

Informatie over gegevensbescherming

Informatie over gegevensbescherming met betrekking tot het melden en onderzoeken van schendingen van de naleving

I. De verantwoordelijke voor en het doel van de verwerking van persoonsgegevens

Wij, BSH Hausgeräte GmbH, Carl-Wery-Strasse 34, 81739 München, Duitsland ("**BSH HQ**" of "**Wij/Ons**") en de BSH-entiteiten binnen de Europese Unie, Noorwegen, Zwitserland en het Verenigd Koninkrijk (hierna "**BSH-entiteit**"), zijn de aanbieders van de hierin beschreven diensten, inclusief de bijbehorende verwerking van persoonsgegevens.

Met het oog op het beheer en het onderzoek van beschuldigingen van nalevingsschendingen ("Allegation Management & Compliance Investigations") treden wij en de betreffende BSH-entiteit op als gezamenlijke verwerkingsverantwoordelijken (zie art. 26 AVG), aangezien wij gezamenlijk de doeleinden en middelen voor de verwerking van uw persoonsgegevens bepalen.

Wij en de BSH-entiteit bieden verschillende meldingskanalen aan om meldingen over mogelijke niet-naleving in te dienen, zowel op centraal als op lokaal niveau:

- Het klokkenluiderssysteem "Trust and Tell" (TnT)
- Lawyer of Trust (LoT)
- Lokale compliance officer (LCO), gevestigd op het hoofdkantoor van BSH of bij de betreffende BSH-entiteit.

Deze informatie over gegevensbescherming informeert u (hierna "**u**") over de relevante verwerkingen van persoonsgegevens in het kader van Allegation Management & Compliance Investigations.

II. Onze gegevensbeschermingsprincipes

In het kader van de levering van de hierin beschreven diensten en de exploitatie van websites en andere contactpunten verwerken wij uw persoonsgegevens op verschillende manieren. Wij informeren u over elke

verwerking van persoonsgegevens, evenals over de respectieve rechtsgrondslag en principes op basis waarvan deze verwerking plaatsvindt.

Wij zetten ons in voor de bescherming van uw persoonsgegevens. Daarom verwerken wij uw gegevens met de grootste zorg en in strikte naleving van de toepasselijke wetgeving inzake gegevensbescherming en de individuele toestemmingen die u ons mogelijk gegeven heeft. Wij hebben organisatorische en technische beveiligingsmaatregelen genomen om al onze websites, apps en andere (digitale) contactpunten te beschermen tegen de potentiële risico's die gepaard gaan met de verwerking van persoonsgegevens. Onze groepsvennootschappen en partners die ons ondersteunen bij het verlenen van de diensten moeten zich eveneens aan deze regels en beginselen houden.

Gebruik de contactgegevens in deze informatie over gegevensbescherming om contact met ons op te nemen, hetzij in het algemeen, hetzij met specifieke vragen en/of verzoeken over gegevensbescherming. Er zijn verschillende wetten die de gegevensbescherming regelen, afhankelijk van het land waarin u zich bevindt. Op basis van de beginselen van de Europese Algemene Verordening Gegevensbescherming, d.w.z. VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG ("AVG"), hebben wij de volgende basisprincipes vastgesteld als onze richtlijnen voor de manier waarop wij uw persoonsgegevens verwerken en beschermen bij het aanbieden van onze websites en diensten:

1. Rechtmatigheid

Wij gebruiken persoonsgegevens alleen indien dit rechtmatig is, wat in het geval van het behandelen van beschuldigingen en het onderzoeken van gemelde nalevingsschendingen, gebaseerd is op de volgende rechtsgrondslagen:

- **Art. 6, lid 1, onder c) AVG:** In Europa is de implementatie van een klokkenluiderssysteem een wettelijke verplichting die voortvloeit uit de Europese klokkenluidersrichtlijn (Richtlijn (EU) 2019/1937) en daaruit afgeleide nationale omzettingswetgeving inzake de bescherming van klokkenluiders. De richtlijn staat de verwerking van persoonsgegevens toe die noodzakelijk is voor de afhandeling van een melding in overeenstemming met de wetgeving.
- **Art. 6, lid 1, onder f) AVG:** De verwerking van persoonsgegevens in het BKMS®-systeem is gebaseerd op de gerechtvaardigde belangen van ons bedrijf om wangedrag op te sporen en te voorkomen en zo schade aan BSH, haar medewerkers en klanten te vermijden, **alsook om strafbare feiten te vervolgen, civiele vorderingen in te stellen en overtredingen van regelgeving te voorkomen.**

Voor alle verwerkingen van persoonsgegevens die wij hierin beschrijven, zullen wij ook de rechtsgrond voor de verwerking vermelden in de beschrijving van de specifieke gezamenlijke verwerkingsverantwoordelijke-relatie tussen ons en de betreffende BSH-entiteit in paragraaf IV van deze informatie over gegevensbescherming.

