

Information om dataskydd

Information om dataskydd vid rapportering och utredning av regelöverträdelser

I. Ansvarig för och syftet med behandlingen av personuppgifter

Vi, BSH Hausgeräte GmbH, Carl-Wery-Strasse 34, 81739 München, Tyskland ("**BSH HQ**" eller "**vi/oss**") och BSH-enheterna inom Europeiska unionen, Norge, Schweiz och Storbritannien (nedan kallade "**BSH-enhet**"), är leverantörer av de tjänster som beskrivs här, inklusive respektive behandling av personuppgifter.

I syfte att hantera och utreda anklagelser om regelöverträdelser agerar vi och respektive BSH-enhet som gemensamt personuppgiftsansvariga (se artikel 26 i GDPR), eftersom vi gemensamt bestämmer ändamålen och medlen för behandlingen av dina personuppgifter.

Vi och BSH-enheten erbjuder olika rapporteringskanaler för att lämna in rapporter om potentiella överträdelser, både på central och lokal nivå:

- Whistleblowing-systemet "Trust and Tell" (TnT)
- Lawyer of Trust (LoT)
- Local Compliance Officer (LCO), placerad vid BSH HQ eller respektive BSH-enhet.

Denna dataskyddsinformation informerar dig (nedan kallad "du") om relevant behandling av personuppgifter inom ramen för hantering och utredning av anklagelser om regelöverträdelser.

II. Våra dataskyddsprinciper

I samband med tillhandahållandet av de tjänster som beskrivs här och driften av webbplatser och andra kontaktpunkter behandlar vi dina personuppgifter på olika sätt. Vi informerar dig om varje behandling av personuppgifter samt om respektive rättslig grund och principer enligt vilka denna behandling sker.

Vi är fast beslutna att skydda dina personuppgifter. Därför behandlar vi dina uppgifter med stor omsorg och i strikt överensstämmelse med tillämpliga dataskyddslagar och de individuella tillstånd du eventuellt

har gett oss. Vi har vidtagit organisatoriska och tekniska säkerhetsåtgärder för att skydda alla våra webbplatser, appar och andra (digitala) kontaktpunkter mot de potentiella risker som finns vid behandling av personuppgifter. Våra koncernbolag och partners som stöder oss i tillhandahållandet av tjänsterna måste också följa dessa regler och principer.

Använd kontaktuppgifterna i denna dataskyddsinformation för att kontakta oss, antingen för allmänna frågor eller för specifika frågor och/eller förfrågningar om dataskydd. Det finns olika lagar som reglerar dataskydd beroende på vilket land du befinner dig i. Baserat på principerna i den europeiska allmänna dataskyddsförordningen, dvs. EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG ("GDPR"), har vi fastställt följande grundläggande principer som riktlinjer för hur vi behandlar och skyddar dina personuppgifter när vi tillhandahåller våra webbplatser och tjänster:

1. Laglighet

Vi använder endast personuppgifter om sådan användning är laglig, vilket i fallet med hantering och utredning av anklagelser om regelöverträdelser baseras på följande rättsliga grunder:

- **Art. 6.1 c) GDPR:** I Europa är införandet av ett system för hantering av visselblåsning en rättslig skyldighet som följer av det europeiska direktivet om visselblåsning (förordning (EU) 2019/1937) och nationella införlivandelagar om skydd för visselblåsare. Direktivet tillåter behandling av personuppgifter som är nödvändiga för hantering av en anmälan i enlighet med lagstiftningen.
- **Art. 6.1 f) GDPR:** Behandlingen av personuppgifter i BKMS®-systemet grundar sig på vårt företags berättigade intresse av att upptäcka och förebygga oegentligheter och därmed undvika skada för BSH, dess anställda och kunder, **samt att utreda brott, göra gällande civilrättsliga anspråk och förebygga regelöverträdelser.**

För all behandling av personuppgifter som vi beskriver här kommer vi även att ange den rättsliga grunden för behandlingen i beskrivningen av det specifika förhållandet mellan oss och respektive BSH-enhet som gemensamt personuppgiftsansvariga i avsnitt IV i denna information om dataskydd.

