B/S/H/

BSH Hausgeräte Gruppe

Data Protection Information

Data Protection Information for the reporting and investigation of compliance violations

I. The responsible for and purpose of the processing of personal data

We, BSH Hausgeräte GmbH, Carl-Wery-Strasse 34, 81739 Munich, Germany (“**BSH HQ” or “We/Us”)** and the BSH Entities within the European Union, Norway, Switzerland and United Kingdom (hereinafter "**BSH Entity**"), are the providers of the services described herein including the respective processing of personal data.

For the purpose of managing and investigating allegations of compliance violations ("Allegation Management & Compliance Investigations"), We and the respective BSH Entity act as joint controllers (see Art. 26 GDPR), as we jointly determine the purposes and means of processing your personal data.

We and the BSH Entity offer different reporting channels to submit reports about potential non-compliance, both on a central and local level:

- The Whistleblowing system "Trust and Tell" (TnT)
- Lawyer of Trust (LoT)
- Local Compliance Officer (LCO), located at BSH HQ or the respective BSH Entity.

This Data Protection Information informs you (hereinafter “You”), about the relevant processings of personal data within the scope of Allegation Management & Compliance Investigations.

II. Our Data Protection Principles

In the context of provision of the services described herein and the operation of websites and other touchpoints, We process your personal data in different ways. We are informing you about each processing of personal data as well as the respective legal basis and principles under which this processing takes place.

We are committed to protecting your personal data. Therefore, We process your data with great care and in strict compliance with applicable data protection laws and the individual permissions you may have given to Us. We have taken organisational and technical security measures to protect all our websites, apps and other (digital) touchpoints against the potential risks present in processing personal data. Our group companies and partners who support Us in the provision of the services must also comply with these rules and principles.

Please use the contact information provided in this Data Protection Information to contact Us either generally or with specific data protection questions and/or enquiries. There are different laws that regulate Data Protection depending on the country in which you are located. Based on the principles of the European General Data Protection Regulation, i.e. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC ("GDPR"), We defined the following basic principles as our guidelines on how We process and protect your personal data when providing our websites and services:

1. **Lawfulness**

We only use personal data if such use is lawful which in case of managing allegations and investigation of reported compliance violations is based on the following legal bases:

- **Art. 6 para. 1 lit. c) GDPR:** In Europe, the implementation of a whistleblowing management system is a legal obligation arising from the European Whistleblowing Directive (Regulation (EU) 2019/1937) and derived national transposition laws on whistleblower protection. The Directive allows the processing of personal data, which is necessary for handling of a report in accordance with the legislation.
- **Art. 6 para. 1 lit. f) GDPR:** The processing of personal data in the BKMS® System is based on the legitimate interests of our company to detect and prevent misconduct and thus avoid damage to BSH, its employees and customers, **as well as to pursue criminal offenses, assert civil claims, and prevent regulatory offenses.**

For all processing of personal data, We describe herein, We will also provide the legal reason for the processing in the description of the specific joint controller relationship between Us and the respective BSH Entity in Section IV of this data protection information.

2. **Fairness and Transparency**

We will inform you about the personal data We collect and why We collect it in a fair and transparent manner in this Data Protection Information. You can access the Data Protection Information directly or via a link when you register and/or at any touchpoint where you interact with Us. Users below the age of 16 should only transmit personal data to Us with the consent of their parent or legal guardian. The data protection law that applies in your country may result in different age limits in this regard.

3. **Purpose limitation and data minimization**

We only collect and use personal data that We really need and for the purpose that you provided the personal data to Us. If We can achieve the purpose with less personal data, We will only use the minimum data required. Nevertheless, at any time, you are free to provide additional personal data, if this would enhance your experience with the services provided.

4. **Types of processing including third parties**

In cases in which We do not process your personal data directly as data controller (e.g. website hosting, technical services etc.) We contract with third parties who deliver these services on our behalf as data processors. These contracts bind them for the processing of your personal data to secure the lawfulness and security of the processing. This is named a Controller to Processor relationship and is defined in Artt. 28/29 GDPR, where We are the Controller and the respective third party is the Processor. You will find a list of the data processors We engage at the end of this Data Protection Information.