2. Eerlijkheid en transparantie

In deze informatie over gegevensbescherming informeren wij u op een eerlijke en transparante manier over de persoonsgegevens die wij verzamelen en waarom wij deze verzamelen. U kunt de informatie over gegevensbescherming rechtstreeks of via een link raadplegen wanneer u zich registreert en/of op elk contactpunt waar u met ons in contact komt. Gebruikers jonger dan 16 jaar mogen alleen met toestemming van hun ouder of wettelijke voogd persoonsgegevens aan ons doorgeven. De

gegevensbeschermingswetgeving die in uw land van toepassing is, kan in dit opzicht tot andere leeftijdsgrenzen leiden.

3. Doelbinding en gegevensminimalisatie

Wij verzamelen en gebruiken alleen persoonsgegevens die wij echt nodig hebben en voor het doel waarvoor u de persoonsgegevens aan ons heeft verstrekt. Als wij het doel met minder persoonsgegevens kunnen bereiken, zullen wij alleen de minimaal vereiste gegevens gebruiken. Niettemin staat het u te allen tijde vrij om aanvullende persoonsgegevens te verstrekken, indien dit uw ervaring met de aangeboden diensten zou verbeteren.

4. Soorten verwerking, inclusief derden

In gevallen waarin wij uw persoonsgegevens niet rechtstreeks verwerken als verwerkingsverantwoordelijke (bijv. websitehosting, technische diensten enz.), sluiten wij contracten met derden die deze diensten namens ons leveren als verwerkers. Deze contracten binden hen bij de verwerking van uw persoonsgegevens om de rechtmatigheid en veiligheid van de verwerking te waarborgen. Dit wordt een relatie tussen verwerkingsverantwoordelijke en verwerker genoemd en is gedefinieerd in de artikelen 28 en 29 van de AVG, waarbij wij de verwerkingsverantwoordelijke zijn en de betreffende derde partij de verwerker. Aan het einde van deze privacyverklaring vindt u een lijst met de verwerkers die wij inschakelen.

Gezamenlijke verwerkingsverantwoordelijkheid beschrijft de situatie waarin meerdere partijen, waarvan wij er één zijn, samenwerken om te beslissen hoe gegevens worden gebruikt en beheerd (gezamenlijke verwerkingsverantwoordelijken, zie art. 26 AVG). Gezamenlijke verwerkingsverantwoordelijken moeten duidelijk informeren over wie welke persoonsgegevens verwerkt en welke verplichtingen elke partij heeft aangenomen met betrekking tot de toepasselijke gegevensbeschermingsregels. Aangezien gezamenlijke verwerkingsverantwoordelijken overeenstemming bereiken over hun rollen en ervoor zorgen dat de betrokkenen (de personen op wie de gegevens betrekking hebben) over deze rollen worden geïnformeerd, zullen wij u informeren over deze rollen en uw individuele rechten voor elk van de hierin beschreven situaties van gezamenlijk verwerkingsverantwoordelijkheid. Wanneer wij gebruikmaken van een externe dienst of partner die persoonsgegevens verwerkt als medeverantwoordelijke, zullen wij u informeren over de rechten en rollen in de lijst van externe dienstverleners in paragraaf IV helemaal aan het einde van dit document.

5. Beveiliging

Wij zullen uw gegevens verwerken op een manier die een passende beveiliging van de persoonsgegevens waarborgt, met inbegrip van bescherming tegen ongeoorloofde of onwettige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging, door middel van passende technische of organisatorische maatregelen. Wanneer wij derden inschakelen om persoonsgegevens te verwerken, verplichten wij deze derden tot het naleven van een passend niveau van technische of organisatorische maatregelen.

6. Rechten van de gebruiker

U heeft de volgende rechten ten opzichte van ons, waaraan wij tijdig en op passende wijze voldoen zodra wij uw verzoek hebben ontvangen, zoals hieronder uiteengezet:

- **Uw recht om inzage te vragen in uw persoonsgegevens overeenkomstig artikel 15 AVG:** Wij zullen u meedelen of wij persoonsgegevens over u bewaren en, indien dit het geval is, u inzage in en informatie over deze gegevens verstrekken.

