използваме лични данни само ако това е законно, което в случая с управлението на твърдения и разследването на сигнали за нарушения на съответствието се основава на следните правни основания:

- **Чл. 6, ал. 1, буква в) от GDPR:** В Европа внедряването на система за управление на сигналите за нередности е законово задължение, произтичащо от Европейската директива за сигналите за нередности (Регламент (ЕС) 2019/1937) и произтичащите от нея национални закони за транспониране относно защитата на лицата, подаващи сигнали за нередности. Директивата позволява обработката на лични данни, която е необходима за обработката на сигнал в съответствие със законодателството.
- **Чл. 6, ал. 1, буква е) от GDPR:** Обработката на лични данни в системата BKMS® се основава на легитимните интереси на нашата компания да открива и предотвратява неправомерни действия и по този начин да избягва вреди за BSH, нейните служители и клиенти, **както и да преследва престъпления, да предявява граждански иски и да предотвратява нарушения на нормативните изисквания.**

За всяко обработване на лични данни, което описваме тук, ще посочим и правното основание за обработването в описанието на конкретните отношения между нас и съответното юридическо лице на BSH в раздел IV на настоящата информация за защита на данните.

2. Справедливост и прозрачност

В настоящата информация за защита на данните ще Ви информираме по справедлив и прозрачен начин за личните данни, които събираме, и защо ги събираме. Можете да получите достъп до информацията за защита на данните директно или чрез линк при регистрация и/или на всеки пункт за контакт, където взаимодействате с нас. Потребители на възраст под 16 години трябва да ни

предоставят лични данни само с съгласието на родител или законен настойник. Законодателството за защита на данните, приложимо във Вашата страна, може да предвижда различни възрастови ограничения в това отношение.

3. Ограничаване на целта и минимизиране на данните

Ние събираме и използваме само лични данни, от които наистина се нуждаем, и за целта, за която сте ни предоставили личните данни. Ако можем да постигнем целта с по-малко лични данни, ще използваме само минимално необходимите данни. Въпреки това, по всяко време сте свободни да предоставите допълнителни лични данни, ако това би подобрило вашето преживяване с предоставяните услуги.

4. Видове обработка, включително трети страни

В случаите, в които ние не обработваме вашите лични данни директно като администратор на данни (например хостинг на уебсайта, технически услуги и др.), ние сключваме договори с трети страни, които предоставят тези услуги от наше име като обработващи лични данни. Тези договори ги обвързват при обработката на вашите лични данни, за да се гарантира законността и сигурността на обработката. Това се нарича „връзка между администратор и обработващ лични данни“ и е дефинирано в чл. 28/29 от GDPR, където ние сме администраторът, а съответната трета страна е обработващият лични данни. В края на настоящата информация за защита на личните данни ще намерите списък с обработващите лични данни, с които работим.

Съвместното администраторство описва ситуацията, при която няколко страни, като ние сме една от тях, работят заедно, за да решат как ще се използват и управляват данните (съвместни администратори, вж. чл. 26 от GDPR). Съвместните администратори трябва да информират ясно кои лични данни се обработват от кого и какви задължения е поела всяка страна по отношение на приложимите правила за защита на данните. Тъй като съвместните администратори се споразумяват за своите роли и се уверяват, че субектите на данни (хората, за които се отнасят данните) са информирани за тези роли, ние ще Ви информираме за тези роли и Вашите индивидуални права за всяка от описаните тук ситуации на съвместно управление. Когато използваме услуга на трета страна или партньор, който обработва лични данни като съвместен администратор, ще Ви информираме за правата и ролите съответно в списъка с трети страни в раздел IV в края на настоящия документ.

5. Сигурност

Ние ще обработваме Вашите данни по начин, който гарантира подходяща сигурност на личните данни, включително защита срещу неразрешено или незаконно обработване и срещу случайна загуба, унищожаване или повреда, като използваме подходящи технически или организационни мерки. Когато използваме трети страни за обработване на лични данни, ние задължаваме тези трети страни да спазват подходящо ниво на технически или организационни мерки.