Joint Controllership describes the situation, when multiple parties, We are being one of them, work together to decide how data will be used and managed (Joint Controllers, see Art. 26 GDPR). Joint Controllers need to inform clearly about who is processing which personal data and what obligations each party has taken over regarding the applicable data protection rules. As Joint Controllers agree on their roles and make sure the data subjects (people the data is about) are informed about these roles, We will inform you about these roles and your individual rights for each of the Joint Controllership situations described herein. When We use a third-party service or partner, who is processing personal data as a Joint Controller, We will inform you about the rights and roles accordingly in the third-party providers listing in Section XII at the very end of this document.

5. Security

We will process your data in a manner, which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Where We use third parties to process personal data, We commit these third parties to an appropriate level of technical or organisational measures to be followed.

6. User Rights

You have the following rights against Us which We comply with in a timely and adequate manner upon receipt of your respective request as outlined below:

- **Your right to request access to your personal data according to Art 15 GDPR:** We will inform you whether We hold personal data on you and if so, provide you access to and information about such data.
- **Your right to request rectification of your data according to Art. 16 GDPR:** We will correct inaccurate information or complete incomplete personal data, provided this data is necessary for the intended purpose of processing your data.
- **Your right to request deletion of your data according to Art. 17 GDPR:** We will delete the personal data We hold about you. Unless such data are subject to retention periods or retention rights, for example because We need to retain your data to fulfil our contractual obligations or as required by law.
- **Your right to request restricting processing of your data according to Art 18 GDPR:** In cases as outlined in Art. 18 (1) GDPR you may request Us to block your data. We will process blocked data only further to a very limited extent and if necessary to provide such services or obligations, which performance is necessary after the blocking of your data requested by you.
- **Your right to withdraw consent according to Art. 7 (3) GDPR:** For those data processings requiring your consent, you can withdraw your consent at any time to prevent future processing of your data. Data processings based on your consent prior to your withdrawal remain valid and lawful.
- **Your right to object to the processing of your data according to Art. 21 GDPR:** You can object to future processing of your data, if We are processing your data based on one of the legal

justifications set out in article 6 (1e or 1f) GDPR. If you object, We will cease processing your data, unless We have compelling legitimate grounds for further processing which override your interests and rights or for the establishment, exercise or defence of legal claims. The processing of your data for the purposes of direct marketing never constitutes compelling and legitimate grounds for Us.

- **Your right to data portability according to Art. 20 GDPR:** Where data processing is carried out by automated means and based on consent or contract, We can provide you your data you provided to Us in a structured, commonly used and machine-readable format.
- **Your right to appeal to a regulatory authority:** You can lodge an appeal pertaining to data protection with a Data Protection Authority. To do so, contact the relevant Data Protection Authority that is responsible for your place of residence or the data protection authority under whose jurisdiction We fall (named below in the List of the Data Protection Authorities).

7. Deletion principles

As a matter of principle, We store your data for as long as is necessary to investigate the compliance incident to which your report relates. After the investigation is complete and the applicable retention period has passed, We will delete your personal data, except for data whose further storage is required for the establishment, exercise or defence of legal claims. The deletion of such data is governed by the maximum statutory limitation periods under the applicable laws.

8. Data Protection Officer

If you have any questions regarding data protection or if you would like to exercise your rights, our Data Protection Officer (DPO) is here to assist you. You can easily get in touch with our DPO directly by sending a letter or an email using the contact information provided below:

- **If you are resident in an EU/EEA-Member-State, please contact:**
  BSH Hausgeräte GmbH, Data Protection Officer, Carl-Wery-Str. 34, 81739 Munich, Germany, Data-Protection-DE@bshg.com
- **If you are resident in the United Kingdom, please contact:**
  BSH Home Appliances Limited, Data Protection Officer, Grand Union House, Old Wolverton Road, Wolverton, Milton Keynes, MK12 5PT, Data-Protection-UK@bshg.com
- **If you are resident in Switzerland, please contact:**
  BSH Hausgeräte AG, Representative for Home Connect GmbH, BSH Hausgeräte AG, Fahrweidstrasse 80, CH-8954 Geroldswil, Data-Protection-CH@bshg.com

9. Changes to this Data Protection Information

This Data Protection Information reflects the current state of data processing on our website/and other points of interaction. In the event of changes to data processing, this Data Protection Information will be updated accordingly. We always provide the latest version of this Data Protection Information on our website so that you can be informed about the scope of data processing via this website.