- **Uw recht om rectificatie van uw gegevens te verzoeken overeenkomstig artikel 16 AVG:** Wij zullen onjuiste informatie corrigeren of onvolledige persoonsgegevens aanvullen, mits deze gegevens noodzakelijk zijn voor het beoogde doel van de verwerking van uw gegevens.
- **Uw recht om verwijdering van uw gegevens te verzoeken overeenkomstig artikel 17 AVG:** Wij zullen de persoonsgegevens die wij over u bewaren, verwijderen. Tenzij deze gegevens onderworpen zijn aan bewaartermijnen of bewaarplichten, bijvoorbeeld omdat wij uw gegevens moeten bewaren om aan onze contractuele verplichtingen te voldoen of zoals vereist door de wet.
- **Uw recht om beperking van de verwerking van uw gegevens te verzoeken overeenkomstig artikel 18 AVG:** In gevallen zoals beschreven in artikel 18 lid 1 AVG kunt u ons verzoeken uw gegevens te blokkeren. Wij zullen geblokkeerde gegevens slechts in zeer beperkte mate verder verwerken en indien nodig om dergelijke diensten of verplichtingen te vervullen, waarvan de uitvoering noodzakelijk is na de door u gevraagde blokkering van uw gegevens.
- **Uw recht om uw toestemming in te trekken overeenkomstig artikel 7 lid 3, AVG:** Voor gegevensverwerkingen waarvoor uw toestemming vereist is, kunt u uw toestemming te allen tijde intrekken om toekomstige verwerking van uw gegevens te voorkomen. Gegevensverwerkingen op basis van uw toestemming vóór uw intrekking blijven geldig en rechtmatig.
- **Uw recht om bezwaar te maken tegen de verwerking van uw gegevens overeenkomstig artikel 21 AVG:** U kunt bezwaar maken tegen toekomstige verwerking van uw gegevens, indien wij uw gegevens verwerken op basis van een van de rechts en zoals uiteengezet in artikel 6 lid 1, onder e) of f) van de AVG. Indien u bezwaar maakt, zullen wij de verwerking van uw gegevens staken, tenzij wij dwingende gerechtvaardigde gronden voor verdere verwerking hebben die zwaarder wegen dan uw belangen en rechten, of voor de vaststelling, uitoefening of verdediging van rechtsvorderingen. De verwerking van uw gegevens voor direct marketingdoeleinden vormt voor ons nooit een dwingende en gerechtvaardigde grond.
- **Uw recht op gegevensoverdraagbaarheid volgens artikel 20 AVG:** Wanneer de gegevensverwerking geautomatiseerd plaatsvindt en op basis van toestemming of een overeenkomst, kunnen wij u de gegevens die u aan ons heeft verstrekt, verstrekken in een gestructureerd, gangbaar en machinaal leesbaar formaat.
- **Uw recht om beroep in te stellen bij een toezichthoudende autoriteit:** U kunt een beroep inzake gegevensbescherming indienen bij een gegevensbeschermingsautoriteit. Neem hiervoor contact op met de relevante gegevensbeschermingsautoriteit die verantwoordelijk is voor uw woonplaats of de gegevensbeschermingsautoriteit onder wiens jurisdictie wij vallen (hieronder vermeld in de lijst van gegevensbeschermingsautoriteiten).

7. Beleid inzake verwijdering

In principe bewaren wij uw gegevens zo lang als nodig is om het nalevingsincident waarop uw melding betrekking heeft, te onderzoeken. Nadat het onderzoek is afgerond en de toepasselijke bewaartermijn is verstreken, zullen wij uw persoonsgegevens verwijderen, met uitzondering van gegevens waarvan verdere opslag vereist is voor de vaststelling, uitoefening of verdediging van rechtsvorderingen. De verwijdering van dergelijke gegevens wordt beheerst door de maximale wettelijke verjaringstermijnen krachtens de toepasselijke wetgeving.