6. Права на потребителите

Имате следните права спрямо нас, които ние спазваме своевременно и по подходящ начин след получаване на съответното Ви искане, както е описано по-долу:

- **Вашето право да поискате достъп до Вашите лични данни съгласно чл. 15 от GDPR:** Ние ще Ви информираме дали съхраняваме лични данни за Вас и, ако е така, ще Ви предоставим достъп до и информация за тези данни.

- **Вашето право да поискате коригиране на вашите данни съгласно чл. 16 от GDPR:** Ние ще коригираме неточната информация или ще допълним непълните лични данни, при условие че тези данни са необходими за предвидената цел на обработката на вашите данни.
- **Вашето право да поискате изтриване на вашите данни съгласно чл. 17 от GDPR:** Ние ще изтрием личните данни, които съхраняваме за вас. Освен ако тези данни не подлежат на срокове за съхранение или права на съхранение, например защото трябва да съхраняваме вашите данни, за да изпълним нашите договорни задължения или както се изисква от закона.
- **Вашето право да поискате ограничаване на обработката на вашите данни съгласно чл. 18 от GDPR:** В случаите, описани в чл. 18, ал. 1 от GDPR, можете да ни поискате да блокираме вашите данни. Ще обработваме блокираните данни само в много ограничена степен и ако е необходимо, за да предоставим такива услуги или да изпълним такива задължения, чието изпълнение е необходимо след блокирането на вашите данни, поискано от вас.
- **Вашето право да оттеглите съгласието си съгласно чл. 7, ал. 3 от GDPR:** За онези обработки на данни, които изискват вашето съгласие, можете да оттеглите съгласието си по всяко време, за да предотвратите бъдеща обработка на вашите данни. Обработките на данни, основани на вашето съгласие преди оттеглянето му, остават валидни и законни.
- **Вашето право да възразите срещу обработката на вашите данни съгласно чл. 21 от GDPR:** Можете да възразите срещу бъдеща обработка на вашите данни, ако обработваме вашите данни въз основа на едно от законните основания, изложени в член 6, параграф 1, буква е) или ж) от GDPR. Ако възразите, ние ще преустановим обработката на вашите данни, освен ако нямаме убедителни законни основания за по-нататъшна обработка, които имат предимство пред вашите интереси и права, или за установяване, упражняване или защита на правни претенции. Обработката на вашите данни за целите на директния маркетинг никога не представлява убедително и законно основание за нас.
- **Вашето право на преносимост на данните съгласно чл. 20 от GDPR:** Когато обработката на данни се извършва по автоматизиран начин и въз основа на съгласие или договор, ние можем да Ви предоставим данните, които сте ни предоставили, в структуриран, широко използван и машинно четим формат.
- **Вашето право на обжалване пред регулаторен орган:** Можете да подадете жалба, свързана със защитата на данните, пред орган за защита на данните. За да направите това, свържете се със съответния орган за защита на данните, който отговаря за Вашето местожителство, или с органа за защита на данните, под чиято юрисдикция попадаме (посочен по-долу в Списъка на органите за защита на данните).

7. Принципи на изтриване

По принцип съхраняваме Вашите данни толкова дълго, колкото е необходимо за разследване на инцидента, свързан с несъответствие, за който се отнася Вашият сигнал. След приключване на разследването и изтичане на приложимия срок за съхранение ще изтрием Вашите лични данни, с изключение на данните, чието по-нататъшно съхранение е необходимо за установяване, упражняване или защита на правни претенции. Изтриването на такива данни се урежда от максималните законоустановени срокове за давност съгласно приложимите закони.