2. Rättvisa och öppenhet

Vi kommer att informera dig om de personuppgifter vi samlar in och varför vi samlar in dem på ett rättvist och öppet sätt i denna dataskyddsinformation. Du kan komma åt dataskyddsinformationen direkt eller via en länk när du registrerar dig och/eller vid alla kontaktpunkter där du interagerar med oss. Användare under 16 år bör endast överföra personuppgifter till oss med samtycke från en förälder eller vårdnadshavare. Den dataskyddslagstiftning som gäller i ditt land kan medföra andra åldersgränser i detta avseende.

3. Ändamålsbegränsning och dataminimering

Vi samlar endast in och använder personuppgifter som vi verkligen behöver och för det ändamål som du lämnade personuppgifterna till oss. Om vi kan uppnå syftet med mindre personuppgifter kommer vi endast att använda de uppgifter som krävs. Du är dock när som helst fri att lämna ytterligare personuppgifter, om detta skulle förbättra din upplevelse av de tjänster som tillhandahålls.

4. Typer av behandling, inklusive tredje part

I de fall där vi inte behandlar dina personuppgifter direkt som personuppgiftsansvarig (t.ex. webbhotell,

tekniska tjänster etc.) ingår vi avtal med tredje parter som tillhandahåller dessa tjänster för vår räkning som personuppgiftsbiträden. Dessa avtal förpliktar dem att behandla dina personuppgifter på ett sätt som säkerställer behandlingens laglighet och säkerhet. Detta kallas för ett förhållande mellan en personuppgiftsansvarig och ett personuppgiftsbiträde och definieras i artiklarna 28–29 i GDPR, där vi är den personuppgiftsansvarige och respektive tredje part är personuppgiftsbiträdet. Du hittar en lista över de personuppgiftsbiträden vi anlitat i slutet av denna dataskyddsinformation.

Gemensamt personuppgiftsansvar beskriver situationen när flera parter, där vi är en av dem, samarbetar för att fastställa hur uppgifterna ska användas och hanteras (gemensamt personuppgiftsansvariga, se artikel 26 i GDPR). Gemensamt personuppgiftsansvariga måste tydligt informera om vem som behandlar vilka personuppgifter och vilka skyldigheter varje part har åtagit sig med avseende på tillämpliga dataskyddsregler. I takt med att gemensamt personuppgiftsansvariga kommer överens om sina respektive roller och säkerställer att de registrerade (personerna som uppgifterna gäller) informeras om dessa roller, kommer vi att informera dig om dessa roller och dina individuella rättigheter för var och en av de situationer med gemensamt ansvar som beskrivs här. När vi använder en tredjepartstjänst eller partner som behandlar personuppgifter som gemensamt personuppgiftsansvarig kommer vi att informera dig om rättigheter och roller i enlighet med detta i förteckningen över tredjepartsleverantörer i avsnitt IV längst bak i detta dokument.

5. Säkerhet

Vi kommer att behandla dina uppgifter på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inklusive skydd mot obehörig eller olaglig behandling och mot oavsiktlig förlust, förstörelse eller skada, med hjälp av lämpliga tekniska eller organisatoriska åtgärder. När vi använder tredje part för att behandla personuppgifter ålägger vi dessa tredje parter att följa en lämplig nivå av tekniska eller organisatoriska åtgärder.

