

Datenschutz- Hinweise

Datenschutzhinweise zur Meldung und Untersuchung von Compliance-Verstößen

I. Verantwortlicher und Zweck der Verarbeitung personenbezogener Daten

Wir, die BSH Hausgeräte GmbH, Carl-Wery-Straße 34, 81739 München, Deutschland („**BSH-Zentrale**“ oder „**Wir/Uns**“) und die BSH-Einheiten innerhalb der Europäischen Union, in Norwegen, der Schweiz und im Vereinigten Königreich (im Folgenden „**BSH-Einheit**“), sind die Anbieter der hierin beschriebenen Dienste einschließlich der jeweiligen Verarbeitung personenbezogener Daten.

Zum Zweck der Bearbeitung und Untersuchung von Vorwürfen wegen Compliance-Verstößen („Allegation Management & Compliance Investigations“) agieren wir und die jeweilige BSH-Einheit als gemeinsam Verantwortliche (siehe Art. 26 DSGVO), da wir gemeinsam die Zwecke und Mittel der Verarbeitung Ihrer personenbezogenen Daten festlegen.

Wir und die BSH-Einheit bieten verschiedene Meldewege an, um Meldungen über potenzielle Compliance-Verstöße sowohl auf zentraler als auch auf lokaler Ebene einzureichen:

- Das Whistleblowing-System „Trust and Tell“ (TnT)
- Lawyer of Trust (LoT)
- Lokaler Compliance-Beauftragter (LCO) am BSH-Hauptsitz oder bei der jeweiligen BSH-Einheit.

Diese Datenschutzhinweise informieren Sie (im Folgenden „Sie“) über die relevanten Verarbeitungen personenbezogener Daten im Rahmen des Allegation Management & Compliance Investigations.

II. Unsere Datenschutzgrundsätze

Im Zusammenhang mit der Erbringung der hier beschriebenen Dienstleistungen und dem Betrieb von Webseiten und anderen Kontaktpunkten verarbeiten Wir Ihre personenbezogenen Daten auf verschiedene Weise. Wir informieren Sie über jede Verarbeitung personenbezogener Daten sowie über die jeweilige Rechtsgrundlage und die Grundsätze, nach denen diese Verarbeitung erfolgt.

Wir verpflichten uns zum Schutz Ihrer personenbezogenen Daten. Daher verarbeiten wir Ihre Daten mit großer Sorgfalt und unter strikter Einhaltung der geltenden Datenschutzgesetze sowie der individuellen Einwilligungen, die Sie uns gegebenenfalls erteilt haben. Wir haben organisatorische und technische Sicherheitsmaßnahmen getroffen, um alle unsere Webseiten, Apps und sonstigen (digitalen) Kontaktpunkte vor den potenziellen Risiken zu schützen, die bei der Verarbeitung personenbezogener Daten bestehen. Unsere Konzernunternehmen und Partner, die uns bei der Erbringung der Dienstleistungen unterstützen, müssen diese Regeln und Grundsätze ebenfalls einhalten.

Bitte nutzen Sie die in dieser Datenschutzerklärung angegebenen Kontaktdaten, um uns allgemein oder bei spezifischen Fragen und/oder Anfragen zum Datenschutz zu kontaktieren. Je nach dem Land, in dem Sie sich befinden, gelten unterschiedliche Gesetze zum Datenschutz. Auf der Grundlage der Grundsätze der Europäischen Datenschutz-Grundverordnung, d. h. der VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („DSGVO“), haben wir die folgenden Grundprinzipien als Leitlinien für die Verarbeitung und den Schutz Ihrer personenbezogenen Daten bei der Bereitstellung unserer Webseiten und Dienste festgelegt:

1. Rechtmäßigkeit

Wir verwenden personenbezogene Daten nur, wenn diese Verwendung rechtmäßig ist, was im Falle der Bearbeitung von Vorwürfen und der Untersuchung gemeldeter Compliance-Verstöße auf den folgenden Rechtsgrundlagen beruht:

- **Art. 6 Abs. 1 lit. c) DSGVO:** In Europa ist die Einrichtung eines Whistleblowing-Managementsystems eine gesetzliche Verpflichtung, die sich aus der Europäischen Whistleblowing-Richtlinie (Verordnung (EU) 2019/1937) und den daraus abgeleiteten nationalen Umsetzungsgesetzen zum Whistleblower-Schutz ergibt. Die Richtlinie erlaubt die Verarbeitung personenbezogener Daten, die für die Bearbeitung einer Meldung im Einklang mit den gesetzlichen Bestimmungen erforderlich ist.
- **Art. 6 Abs. 1 lit. f) DSGVO:** Die Verarbeitung personenbezogener Daten im BKMS®-System stützt sich auf die berechtigten Interessen unseres Unternehmens, Fehlverhalten aufzudecken und zu verhindern und damit Schäden für die BSH, ihre Mitarbeiter und Kunden abzuwenden **sowie Straftaten zu verfolgen, zivilrechtliche Ansprüche geltend zu machen und Ordnungswidrigkeiten zu verhindern.**