III. Allegation Management and Compliance Investigation

1. Data Processing

a. Allegation Management & Compliance Investigations

The party receiving reports (“**Receiving Party**”) can be either Us or the respective BSH Entity and is responsible for the initial intake and documentation of reports, ensuring confidentiality and that a

confirmation of receipt is sent to the whistleblower where possible, and determining the responsible topic owner and the appropriateness of pursuing an investigation while safeguarding the rights of whistleblowers and those accused. The party conducting investigations ("**Investigating Party**") can be either Us or the respective BSH Entity and is responsible for in-depth investigations, including the addressing or implementation of subsequent measures, proper documentation and final reporting. Both parties will coordinate their actions to ensure transparency and compliance with data protection requirements.
Within the framework of joint controllership, the parties are responsible for the processing of personal data as follows:

- **Action A (Receiving Party)**: This party manages the initial intake of whistleblower reports, including communicating with the whistleblower, performing initial plausibility checks and classification of the subject matter, and documenting the case for handover.
- **Action B (Investigating Party)**: This party conducts the in-depth investigation of plausible misconduct, including further checks and documenting all investigation data and findings.

b. Steering, Final Documentation and Analysis

Within the framework of joint controllership, the parties are responsible for the processing of personal data for steering and closing and analysing of reports received and Compliance Investigations conducted as follows:

- **Action C**: We steer the overall process by providing guidance on investigations and creating final analytical reports for internal and external stakeholders.
- **Action D**: The respective BSH Entity is responsible for the central lifecycle management of all data, including preparing, storing, and deleting whistleblower reports and compliance investigation data on central IT systems.

2. Confidential Handling of Reports and Data Transfer

Incoming reports are received by a small circle of expressly authorized and specially trained employees and are always handled confidentially. As part of processing a report, it may be necessary to forward it to the responsible employees at BSH HQ or the respective BSH Entity. Your information will only be made accessible to those employees who require it to process your report and only to the extent permitted by whistleblower protection laws. All persons who gain access to your report are obligated to maintain confidentiality. Data may also be transferred to other responsible bodies (e.g., public authorities) if We are legally required to do so and to the extent permitted by whistleblower protection laws.

3. Using the "Trust and Tell" Whistleblowing System

a. Provision of the Website.

The "Trust and Tell" service is provided via a website operated by a specialised external service provider, EQS Group GmbH, on our behalf. The communication between your computer and the BKMS® System for compliance reporting takes place via an encrypted connection (TLS).

b. About the service

The "Trust and Tell" reporting system serves the purpose of securely and confidentially receiving, processing, and managing reports regarding compliance violations within or related to Us and/or the respective BSH Entity.

Use of the reporting system takes place on a voluntary basis. It is possible to set up a mailbox within the reporting system that is secured with an individually chosen pseudonym / username and password. This allows you to send reports to the responsible employee at Us or the respective BSH Entity either by name or in an anonymous, safe way. This system only stores data inside the reporting system, which makes it particularly secure. It is not a form of regular e-mail communication.

When submitting a report or an addition, you can simultaneously send attachments to the responsible employee at Us or the respective BSH Entity. If you wish to submit an anonymous report, please take note of the following security advice: Files can contain hidden personal data that could compromise your anonymity. Remove this data before sending. If you are unable to remove this data or are unsure how to do so, copy the text of your attachment into your report text.

c. IP address, Cookies etc.

The reporting system does not log IP address data, time stamps or metadata relating to its use by whistleblowers.

During use of the BKMS® Incident Reporting, the server is not capable of uniquely identifying the client (the user's computer). To be able to clearly identify the client during a session, the application transmits a session cookie to the user's Computer. This session cookie is only used for the current connection and only has an Identification number for the session in progress. This cookie is deleted once the browser is closed. This session number bears no relation to the whistleblower, or the data being submitted and is only necessary for technical reasons.