6. Användarrättigheter

Du har följande rättigheter gentemot oss, vilka vi tillmötesgår på ett skyndsamt och adekvat sätt så snart vi mottagit din begäran enligt nedan:

- **Din rätt att begära tillgång till dina personuppgifter enligt artikel 15 i GDPR:** Vi kommer att informera dig om vi lagrar personuppgifter om dig och, om så är fallet, ge dig tillgång till och information om sådana uppgifter.
- **Din rätt att begära rättelse av dina personuppgifter enligt artikel 16 i GDPR:** Vi kommer att korrigera felaktiga uppgifter eller komplettera ofullständiga personuppgifter, förutsatt att dessa uppgifter är nödvändiga för det avsedda ändamålet med behandlingen av dina uppgifter.
- **Din rätt att begära radering av dina personuppgifter enligt artikel 17 i GDPR:** Vi kommer att radera de personuppgifter vi har om dig, om inte sådana uppgifter omfattas av lagringskrav eller -rättigheter, till exempel för att vi behöver behålla dina uppgifter för att uppfylla våra avtalsenliga skyldigheter eller på grund av rättsliga krav.
- **Din rätt att begära begränsning av behandlingen av dina personuppgifter enligt artikel 18 i GDPR:** I de fall som anges i artikel 18.1 i GDPR kan du begära att vi begränsar behandlingen av dina uppgifter. Vi kommer att fortsätta behandla begränsade uppgifter endast i mycket begränsad utsträckning och endast om det är nödvändigt för att fullgöra tjänster eller skyldigheter som fortfarande krävs efter den begränsning av dina uppgifter som du har begärt.
- **Din rätt att återkalla samtycke enligt artikel 7.3 i GDPR:** För personuppgiftsbehandling som kräver ditt samtycke kan du när som helst återkalla ditt samtycke för att förhindra framtida behandling av dina uppgifter. Personuppgiftsbehandling som baseras på ditt samtycke före återkallandet förblir giltig och laglig.

- **Din rätt att invända mot behandlingen av dina personuppgifter enligt artikel 21 i GDPR:** Du kan invända mot framtida behandling av dina uppgifter om vi behandlar dina uppgifter baserat på av en av de rättsliga grunderna i artikel 6.1 e eller f i GDPR. Om du invänder kommer vi att upphöra med behandlingen av dina uppgifter, såvida vi inte har tvingande berättigade skäl för fortsatt behandling som väger tyngre än dina intressen och rättigheter eller för att fastställa, utöva eller försvara rättsliga anspråk. Behandlingen av dina uppgifter för direktmarknadsföring utgör aldrig tvingande och berättigade skäl för oss.
- **Din rätt till dataportabilitet enligt artikel 20 i GDPR:** Om databehandlingen sker automatiserat och baseras på samtycke eller avtal kan vi tillhandahålla dig de uppgifter du har lämnat till oss i ett strukturerat, allmänt använt och maskinläsbart format.
- **Din rätt att överklaga till en tillsynsmyndighet:** Du kan lämna in ett klagomål avseende dataskydd till en dataskyddsmyndighet. För att göra detta, kontakta den relevanta dataskyddsmyndigheten som är ansvarig för din bostadsort eller den dataskyddsmyndighet under vars jurisdiktion vi faller (se listan över dataskyddsmyndigheter nedan).

7. Principer för radering

I princip lagrar vi dina uppgifter så länge som det är nödvändigt för att utreda den regelöverträdelse som din anmälan avser. När utredningen är avslutad och den tillämpliga lagringstiden har löpt ut kommer vi att radera dina personuppgifter, med undantag för uppgifter vars fortsatta lagring krävs för att fastställa, utöva eller försvara rättsliga anspråk. Raderingen av sådana uppgifter regleras av de maximala preskriptionstiderna enligt tillämplig lagstiftning.