8. Functionaris voor gegevensbescherming

Als u vragen heeft over gegevensbescherming of als u uw rechten wilt uitoefenen, staat onze functionaris voor gegevensbescherming (DPO) klaar om u te helpen. U kunt eenvoudig rechtstreeks contact opnemen met onze DPO door een brief of e-mail te sturen via de onderstaande contactgegevens:

- **Als u inwoner bent van een EU-/EER-lidstaat, neem dan contact op met:**
BSH Hausgeräte GmbH, Functionaris voor gegevensbescherming, Carl-Wery-Str. 34, 81739 München, Duitsland, Data-Protection-DE@bshg.com
- **Als u in het Verenigd Koninkrijk woont, neem dan contact op met:**
BSH Home Appliances Limited, Functionaris voor gegevensbescherming, Grand Union House, Old Wolverton Road, Wolverton, Milton Keynes, MK12 5PT, Data-Protection-UK@bshg.com
- **Als u in Zwitserland woont, neem dan contact op met:**
BSH Hausgeräte AG, vertegenwoordiger van Home Connect GmbH, BSH Hausgeräte AG, Fahrweidstrasse 80, CH-8954 Geroldswil, Data-Protection-CH@bshg.com

9. Wijzigingen in deze informatie over gegevensbescherming

Deze informatie over gegevensbescherming weerspiegelt de huidige stand van zaken met betrekking tot de gegevensverwerking op onze website en andere interactiepunten. In geval van wijzigingen in de gegevensverwerking wordt deze informatie over gegevensbescherming dienovereenkomstig bijgewerkt. Wij stellen altijd de meest recente versie van deze informatie over gegevensbescherming op onze website ter beschikking, zodat u op de hoogte bent van de omvang van de gegevensverwerking via deze website.

III. Behandeling van beschuldigingen en nalevingsonderzoek

1. Gegevensverwerking

a. Beheer van meldingen en nalevingsonderzoeken

De partij die meldingen ontvangt ("**Ontvangende Partij**") kan zowel wij zijn als de betreffende BSH-entiteit en is verantwoordelijk voor de eerste intake en documentatie van meldingen, het waarborgen van vertrouwelijkheid en het verzenden van een ontvangstbevestiging aan de klokkenluider waar mogelijk. Hierbij worden de verantwoordelijke themabeheerder en de wenselijkheid van het instellen van een onderzoek bepaald, waarbij de rechten van klokkenluiders en de beschuldigten worden gewaarborgd. De partij die het onderzoek uitvoert ("**Onderzoekende Partij**") kan zowel wij als de betreffende BSH-entiteit zijn en is verantwoordelijk voor diepgaand onderzoek, inclusief het aanpakken of implementeren van vervolmaatregelen, de juiste documentatie en de eindrapportage. Beide partijen zullen hun acties coördineren om transparantie en naleving van de vereisten inzake gegevensbescherming te waarborgen.

In het kader van gezamenlijke verwerkingsverantwoordelijkheid zijn de partijen als volgt verantwoordelijk voor de verwerking van persoonsgegevens:

- **Actie A (Ontvangende Partij):** Deze partij beheert de eerste intake van klokkenluidersmeldingen, inclusief de communicatie met de klokkenluider, het uitvoeren van eerste plausibiliteitscontroles en de classificatie van het onderwerp, en het documenteren van de zaak voor overdracht.
- **Actie B (Onderzoekende Partij):** Deze partij voert het diepgaande onderzoek uit naar aannemelijk wangedrag, inclusief verdere controles en het documenteren van alle onderzoeksgegevens en bevindingen.

b. Sturing, einddocumentatie en analyse

In het kader van gezamenlijke verwerkingsverantwoordelijkheid zijn de partijen als volgt verantwoordelijk voor de verwerking van persoonsgegevens voor de sturing, afsluiting en analyse van ontvangen meldingen en uitgevoerde compliance-onderzoeken:

- **Actie C:** Wij sturen het totale proces aan door begeleiding te bieden bij onderzoeken en door definitieve analytische rapporten op te stellen voor interne en externe belanghebbenden.
- **Actie D:** De betreffende BSH-entiteit is verantwoordelijk voor het centrale levenscyclusbeheer van alle gegevens, inclusief het opstellen, opslaan en verwijderen van klokkenluidersmeldingen en gegevens van nalevingsonderzoeken op centrale IT-systemen.