8. Длъжностно лице по защита на данните

Ако имате въпроси относно защитата на данните или искате да упражните правата си, нашият длъжностно лице по защита на данните (DPO) е на Ваше разположение. Можете лесно да се

свържете директно с нашия DPO, като изпратите писмо или имейл, използвайки предоставената по-долу информация за контакт:

- **Ако сте жител на държава-членка на ЕС/ЕИП, моля, свържете се с:**
BSH Hausgeräte GmbH, Длъжностно лице по защита на данните, Carl-Wery-Str. 34, 81739 Мюнхен, Германия, Data-Protection-DE@bshg.com
- **Ако сте жител на Обединеното кралство, моля, свържете се с:**
BSH Home Appliances Limited, Длъжностно лице по защита на данните, Grand Union House, Old Wolverton Road, Wolverton, Milton Keynes, MK12 5PT, Data-Protection-UK@bshg.com
- **Ако сте жител на Швейцария, моля, свържете се с:**
BSH Hausgeräte AG, представител на Home Connect GmbH, BSH Hausgeräte AG, Fahrweidstrasse 80, CH-8954 Geroldswil, Data-Protection-CH@bshg.com

9. Промени в настоящата информация за защита на данните

Настоящата информация за защита на данните отразява текущото състояние на обработката на данни на нашия уебсайт и други точки на взаимодействие. В случай на промени в обработката на данни, настоящата информация за защита на данните ще бъде съответно актуализирана. Винаги предоставяме най-новата версия на настоящата информация за защита на данните на нашия уебсайт, за да можете да бъдете информирани за обхвата на обработката на данни чрез този уебсайт.

III. Управление на твърденията и разследване на съответствието

1. Обработка на данни

a. Управление на сигнали и разследвания за съответствие

Страната, която получава сигналите („Получаваща страна“) , може да бъде или ние, или съответното юридическо лице на BSH и е отговорна за първоначалното приемане и документиране на сигналите, гарантиране на поверителността и изпращане на потвърждение за получаване до сигнализиращия, когато е възможно, както и за определяне на отговорния за темата и целесъобразността на провеждането на разследване, като същевременно се защитават правата на сигнализиращите и на обвинените. Страната, провеждаща разследванията („разследваща страна“), може да бъде или ние, или съответното юридическо лице на BSH и отговаря за задълбочени разследвания, включително разглеждане или прилагане на последващи мерки, подходящо документиране и окончателно докладване. Двете страни ще координират действията си, за да гарантират прозрачност и спазване на изискванията за защита на данните.

В рамките на съвместния контрол страните носят отговорност за обработката на лични данни, както следва:

- **Действие А (Приемаща страна):** Тази страна управлява първоначалното приемане на сигналите от лицата, подали сигнали, включително комуникацията с тях, извършването на първоначални проверки за правдоподобност и класифициране на предмета на сигнала, както и документирането на случая за предаване.
- **Действие Б (разследваща страна):** Тази страна провежда задълбочено разследване на вероятни нарушения, включително допълнителни проверки и документиране на всички данни и констатации от разследването.

b. Управление, окончателна документация и анализ

В рамките на съвместния контрол страните носят отговорност за обработката на лични данни за ръководство, приключване и анализ на получените сигнали и проведените разследвания за съответствие, както следва:

- **Действие В:** Ние ръководим цялостния процес, като предоставяме насоки за разследванията и изготвяме окончателни аналитични доклади за вътрешни и външни заинтересовани страни.
- **Действие Г:** Съответното юридическо лице на BSH отговаря за централизираното управление на жизнения цикъл на всички данни, включително подготовката, съхранението и изтриването на сигналите на лицата, подали сигнали, и данните от разследванията за съответствие в централните ИТ системи.

2. Конфиденциално обработване на сигнали и пренос на данни

Получените сигнали се приемат от тесен кръг изрично упълномощени и специално обучени служители и винаги се обработват конфиденциално. В рамките на обработката на сигнала може да се наложи той да бъде препратен към отговорните служители в централата на BSH или в съответното юридическо лице на BSH. Вашата информация ще бъде достъпна само за онези служители, които се нуждаят от нея, за да обработят сигнала Ви, и само до степента, позволена от законите за защита на лицата, подаващи сигнали. Всички лица, които получават достъп до Вашия сигнал, са длъжни да запазят конфиденциалност. Данните могат да бъдат предавани и на други отговорни органи (напр. публични власти), ако сме задължени по закон да го направим и до степента, позволена от законите за защита на лицата, подаващи сигнали.