IV. List of the third-party providers and joint controllers and their use

The party receiving reports can be either Us or the respective BSH Entity and is responsible for the initial intake and documentation of reports, ensuring confidentiality and that a confirmation of receipt is sent to the whistleblower where possible, and determining the responsible topic owner and the appropriateness of pursuing an investigation while safeguarding the rights of whistleblowers and those accused. The party conducting investigations can be either Us or the respective BSH Entity and is responsible for in depth investigations, including the addressing or implementation of subsequent measures, proper documentation and final reporting. Both parties will coordinate their actions to ensure transparency and compliance with data protection requirements.

Within the framework of joint controllership, the parties are responsible for the processing of personal data for allegation management and compliance investigation as follows:

Obligations under the EU GDPR, the UK GDPR and the Swiss FADP) *The Responsible Party place a cross in the table under its respective responsibility*	Scope of Action A, B, C (BSH HQ)	Scope of Action A, B, D (BSH Entity)
Requirement of legal basis for Joint Processing (Article 6 EU GDPR and UK GDPR, Article 6 Swiss FADP),	[x] regarding its own processings	[x] regarding its own processings

Obligations under the EU GDPR, the UK GDPR and the Swiss FADP) *The Responsible Party place a cross in the table under its respective responsibility*	Scope of Action A, B, C (BSH HQ)	Scope of Action A, B, D (BSH Entity)
Providing information on Joint Processing of Personal Data (Article 13,14 EU GDPR and UK GDPR, Article 19 Swiss FADP)	[x] regarding its own processings	[x] regarding its own processings
Making available the essence of this JCA (Article 26(2) EU GDPR and UK GDPR)	[x] regarding its own processings	[x] regarding its own processings
Rights of the Data Subject with regards to the Personal Data stored by the parties after the Joint Processing (Articles 15-20 EU GDPR and UK GDPR, Articles 25-29 Swiss FADP)	[x] as central coordinator also for the respective BSH Entity	
Right to object insofar as the Joint Processing is based on legitimate interest (Article 21 EU GDPR and UK GDPR)	[x] as central coordinator also for the respective BSH Entity	
Security of the Joint Processing (Article 32:EU GDPR and UK GDPR, Article 8 Swiss FADP)	[x] for IT systems managed by Us	[x] for IT systems managed by BSH entity
Personal Data Breaches concerning the Joint Processing (Articles 33, 34 EU GDPR and UK GDPR, Article 24 Swiss FADP)	[x] for IT systems managed by Us	[x] for IT systems managed by BSH entity

Additionally, personal data may be transferred to these third parties for the following purposes:

- The "Trust and Tell" reporting system is operated by a specialised external service provider, EQS Group GmbH, Karlstraße 47, D-80333 München, Germany, acting as a processor for BSH. The data is stored in a database operated by EQS Group GmbH in a high-security data centre in the European Union. The service provider has no access to the data. This is ensured through a certified procedure and comprehensive technical and organizational measures.
- The Ombudsman Dr. Karl Sidhu (SvS Attorneys at Law), Widenmayerstr. 36, 80538 Munich, Germany acting as lawyer of trust as one of the intake channels for whistleblowers.
- External legal counsel to support the investigation and remediation.

- Transfer to Robert Bosch GmbH (our parent company), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, for technical processing of data on IT systems operated on behalf of Us and the respective BSH Entity.
- Transfer to Robert Bosch GmbH (our parent company), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, for the provision of e-discovery services (in particular the operation of tools to review and analyse emails in a structured way) on behalf of Us and the respective BSH Entity.

V. Involvement of the Supervisory Body according to Legislative Decree no. 231/2001

In case of reports concerning facts or conduct relevant pursuant to Legislative Decree no. 231/2001 and/or violations of the Organization, Management and Control Model adopted by the Company, the personal data contained in the report - including the data of the reporting person, if not anonymous, the reported person and any third parties involved, as well as the attached documentation - may be transmitted, in whole or in part, to the Supervisory Body (OdV) appointed pursuant to art. 6, D.Lgs. 231/2001.

Such communication is necessary for the fulfillment of legal obligations and for the pursuit of the legitimate interest of the Data Controller to ensure the proper functioning of the Model 231, preventing the commission of crimes required by art. 24 et seq. D.Lgs. 231/2001 and to ensure the correct management of the alert and to enable the ODV to carry out the supervisory tasks on the operation and compliance with Model 231 assigned to it by law and to assess the need to adopt corrective measures and adaptation of the Model itself.