2. Vertrouwelijke behandeling van meldingen en gegevensoverdracht

Binnenkomende meldingen worden ontvangen door een kleine kring van uitdrukkelijk bevoegde en speciaal opgeleide medewerkers en worden altijd vertrouwelijk behandeld. Als onderdeel van de verwerking van een melding kan het nodig zijn deze door te sturen naar de verantwoordelijke medewerkers op het hoofdkantoor van BSH of de betreffende BSH-entiteit. Uw informatie wordt alleen toegankelijk gemaakt voor die medewerkers die deze nodig hebben om uw melding te verwerken en alleen voor zover toegestaan door de wetgeving inzake de bescherming van klokkenluiders. Alle personen die toegang krijgen tot uw melding zijn verplicht tot geheimhouding. Gegevens kunnen ook worden doorgegeven aan andere verantwoordelijke instanties (bijv. overheidsinstanties) indien wij hiertoe wettelijk verplicht zijn en voor zover dit is toegestaan door de wetgeving inzake de bescherming van klokkenluiders.

3. Gebruik van het klokkenluiderssysteem "Trust and Tell"

a. Beschikbaarstelling van de website.

De "Trust and Tell"-dienst wordt aangeboden via een website die namens ons wordt beheerd door een gespecialiseerde externe dienstverlener, EQS Group GmbH. De communicatie tussen uw computer en het BKMS®-systeem voor compliance-meldingen vindt plaats via een versleutelde verbinding (TLS).

b. Over de dienst

Het "Trust and Tell"-meldingssysteem dient om meldingen over compliance-overtredingen binnen of met betrekking tot ons en/of de betreffende BSH-entiteit veilig en vertrouwelijk te ontvangen, te verwerken en te beheren.

Het gebruik van het meldingssysteem is vrijwillig. Het is mogelijk om binnen het meldingssysteem een mailbox aan te maken die beveiligd is met een individueel gekozen pseudoniem/gebruikersnaam en wachtwoord. Hierdoor kunt u meldingen naar de verantwoordelijke medewerker bij ons of de betreffende BSH-entiteit sturen, hetzij onder uw eigen naam, hetzij op een anonieme, veilige manier. Dit systeem slaat gegevens uitsluitend op binnen het meldingssysteem, wat het bijzonder veilig maakt. Het is geen vorm van reguliere e-mailcommunicatie.

Wanneer u een melding of een aanvulling indient, kunt u tegelijkertijd bijlagen sturen naar de verantwoordelijke medewerker bij ons of de betreffende BSH-entiteit. Als u een anonieme melding wilt indienen, houd dan rekening met het volgende veiligheidsadvies: bestanden kunnen verborgen persoonlijke gegevens bevatten die uw anonimiteit in gevaar kunnen brengen. Verwijder deze gegevens voordat u ze verstuurt. Als u deze gegevens niet kunt verwijderen of niet zeker weet hoe u dit moet doen, kopieer dan de tekst van uw bijlage naar de tekst van uw melding.

c. IP-adres, cookies enz.

Het meldingssysteem registreert geen IP-adresgegevens, tijdstempels of metagegevens met betrekking tot het gebruik ervan door klokkenluiders.

Tijdens het gebruik van BKMS® Incident Reporting is de server niet in staat om de client (de computer van de gebruiker) uniek te identificeren. Om de client tijdens een sessie duidelijk te kunnen identificeren, verzendt de applicatie een sessiecookie naar de computer van de gebruiker. Deze sessiecookie wordt alleen gebruikt voor de huidige verbinding en bevat alleen een identificatienummer voor de lopende sessie. Deze cookie wordt verwijderd zodra de browser wordt gesloten. Dit sessienummer heeft geen verband met de klokkenluiders of de gegevens die worden ingediend en is alleen nodig om technische redenen.

IV. Lijst van externe dienstverleners en gezamenlijke verwerkingsverantwoordelijken en hun gebruik

De Ontvangende Partij kan zowel wij als de betreffende BSH-entiteit zijn en is verantwoordelijk voor de eerste ontvangst en documentatie van meldingen, het waarborgen van de vertrouwelijkheid en het verzenden van een ontvangstbevestiging aan de klokkenluiders waar mogelijk, en het bepalen van de verantwoordelijke themabeheerder en de wenselijkheid van het instellen van een onderzoek, met inachtneming van de rechten van klokkenluiders en de beschuldigten. De Onderzoekende Partij uitvoert, kan zowel wij als de betreffende BSH-entiteit zijn en is verantwoordelijk voor diepgaand onderzoek, inclusief het aanpakken of implementeren van vervolgmaatregelen, de juiste documentatie en de eindrapportage. Beide partijen zullen hun acties coördineren om transparantie en naleving van de gegevensbeschermingsvereisten te waarborgen.