Für alle hierin beschriebenen Verarbeitungen personenbezogener Daten werden Wir den Rechtsgrund für die Verarbeitung auch in der Beschreibung der konkreten Beziehung zwischen den gemeinsamen Verantwortlichen zwischen Uns und der jeweiligen BSH-Einheit in Abschnitt IV dieser Datenschutzhinweise angeben.

2. Fairness und Transparenz

Wir informieren Sie in dieser Datenschutzerklärung auf faire und transparente Weise darüber, welche personenbezogenen Daten Wir erheben und warum wir dies tun. Sie können direkt oder über einen Link auf die Datenschutzerklärung zugreifen, wenn Sie sich registrieren und/oder an jedem Kontaktpunkt, an dem Sie mit uns interagieren. Nutzer unter 16 Jahren sollten personenbezogene Daten nur mit Zustimmung ihrer Eltern oder ihres Erziehungsberechtigten an uns übermitteln. Das in Ihrem Land geltende Datenschutzrecht kann diesbezüglich zu unterschiedlichen Altersgrenzen führen.

3. Zweckbindung und Datenminimierung

Wir erheben und verwenden personenbezogene Daten nur, soweit Wir diese tatsächlich benötigen und für den Zweck, für den Sie Uns die personenbezogenen Daten zur Verfügung gestellt haben. Wenn Wir den Zweck mit weniger personenbezogenen Daten erreichen können, verwenden Wir nur die minimal erforderlichen Daten. Es steht Ihnen jedoch jederzeit frei, zusätzliche personenbezogene Daten anzugeben, wenn dies Ihre Erfahrung mit den angebotenen Diensten verbessern würde.

4. Arten der Datenverarbeitung unter Einbeziehung Dritter

In Fällen, in denen Wir Ihre personenbezogenen Daten nicht direkt als Verantwortlicher verarbeiten (z. B. Webseiten-Hosting, technische Dienste usw.), beauftragen wir Dritte, die diese Dienste in unserem Auftrag als Auftragsverarbeiter erbringen. Diese Verträge verpflichten die Auftragsverarbeiter zur Verarbeitung Ihrer personenbezogenen Daten, um die Rechtmäßigkeit und Sicherheit der Verarbeitung zu gewährleisten. Dies wird als Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter bezeichnet und ist in den Art. 28/29 DSGVO definiert, wobei Wir der Verantwortliche sind und der jeweilige Dritte der Auftragsverarbeiter ist. Eine Liste der von Uns beauftragten Auftragsverarbeiter finden Sie am Ende dieser Datenschutzerklärung.

Die gemeinsame Verantwortlichkeit beschreibt die Situation, in der mehrere Parteien, zu denen auch Wir gehören, gemeinsam entscheiden, wie Daten verwendet und verwaltet werden (gemeinsame Verantwortliche, siehe Art. 26 DSGVO). Gemeinsame Verantwortliche müssen klar darüber informieren, wer welche personenbezogenen Daten verarbeitet und welche Verpflichtungen jede Partei hinsichtlich der geltenden Datenschutzvorschriften übernommen hat. Da sich die gemeinsam Verantwortlichen über ihre Rollen einigen und sicherstellen, dass die betroffenen Personen (die Personen, auf die sich die Daten beziehen) über diese Rollen informiert werden, werden wir Sie über diese Rollen und Ihre individuellen Rechte für jede der hier beschriebenen Situationen der gemeinsamen Verantwortlichkeit informieren. Wenn Wir einen Drittanbieter oder Partner nutzen, der personenbezogene Daten als gemeinsam Verantwortlicher verarbeitet, werden wir Sie über die entsprechenden Rechte und Rollen in der Liste der Drittanbieter in Abschnitt IV ganz am Ende dieses Dokuments informieren.

5. Sicherheit

Wir verarbeiten Ihre Daten in einer Weise, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor versehentlichem Verlust, Zerstörung oder Beschädigung, unter Einsatz geeigneter technischer oder organisatorischer Maßnahmen. Wenn Wir Dritte zur Verarbeitung personenbezogener Daten einsetzen, verpflichten wir diese Dritten zur Einhaltung eines angemessenen Niveaus an technischen oder organisatorischen Maßnahmen.