8. Dataskyddsombud

Om du har några frågor om dataskydd eller om du vill utöva dina rättigheter finns vårt dataskyddsombud (DPO) här för att hjälpa dig. Du kan enkelt kontakta vårt dataskyddsombud direkt genom att skicka ett brev eller ett e-postmeddelande med hjälp av kontaktuppgifterna nedan:

- **Om du är bosatt i en EU-/EES-medlemsstat, vänligen kontakta:**
BSH Hausgeräte GmbH, Data Protection Officer, Carl-Wery-Str. 34, 81739 München, Tyskland, Data-Protection-DE@bshg.com
- **Om du är bosatt i Storbritannien, vänligen kontakta:**
BSH Home Appliances Limited, Data Protection Officer, Grand Union House, Old Wolverton Road, Wolverton, Milton Keynes, MK12 5PT, Data-Protection-UK@bshg.com
- **Om du är bosatt i Schweiz, vänligen kontakta:**
BSH Hausgeräte AG, representant för Home Connect GmbH, BSH Hausgeräte AG, Fahrweidstrasse 80, CH-8954 Geroldswil, Data-Protection-CH@bshg.com

9. Ändringar i denna dataskyddsinformation

Denna dataskyddsinformation återspeglar det aktuella läget för personuppgiftsbehandlingen på vår webbplats och andra kontaktpunkter. Vid ändringar i personuppgiftsbehandlingen kommer denna dataskyddsinformation att uppdateras i enlighet därmed. Vi gör alltid den senaste versionen av denna dataskyddsinformation tillgänglig på vår webbplats så att du där kan hålla dig informerad om omfattningen av den personuppgiftsbehandling som utförs.

III. Hantering av anmälningar och utredning av regelöverträdelser

1. Personuppgiftsbehandling

a. Hantering av anmälningar och utredningar av regelöverträdelser

Den part som tar emot anmälningar ("mottagande part") kan vara antingen vi eller respektive BSH-enhet; den ansvarar för det initiala mottagandet och dokumentationen av anmälningar, säkerställer sekretess och att en mottagningsbekaftelse skickas till visselblåsaren där så är möjligt, identifierar den person som är ansvarig för det aktuella ärendet och bedömer lämpligheten av en utredning samtidigt som visselblåsarnas och de anklagades rättigheter skyddas. Den part som genomför utredningar ("utredande part") kan vara antingen vi eller respektive BSH-enhet; den ansvarar för att genomföra utredningar, inklusive att vidta eller implementera uppföljningsåtgärder, korrekt dokumentation och slutrapportering. Båda parter samordnar sina åtgärder för att säkerställa transparens och efterlevnad av dataskyddskrav.

Inom ramen för gemensamt personuppgiftsansvar ansvarar parterna för behandlingen av personuppgifter enligt följande:

- **Åtgärd A (mottagande part):** Denna part hanterar det initiala mottagandet av visselblåsarrapporter, inklusive kommunikation med visselblåsaren, genomförande av preliminära rimlighetskontroller och klassificering av ärendet samt dokumentation av ärendet för överlämning.
- **Åtgärd B (utredande part):** Denna part genomför en fördjupad utredning av ärendet, inklusive ytterligare granskningar och dokumentation av alla utredningsuppgifter och resultat.

b. Styrning, slutdokumentation och analys

Inom ramen för gemensamt personuppgiftsansvar är parterna ansvariga för behandlingen av personuppgifter för styrning, slutförande och analys av mottagna anmälningar och genomförda utredningar enligt följande:

- **Åtgärd C:** Vi styr den övergripande processen genom att ge vägledning om utredningar och skapa slutliga analysrapporter för interna och externa intressenter.
- **Åtgärd D:** Respektive BSH-enhet ansvarar för den centrala livscykelhanteringen av alla uppgifter, inklusive att förbereda, lagra och radera visselblåsarrapporter och uppgifter från utredningar i centrala IT-system.