The OdV operates as authorized subject pursuant to art. 29 GDPR and art. 2-quaterdecies of D.Lgs. 196/2003, specifically appointed and instructed by the Data Controller.

The transmission will take place in a strictly confidential manner, through protected channels and with application of the principle of minimization pursuant to art. 5, par. 1, lett. c) GDPR, restricting access to the only components of the OdV actually responsible for the evaluation.

The confidentiality of the identity of the reporting agent will be guaranteed in accordance with the provisions of art. 12, D. Lgs. 24/2023.

The data will be kept for the time necessary for the management of the report and in any case no later than 5 years from the communication of the final outcome of the procedure, pursuant to art. 14 D.Lgs. 24/2023, unless further storage for legal obligations.

VI. List of the GDPR Data Protection Authorities

In accordance with the General Data Protection Regulation (GDPR), individuals have the right to protect their personal data and can seek assistance from the relevant Data Protection Authorities (DPAs). The list below aims to provide you with a list of DPAs within the GDPR region. It is important to note that data subjects have the option to contact either the DPA of their place of residence or the DPA responsible for the website's provider, depending on the location of the provider. Please note that this list is not exhaustive, and there may be additional DPAs within the GDPR region or, if you are not in the GDPR region, in your country.

- **Austria:** Österreichische Datenschutzbehörde, http://www.dsb.gv.at/
- **Belgium:** Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA), https://www.autoriteprotectiondonnees.be https://www.gegevensbeschermingsautoriteit.be
- **Bulgaria:** Commission for Personal Data Protection, https://www.cpdp.bg/

- **Croatia:** Croatian Personal Data Protection Agency, http://www.azop.hr/
- **Cyprus:** Commissioner for Personal Data Protection, http://www.dataprotection.gov.cy/
- **Czech Republic:** Office for Personal Data Protection, http://www.uoou.cz/
- **Denmark:** Datatilsynet, http://www.datatilsynet.dk/
- **Estonia:** Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon), http://www.aki.ee/
- **Finland:** Office of the Data Protection Ombudsman, http://www.tietosuoja.fi/en/
- **France:** Commission Nationale de l'Informatique et des Libertés – CNIL, http://www.cnil.fr/ https://www.cnil.fr/en/contact-cnil
- **Germany/Bavaria:** Bavarian Data Protection Authority (BayLDA), http://www.baylda.de
- **Greece:** Hellenic Data Protection Authority, http://www.dpa.gr/
- **Hungary:** Hungarian National Authority for Data Protection and Freedom of Information, http://www.naih.hu/
- **Iceland:** Persónuvernd, https://www.personuvernd.is , https://www.dpa.is
- **Ireland:** Data Protection Commission, http://www.dataprotection.ie/
- **Italy:** Garante per la protezione dei dati personali, http://www.garanteprivacy.it/
- **Latvia:** Data State Inspectorate, https://www.dvi.gov.lv/
- **Liechtenstein:** Data Protection Authority, Principality of Liechtenstein, https://www.datenschutzstelle.li
- **Lithuania:** State Data Protection Inspectorate, https://vdai.lrv.lt/
- **Luxembourg:** 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/
- **Netherlands:** Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/
- **Norway:** Datatilsynet, https://www.datatilsynet.no
- **Poland:** Urząd Ochrony Danych Osobowych (Personal Data Protection Office), https://uodo.gov.pl/
- **Portugal:** Comissão Nacional de Proteção de Dados – CNPD, http://www.cnpd.pt/
- **Romania:** The National Supervisory Authority for Personal Data Processing, http://www.dataprotection.ro/
- **Slovakia:** Office for Personal Data Protection of the Slovak Republic, http://www.dataprotection.gov.sk/
- **Slovenia:** Information Commissioner of the Republic of Slovenia, https://www.ip-rs.si/
- **Spain:** Agencia Española de Protección de Datos (AEPD), https://www.aepd.es/
- **Sweden:** Integritetsskyddsmyndigheten, http://www.imy.se/

Valid from: June 2026