3. Използване на системата за подаване на сигнали „Trust and Tell“

а. Предоставяне на уебсайта.

Услугата „Trust and Tell“ се предоставя чрез уебсайт, управляван от специализиран външен доставчик на услуги, EQS Group GmbH, от наше име. Комуникацията между вашия компютър и системата BKMS® за докладване на нарушения се осъществява чрез криптирана връзка (TLS).

б. За услугата

Системата за сигнализиране „Trust and Tell“ служи за сигурно и поверително получаване, обработка и управление на сигнали за нарушения на правилата за съответствие в рамките на или свързани с нас и/или съответното юридическо лице на BSH.

Използването на системата за докладване е на доброволен принцип. Възможно е да създадете пощенска кутия в системата за докладване, която е защитена с индивидуално избран псевдоним/потребителско име и парола. Това ви позволява да изпращате доклади до отговорния служител при нас или съответното юридическо лице на BSH или по име, или по анонимен и сигурен начин. Тази система съхранява данни само вътре в системата за докладване, което я прави особено сигурна. Тя не представлява форма на обикновена електронна поща.

Когато подавате сигнал или допълнение, можете едновременно да изпратите прикачени файлове на отговорния служител в нашата компания или в съответното юридическо лице на BSH. Ако желаете да подадете анонимен сигнал, моля, обърнете внимание на следните съвети за сигурност: Файловете могат да съдържат скрити лични данни, които биха могли да

компрометиранта вашата анонимност. Премахнете тези данни преди изпращане. Ако не можете да премахнете тези данни или не сте сигурни как да го направите, копирайте текста на прикачения файл в текста на сигнала си.

с. IP адрес, бисквитки и др.

Системата за сигнализиране не записва данни за IP адреси, времеви отметки или метаданни, свързани с използването ѝ от лицата, подаващи сигнали.

По време на използването на BKMS® Incident Reporting съвърът не е в състояние да идентифицира еднозначно клиента (компютъра на потребителя). За да може да идентифицира ясно клиента по време на сесията, приложението предава сесийна бисквитка на компютъра на потребителя. Тази сесийна бисквитка се използва само за текущата връзка и има само идентификационен номер за текущата сесия. Тази бисквитка се изтрива веднага след затваряне на браузъра. Този сесиен номер няма никаква връзка с информатора или с подаваните данни и е необходим само по технически причини.

IV. Списък на трети страни доставчици и съвместни администратори и тяхното използване

Страната, която получава сигналите, може да бъде или ние, или съответното юридическо лице на BSH, и е отговорна за първоначалното приемане и документиране на сигналите, гарантиране на поверителността и изпращане на потвърждение за получаване на сигнала до сигнализиращия, когато е възможно, както и за определяне на отговорния за темата и целесъобразността на провеждането на разследване, като се защитят правата на сигнализиращите и на обвинените. Страната, провеждаща разследванията, може да бъде или ние, или съответното юридическо лице на BSH и е отговорна за задълбочени разследвания, включително разглеждане или прилагане на последващи мерки, подходящо документиране и окончателно докладване. Двете страни ще координират действията си, за да гарантират прозрачност и спазване на изискванията за защита на данните.

В рамките на съвместното контрол, страните носят отговорност за обработката на лични данни за управление на твърденията и разследване на съответствието, както следва:

Задължения съгласно Общия регламент за защита на данните (GDPR) на ЕС, Общия регламент за защита на данните (GDPR) на Обединеното кралство и Швейцарския федерален закон за защита на данните (FADP) <i>Отговорната страна поставя кръстче в таблицата под съответната си отговорност</i>	Обхват на действие А, Б, В (Централен офис на BSH)	Обхват на действие А, Б, Г (юридическо лице на BSH)
Изискване за правно основание за съвместна обработка (член 6 от Общия регламент за защита на данните на ЕС и Общия регламент за защита на данните на Обединеното кралство, член 6 от Швейцарския федерален закон за защита на данните),	[x] по отношение на собствените си обработки	[x] по отношение на собствените си обработки