2. Konfidentiell hantering av anmälningar och dataöverföring

Inkommande anmälningar tas emot av en liten krets av uttryckligen behöriga och särskilt utbildade medarbetare och hanteras alltid konfidentiellt. Som en del av behandlingen av en anmälan kan det vara nödvändigt att vidarebefordra den till ansvariga medarbetare vid BSH HQ eller respektive BSH-enhet. Dina uppgifter kommer endast att göras tillgängliga för de medarbetare som behöver dem för att behandla din anmälan och endast i den utsträckning som tillåts enligt lagar om skydd för visselblåsare. Alla personer som får tillgång till din anmälan är skyldiga att iaktta sekretess. Uppgifter kan också överföras till andra ansvariga organ (t.ex. myndigheter) om vi är skyldiga att göra det enligt lag och i den utsträckning som tillåts enligt lagar om skydd för visselblåsare.

3. Användning av visselblåsarsystemet "Trust and Tell"

a. Tillhandahållande av webbplatsen.

Tjänsten "Trust and Tell" tillhandahålls via en webbplats som drivs för vår räkning av en specialiserad extern tjänsteleverantör, EQS Group GmbH. Kommunikationen mellan din dator och BKMS®-systemet för rapportering av överträdelser sker via en krypterad anslutning (TLS).

b. Om tjänsten

Rapporteringsystemet "Trust and Tell" är utformat för att på ett säkert och konfidentiellt sätt ta emot, behandla och hantera rapporter om regelöverträdelser inom eller relaterade till oss och/eller respektive BSH-enhet.

Användningen av rapporteringssystemet är frivilligt. Det är möjligt att skapa en brevlåda inom rapporteringssystemet som är skyddad med ett individuellt valt pseudonym/användarnamn och lösenord. Detta gör det möjligt för dig att skicka rapporter till den ansvariga medarbetaren hos oss eller respektive BSH-enhet, antingen med namn eller på ett anonymt och säkert sätt. Systemet lagrar endast data inom rapporteringssystemet, vilket säkerställer en hög säkerhetsnivå. Det är inte en form av vanlig e-postkommunikation.

När du skickar in en anmälan eller en uppdatering kan du samtidigt skicka bilagor till den ansvariga medarbetaren hos oss eller respektive BSH-enhet. Om du vill skicka in en anonym anmälan, vänligen beakta följande säkerhetsråd: Filer kan innehålla dold personuppgifter som kan äventyra din anonymitet. Ta bort dessa uppgifter innan du skickar. Om du inte kan ta bort dessa uppgifter eller är osäker på hur du ska göra, kopiera texten i din bilaga till din anmälningstext.

c. IP-adress, cookies etc.

Rapporteringsystemet loggar inte IP-adressdata, tidsstämplat eller metadata som är kopplade till visuellblåsarens användning.

Vid användning av BKMS® Incident Reporting kan servern inte identifiera klienten (användarens dator) på ett unikt sätt. För att kunna identifiera klienten under en session överför applikationen en sessionscookie till användarens dator. Denna sessionscookie används endast för den aktuella anslutningen och har endast ett identifikationsnummer för den pågående sessionen. Denna cookie raderas när webbläsaren stängs. Detta sessionsnummer är inte relaterat till visuellblåsaren eller de inlämnade uppgifterna och är endast nödvändigt av tekniska skäl.

IV. Förteckning över tredjepartsleverantörer och gemensamt personuppgiftsansvariga samt deras roller

Den part som tar emot anmälningar kan vara antingen vi eller respektive BSH-enhet. Den ansvarar för det initiala mottagandet och dokumentationen av anmälningar, säkerställer sekretess och att en mottagningsbekaftelse skickas till visuellblåsaren där så är möjligt, samt identifierar den person som är ansvarig för det aktuella ärendet och lämpligheten i att inleda en utredning samtidigt som visuellblåsarnas och de anklagades rättigheter skyddas. Den part som genomför utredningar kan vara antingen vi eller respektive BSH-enhet. Den ansvarar för fördjupade utredningar, inklusive hantering eller genomförande av uppföljningsåtgärder, korrekt dokumentation och slutlig rapportering. Båda parter samordnar sina åtgärder för att säkerställa transparens och efterlevnad av dataskyddskrav.