In het kader van gezamenlijke verwerkingsverantwoordelijkheid zijn de partijen als volgt verantwoordelijk voor de verwerking van persoonsgegevens voor het beheer van beschuldigingen en nalevingsonderzoeken:

Verplichtingen op grond van de EU-AVG, de Britse AVG en de Zwitserse FADP <i>De verantwoordelijke partij plaatst een kruisje in de tabel onder haar respectieve verantwoordelijkheid</i>	Toepassingsgebied van actie A, B, C (BSH HQ)	Toepassingsgebied van actie A, B, D (BSH-entiteit)
Vereiste rechtsgrondslag voor gezamenlijke verwerking (Artikel 6 EU-AVG en Britse AVG, artikel 6 Zwitserse FADP)	[x] met betrekking tot de eigen verwerkingen	[x] met betrekking tot de eigen verwerkingen
Informatie verstrekken over gezamenlijke verwerking van persoonsgegevens (Artikel 13, 14 EU-AVG en Britse AVG, artikel 19 Zwitserse FADP)	[x] met betrekking tot de eigen verwerkingen	[x] met betrekking tot de eigen verwerkingen
De essentie van deze JCA beschikbaar stellen (Artikel 26 lid 2, EU-AVG en Britse AVG)	[x] met betrekking tot zijn eigen verwerkingen	[x] met betrekking tot haar eigen verwerkingen
Rechten van de betrokkene met betrekking tot de persoonsgegevens die door de partijen zijn opgeslagen na de gezamenlijke verwerking (Artikelen 15-20 EU-AVG en Britse AVG, artikelen 25-29 Zwitserse FADP)	[x] als centrale coördinator, ook voor de betreffende BSH-entiteit	

Verplichtingen op grond van de EU-AVG, de Britse AVG en de Zwitserse FADP <i>De verantwoordelijke partij plaatst een kruisje in de tabel onder haar respectieve verantwoordelijkheid</i>	Toepassingsgebied van actie A, B, C (BSH HQ)	Toepassingsgebied van actie A, B, D (BSH-entiteit)
Recht van bezwaar voor zover de gezamenlijke verwerking is gebaseerd op een gerechtvaardigd belang (Artikel 21 EU-AVG en UK-AVG)	[x] als centrale coördinator, ook voor de betreffende BSH-entiteit	
Beveiliging van de gezamenlijke verwerking (Artikel 32 EU-AVG en UK-AVG, artikel 8 Zwitserse FADP)	[x] voor door ons beheerde IT-systemen	[x] voor IT-systemen die worden beheerd door een BSH-entiteit
Inbreuken op persoonsgegevens met betrekking tot de gezamenlijke verwerking (Artikelen 33, 34 EU-AVG en UK-AVG, artikel 24 Zwitserse FADP)	[x] voor IT-systemen die door ons worden beheerd	[x] voor IT-systemen die worden beheerd door een BSH-entiteit

Daarnaast kunnen persoonsgegevens voor de volgende doeleinden aan deze derden worden doorgegeven:

- Het meldingssysteem "Trust and Tell" wordt beheerd door een gespecialiseerde externe dienstverlener, EQS Group GmbH, Karlstraße 47, D-80333 München, Duitsland, die optreedt als verwerker voor BSH. De gegevens worden opgeslagen in een database die door EQS Group GmbH wordt beheerd in een streng beveiligd datacentrum in de Europese Unie. De dienstverlener heeft geen toegang tot de gegevens. Dit wordt gewaarborgd door een gecertificeerde procedure en uitgebreide technische en organisatorische maatregelen.
- De ombudsman Dr. Karl Sidhu (SvS Attorneys at Law), Widenmayerstr. 36, 80538 München, Duitsland, treedt op als vertrouwensadvocaat en is een van de meldpunten voor klokkenluiders.
- Externe juridische adviseur ter ondersteuning van het onderzoek en de herstelmaatregelen.
- Overdracht aan Robert Bosch GmbH (onze moedermaatschappij), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, voor de technische verwerking van gegevens op IT-systemen die namens ons en de betreffende BSH-entiteit worden beheerd.
- Overdracht aan Robert Bosch GmbH (onze moedermaatschappij), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, voor het leveren van e-discovery-diensten (in het bijzonder het gebruik van tools om e-mails op een gestructureerde manier te beoordelen en te analyseren) namens ons en de betreffende BSH-entiteit.