Задължения съгласно Общия регламент за защита на данните (GDPR) на ЕС, Общия регламент за защита на данните (GDPR) на Обединеното кралство и Швейцарския федерален закон за защита на данните (FADP) <i>Отговорната страна поставя кръстче в таблицата под съответната си отговорност</i>	Обхват на действие А, Б, В (Централен офис на BSH)	Обхват на действие А, Б, Г (юридическо лице на BSH)
Предоставяне на информация за съвместното обработване на лични данни (член 13, 14 от Общия регламент за защита на данните на ЕС и Общия регламент за защита на данните на Обединеното кралство, член 19 от Швейцарския федерален закон за защита на данните)	[x] относно собствените си обработки	[x] относно собствените си обработки
Предоставяне на същността на настоящото JCA (член 26, параграф 2 от Общия регламент за защита на данните на ЕС и Общия регламент за защита на данните на Обединеното кралство)	[x] относно собствените си обработки	[x] по отношение на собствените си обработки
Права на субекта на данни по отношение на личните данни, съхранявани от страните след съвместното обработване (членове 15–20 от Общия регламент за защита на данните на ЕС и Общия регламент за защита на данните на Обединеното кралство, членове 25–29 от Швейцарския федерален закон за защита на данните)	[x] като централен координатор и за съответното юридическо лице на BSH	
Право на възражение, доколкото съвместното обработване се основава на законен интерес (член 21 от Общия регламент за защита на данните на ЕС и Общия регламент за защита на данните на Обединеното кралство)	[x] като централен координатор и за съответното юридическо лице на BSH	
Сигурност на съвместното обработване (член 32: GDPR на ЕС и GDPR на Обединеното кралство, член 8 от швейцарския FADP)	[x] за ИТ системи, управлявани от нас	[x] за ИТ системи, управлявани от юридическо лице на BSH
Нарушения на защитата на лични данни, свързани със съвместното обработване (членове 33, 34 от Общия регламент за защита на данните на ЕС и Общия регламент за защита на данните на Обединеното кралство)	[x] за ИТ системи, управлявани от нас	[x] за ИТ системи, управлявани от

Задължения съгласно Общия регламент за защита на данните (GDPR) на ЕС, Общия регламент за защита на данните (GDPR) на Обединеното кралство и Швейцарския федерален закон за защита на данните (FADP) <i>Отговорната страна поставя кръстче в таблицата под съответната си отговорност</i>	Обхват на действие А, Б, В (Централен офис на BSH)	Обхват на действие А, Б, Г (юридическо лице на BSH)
на данните на Обединеното кралство, член 24 от Швейцарския федерален закон за защита на данните)		юридическо лице на BSH

Освен това личните данни могат да бъдат предавани на тези трети страни за следните цели:

- Системата за подаване на сигнали „Trust and Tell“ се управлява от специализиран външен доставчик на услуги – EQS Group GmbH, Karlstraße 47, D-80333 Мюнхен, Германия, който действа в качеството си на обработващ лични данни за BSH. Данните се съхраняват в база данни, управлявана от EQS Group GmbH, в център за данни с висока степен на сигурност в Европейския съюз. Доставчикът на услуги няма достъп до данните. Това се гарантира чрез сертифицирана процедура и всеобхватни технически и организационни мерки.
- Омбудсманът д-р Карл Сиду (SvS Attorneys at Law), Widenmayerstr. 36, 80538 Мюнхен, Германия, действащ като доверен адвокат, е един от каналите за приемане на сигнали от лица, подаващи сигнали за нередности.
- Външен правен съветник за подпомагане на разследването и отстраняването на нарушенията.
- Предаване на Robert Bosch GmbH (нашата компания майка), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, за техническа обработка на данни в ИТ системи, експлоатирани от наше име и от името на съответното юридическо лице на BSH.
- Предаване на Robert Bosch GmbH (нашата компания-майка), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, за предоставяне на услуги за електронно разкриване (по-специално използване на инструменти за преглед и анализ на имейли по структуриран начин) от наше име и от името на съответното юридическо лице на BSH.