Inom ramen för gemensamt personuppgiftsansvar är parterna ansvariga för behandlingen av personuppgifter vid hantering av anklagelser och utredning av regelöverträdelser enligt följande:

Skyldigheter enligt EU:s GDPR, Storbritanniens GDPR och Schweiz FADP <i>Den ansvariga parten sätter ett kryss i tabellen under sitt respektive ansvarsområde</i>	Åtgärdsområde A, B, C (BSH HQ)	Åtgärdsområde A, B, D (BSH-enhet)
Krav på rättslig grund för gemensam behandling (artikel 6 i EU:s GDPR och Storbritanniens GDPR, artikel 6 i Schweiz FADP),	[x] avseende den egna behandlingen	[x] avseende den egna behandlingen
Tillhandahållande av information om gemensam behandling av personuppgifter (Artikel 13, 14 i EU:s GDPR och Storbritanniens GDPR, artikel 19 i Schweiz FADP)	[x] angående sin egen behandling	[x] avseende den egna behandlingen
Att göra innehållet i detta JCA tillgängligt (artikel 26.2 i EU:s GDPR och Storbritanniens GDPR)	[x] avseende sin egen behandling	[x] avseende sin egen behandling
Den registrerades rättigheter avseende de personuppgifter som lagras av parterna efter den gemensamma behandlingen (artiklarna 15–20 i EU:s GDPR och Storbritanniens GDPR, artiklarna 25–29 i Schweiz FADP)	[x] som central samordnare även för respektive BSH-enhet	
Rätt att göra invändningar i den mån den gemensamma behandlingen grundar sig på berättigat intresse (artikel 21 i EU:s GDPR och Storbritanniens GDPR)	[x] som central samordnare även för respektive BSH-enhet	
Säkerhet vid den gemensamma behandlingen (Artikel 32: EU:s GDPR och Storbritanniens GDPR, artikel 8 i schweiziska FADP)	[x] för IT-system som förvaltas av oss	[x] för IT-system som förvaltas av BSH-enheten
Personuppgiftsincidenter avseende gemensam behandling (artiklarna 33 och 34 i EU:s och Storbritanniens GDPR, artikel 24 i schweiziska FADP)	[x] för IT-system som förvaltas av oss	[x] för IT-system som förvaltas av BSH-enheten

Dessutom kan personuppgifter överföras till dessa tredje parter för följande ändamål:

- Rapporteringsystemet "Trust and Tell" drivs av en specialiserad extern tjänsteleverantör, EQS Group GmbH, Karlstraße 47, D-80333 München, Tyskland, som agerar som personuppgiftsbiträde för BSH. Uppgifterna lagras i en databas som drivs av EQS Group GmbH i ett högsäkerhetsdatacenter inom Europeiska unionen. Tjänsteleverantören har ingen tillgång till uppgifterna. Detta säkerställs genom ett certifierat förfarande samt omfattande tekniska och organisatoriska åtgärder.

- Ombudsmannen Dr. Karl Sidhu (SvS Attorneys at Law), Widenmayerstr. 36, 80538 München, Tyskland, fungerar som extern konfidentiell advokat och är en av kontaktpunkterna för visselblåsare.
- Extern juridisk rådgivare för att stödja utredningen och vidtagna åtgärder.
- Överföring till Robert Bosch GmbH (vårt moderbolag), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, för teknisk behandling av data i IT-system som drivs på uppdrag av oss och respektive BSH-enhet.
- Överföring till Robert Bosch GmbH (vårt moderbolag), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, för tillhandahållande av e-discovery-tjänster (i synnerhet drift av verktyg för att granska och analysera e-postmeddelanden på ett strukturerat sätt) på uppdrag av oss och respektive BSH-enhet.