V. Lijst van de AVG-gegevensbeschermingsautoriteiten

In overeenstemming met de AVG hebben personen het recht om hun persoonsgegevens te beschermen en kunnen zij hulp zoeken bij de relevante gegevensbeschermingsautoriteiten ("GBAs"). De onderstaande lijst is bedoeld om u een overzicht te geven van GBAs binnen het AVG-gebied. Het is belangrijk op te merken dat betrokkenen de keuze hebben om contact op te nemen met de GBA van hun woonplaats of de GBA die verantwoordelijk is voor de aanbieder van de website, afhankelijk van de locatie van de aanbieder.

Houd er rekening mee dat deze lijst niet volledig is en dat er mogelijk nog andere GBAs zijn binnen de AVG-regio of, als u zich niet in de AVG-regio bevindt, in uw land.

- **België:** Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA), <https://www.autoriteprotectiondonnees.be> <https://www.gegevensbeschermingsautoriteit.be>
- **Bulgarije:** Commissie voor de bescherming van persoonsgegevens, <https://www.cdpd.bg/>
- **Cyprus:** Commissaris voor de bescherming van persoonsgegevens, <http://www.dataprotection.gov.cy/>
- **Denemarken:** Datatilsynet, <http://www.datatilsynet.dk/>
- **Duitsland/Beieren:** Beierse gegevensbeschermingsautoriteit (BayLDA), <http://www.baylda.de>
- **Estland:** Estse Andmekaitse Inspeksioon (Andmekaitse Inspeksioon), <http://www.aki.ee/>
- **Finland:** Bureau van de Ombudsman voor gegevensbescherming, <http://www.tietosuoja.fi/en/>
- **Frankrijk:** Commission Nationale de l'Informatique et des Libertés – CNIL, <http://www.cnil.fr/> <https://www.cnil.fr/en/contact-cnil>
- **Griekenland:** Helleense Autoriteit voor gegevensbescherming, <http://www.dpa.gr/>
- **Hongarije:** Hongaarse Nationale Autoriteit voor Gegevensbescherming en Vrijheid van Informatie, <http://www.naih.hu/>
- **Ierland:** Data Protection Commission, <http://www.dataprotection.ie/>
- **IJsland:** Persónuvernd, <https://www.personuvernd.is> , <https://www.dpa.is>
- **Italië:** Garante per la protezione dei dati personali, <http://www.garanteprivacy.it/>
- **Kroatië:** Kroatisch Agentschap voor de bescherming van persoonsgegevens, <http://www.azop.hr/>
- **Letland:** Staatsinspectie voor gegevensbescherming, <https://www.dvi.gov.lv/>
- **Liechtenstein:** Autoriteit voor gegevensbescherming, Vorstendom Liechtenstein, <https://www.datenschutzstelle.li>
- **Litouwen:** Staatsinspectie voor gegevensbescherming, <https://vdai.lrv.lt/>
- **Luxemburg:** Nationale Commissie voor de bescherming van gegevens, <http://www.cnpd.lu/>
- **Malta:** Bureau van de commissaris voor informatie en gegevensbescherming, <http://www.idpc.org.mt/>
- **Nederland:** Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>
- **Noorwegen:** Datatilsynet, <https://www.datatilsynet.no>
- **Oostenrijk:** Österreichische Datenschutzbehörde, <http://www.dsb.gv.at/>
- **Polen:** Urząd Ochrony Danych Osobowych (Bureau voor de bescherming van persoonsgegevens), <https://uodo.gov.pl/>
- **Portugal:** Comissão Nacional de Proteção de Dados – CNPD, <http://www.cnpd.pt/>
- **Roemenië:** De Nationale Toezichthoudende Autoriteit voor de Verwerking van Persoonsgegevens, <http://www.dataprotection.ro/>
- **Slovenië:** Informatiecommissaris van de Republiek Slovenië, <https://www.ip-rs.si/>
- **Slowakije:** Bureau voor de bescherming van persoonsgegevens van de Slowaakse Republiek, <http://www.dataprotection.gov.sk/>
- **Spanje:** Agencia Española de Protección de Datos (AEPD), <https://www.aepd.es/>
- **Tsjechië:** Bureau voor de bescherming van persoonsgegevens, <http://www.uouu.cz/>
- **Zweden:** Integritetsskyddsmyndigheten, <http://www.imy.se/>

Geldig vanaf: juni 2026