V. Списък на органите за защита на данните по GDPR

В съответствие с Общия регламент за защита на данните (GDPR) физическите лица имат право да защитават своите лични данни и могат да потърсят помощ от съответните органи за защита на данните (DPA). Списъкът по-долу има за цел да Ви предостави списък на DPA в рамките на региона на GDPR. Важно е да се отбележи, че субектите на данни имат възможност да се свържат или с DPA по мястото си на пребиваване, или с DPA, отговарящ за доставчика на уебсайта, в зависимост от местоположението на доставчика. Моля, имайте предвид, че този списък не е изчерпателен и може да има допълнителни органи за защита на данните в региона на GDPR или, ако не се намират в региона на GDPR, във вашата страна.

- **Австрия:** Österreichische Datenschutzbehörde, <http://www.dsb.gv.at/>
- **Белгия:** Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA), <https://www.autoriteprotectiondonnees.be> <https://www.gegevensbeschermingsautoriteit.be>
- **България:** Комисия за защита на личните данни, <https://www.cpdp.bg/>
- **Хърватия:** Хърватска агенция за защита на личните данни, <http://www.azop.hr/>
- **Кипър:** Комисар по защита на личните данни, <http://www.dataprotection.gov.cy/>
- **Чешка република:** Служба за защита на личните данни, <http://www.uoou.cz/>

- **Дания:** Datatilsynet, <http://www.datatilsynet.dk/>
- **Естония:** Естонска инспекция за защита на данните (Andmekaitse Inspektsioon), <http://www.aki.ee/>
- **Финландия:** Служба на омбудсмана по защита на данните, <http://www.tietosuoja.fi/en/>
- **Франция:** Национална комисия по информатика и свободи – CNIL, <http://www.cnil.fr/>
<https://www.cnil.fr/en/contact-cnil>
- **Германия/Бавария:** Баварска служба за защита на личните данни (BayLDA), <http://www.baylda.de>
- **Гърция:** Гръцка служба за защита на личните данни, <http://www.dpa.gr/>
- **Унгария:** Унгарска национална служба за защита на данните и свобода на информацията, <http://www.naih.hu/>
- **Исландия:** Persónuvernd, <https://www.personuvernd.is> , <https://www.dpa.is>
- **Ирландия:** Комисия за защита на данните, <http://www.dataprotection.ie/>
- **Италия:** Garante per la protezione dei dati personali, <http://www.garanteprivacy.it/>
- **Латвия:** Държавна инспекция по защита на данните, <https://www.dvi.gov.lv/>
- **Лихтенщайн:** Орган за защита на личните данни, Княжество Лихтенщайн, <https://www.datenschutzstelle.li>
- **Литва:** Държавна инспекция за защита на данните, <https://vdai.lrv.lt/>
- **Люксембург:** Национална комисия за защита на данните, <http://www.cnpd.lu/>
- **Малта:** Служба на комисаря по защита на информацията и данните, <http://www.idpc.org.mt/>
- **Нидерландия:** Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>
- **Норвегия:** Datatilsynet, <https://www.datatilsynet.no>
- **Полша:** Urząd Ochrony Danych Osobowych (Служба за защита на личните данни), <https://uodo.gov.pl/>
- **Португалия:** Comissão Nacional de Proteção de Dados – CNPD, <http://www.cnpd.pt/>
- **Румъния:** Национален надзорен орган за обработката на лични данни, <http://www.dataprotection.ro/>
- **Словакия:** Служба за защита на личните данни на Словашката република, <http://www.dataprotection.gov.sk/>
- **Словения:** Комисар по информацията на Република Словения, <https://www.ip-rs.si/>
- **Испания:** Испанска агенция за защита на данните (AEPD), <https://www.aepd.es/>
- **Швеция:** Integritetsskyddsmyndigheten, <http://www.imy.se/>

В сила от: юни 2026 г.