V. Förteckning över dataskyddsmyndigheter enligt GDPR

I enlighet med den allmänna dataskyddsförordningen (GDPR) har enskilda personer rätt till skydd av sina personuppgifter och kan kontakta relevanta dataskyddsmyndigheter. Förteckningen nedan ger dig en förteckning över dataskyddsmyndigheter inom GDPR-området. Det är viktigt att notera att registrerade har möjlighet att kontakta antingen dataskyddsmyndigheten på sin hemort eller den dataskyddsmyndighet som ansvarar för webbplatsens leverantör, beroende på leverantörens plats. Observera att denna förteckning inte är uttömmande och att det kan finnas ytterligare dataskyddsmyndigheter inom GDPR-området eller, om du inte befinner dig inom GDPR-området, i ditt land.

- **Österrike:** Österreichische Datenschutzbehörde, <http://www.dsb.gv.at/>
- **Belgien:** Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA), <https://www.autoriteprotectiondonnees.be> <https://www.gegevensbeschermingsautoriteit.be>
- **Bulgarien:** Kommissionen för skydd av personuppgifter, <https://www.cdpd.bg/>
- **Kroatien:** Kroatiska myndigheten för skydd av personuppgifter, <http://www.azop.hr/>
- **Cypern:** Commissioner for Personal Data Protection, <http://www.dataprotection.gov.cy/>
- **Tjeckien:** Kontoret för skydd av personuppgifter, <http://www.uoou.cz/>
- **Danmark:** Datatilsynet, <http://www.datatilsynet.dk/>
- **Estland:** Estniska dataskyddsinspektionen (Andmekaitse Inspektsioon), <http://www.aki.ee/>
- **Finland:** Dataombudsmannens byrå, <http://www.tietosuoja.fi/en/>
- **Frankrike:** Commission Nationale de l'Informatique et des Libertés – CNIL, <http://www.cnil.fr/> <https://www.cnil.fr/en/contact-cnil>
- **Tyskland/Bayern:** Bayerska dataskyddsmyndigheten (BayLDA), <http://www.baylda.de>
- **Grekland:** Grekiska dataskyddsmyndigheten, <http://www.dpa.gr/>
- **Ungern:** Ungerns nationella myndighet för dataskydd och informationsfrihet, <http://www.naih.hu/>
- **Island:** Persónuvernd, <https://www.personuvernd.is>, <https://www.dpa.is>
- **Irland:** Data Protection Commission, <http://www.dataprotection.ie/>
- **Italien:** Garante per la protezione dei dati personali, <http://www.garanteprivacy.it/>
- **Lettland:** Datatilsynet, <https://www.dvi.gov.lv/>
- **Liechtenstein:** Dataskyddsmyndigheten, Furstendömet Liechtenstein, <https://www.datenschutzstelle.li>
- **Litauen:** Statliga dataskyddsinspektionen, <https://vdai.lrv.lt/>
- **Luxemburg:** Commission Nationale pour la Protection des Données, <http://www.cnpd.lu/>
- **Malta:** Office of the Information and Data Protection Commissioner, <http://www.idpc.org.mt/>
- **Nederländerna:** Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>
- **Norge:** Datatilsynet, <https://www.datatilsynet.no>
- **Polen:** Urząd Ochrony Danych Osobowych (Personal Data Protection Office), <https://uodo.gov.pl/>
- **Portugal:** Comissão Nacional de Proteção de Dados – CNPD, <http://www.cnpd.pt/>

- **Rumänien:** Den nationella tillsynsmyndigheten för behandling av personuppgifter, <http://www.dataprotection.ro/>
- **Slovakien:** Office for Personal Data Protection of the Slovak Republic, <http://www.dataprotection.gov.sk/>
- **Slovenien:** Informationskommissionären för Republiken Slovenien, <https://www.ip-rs.si/>
- **Spanien:** Agencia Española de Protección de Datos (AEPD), <https://www.aepd.es/>
- **Sverige:** Integritetsskyddsmyndigheten, <http://www.imy.se/>

Gäller från: juni 2026