6. Nutzerrechte

Sie haben gegenüber uns die folgenden Rechte, denen Wir nach Erhalt Ihrer entsprechenden Anfrage, wie nachstehend beschrieben, zeitnah und angemessen nachkommen:

- **Ihr Recht auf Auskunft über Ihre personenbezogenen Daten gemäß Art. 15 DSGVO:** Wir teilen Ihnen mit, ob Wir personenbezogene Daten über Sie gespeichert haben, und gewähren Ihnen in diesem Fall Auskunft über diese Daten.

- **Ihr Recht auf Berichtigung Ihrer Daten gemäß Art. 16 DSGVO:** Wir werden unrichtige Angaben berichtigen oder unvollständige personenbezogene Daten vervollständigen, sofern diese Daten für den beabsichtigten Zweck der Verarbeitung Ihrer Daten erforderlich sind.
- **Ihr Recht auf Löschung Ihrer Daten gemäß Art. 17 DSGVO:** Wir werden die personenbezogenen Daten, die Wir über Sie gespeichert haben, löschen. Es sei denn, diese Daten unterliegen Aufbewahrungsfristen oder Aufbewahrungsrechten, beispielsweise weil Wir Ihre Daten zur Erfüllung unserer vertraglichen Verpflichtungen oder aufgrund gesetzlicher Vorschriften aufbewahren müssen.
- **Ihr Recht auf Einschränkung der Verarbeitung Ihrer Daten gemäß Art. 18 DSGVO:** In den in Art. 18 Abs. 1 DSGVO genannten Fällen können Sie von Uns die Sperrung Ihrer Daten verlangen. Wir werden gesperrte Daten nur in sehr begrenztem Umfang weiterverarbeiten und nur, soweit dies zur Erfüllung von Dienstleistungen oder Verpflichtungen erforderlich ist, deren Erfüllung nach der von Ihnen beantragten Sperrung Ihrer Daten notwendig ist.
- **Ihr Recht auf Widerruf der Einwilligung gemäß Art. 7 Abs. 3 DSGVO:** Bei Datenverarbeitungen, die Ihrer Einwilligung bedürfen, können Sie Ihre Einwilligung jederzeit widerrufen, um eine künftige Verarbeitung Ihrer Daten zu verhindern. Datenverarbeitungen, die auf Ihrer Einwilligung vor dem Widerruf beruhen, bleiben gültig und rechtmäßig.
- **Ihr Recht auf Widerspruch gegen die Verarbeitung Ihrer Daten gemäß Art. 21 DSGVO:** Sie können der künftigen Verarbeitung Ihrer Daten widersprechen, wenn Wir Ihre Daten auf der Grundlage einer der in Artikel 6 Absatz 1 Buchstabe e oder f DSGVO genannten Rechtsgrundlagen verarbeiten. Wenn Sie Widerspruch einlegen, werden wir die Verarbeitung Ihrer Daten einstellen, es sei denn, Wir haben zwingende berechtigte Gründe für die weitere Verarbeitung, die Ihre Interessen und Rechte überwiegen, oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Die Verarbeitung Ihrer Daten zum Zwecke des Direktmarketings stellt für Uns niemals einen zwingenden und berechtigten Grund dar.
- **Ihr Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO:** Sofern die Datenverarbeitung automatisiert erfolgt und auf einer Einwilligung oder einem Vertrag beruht, können Wir Ihnen die Daten, die Sie uns zur Verfügung gestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.
- **Ihr Recht auf Beschwerde bei einer Aufsichtsbehörde:** Sie können eine Beschwerde in Bezug auf den Datenschutz bei einer Datenschutzbehörde einreichen. Wenden Sie sich dazu an die für Ihren Wohnsitz zuständige Datenschutzbehörde oder an die Datenschutzbehörde, deren Zuständigkeit Wir unterliegen (siehe unten in der Liste der Datenschutzbehörden).

7. Löschgrundsätze

Grundsätzlich speichern Wir Ihre Daten so lange, wie es zur Untersuchung des Compliance-Vorfalles, auf den sich Ihre Meldung bezieht, erforderlich ist. Nach Abschluss der Untersuchung und Ablauf der geltenden Aufbewahrungsfrist löschen Wir Ihre personenbezogenen Daten, mit Ausnahme von Daten, deren weitere Speicherung zur Begründung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Die Löschung solcher Daten unterliegt den maximalen gesetzlichen Verjährungsfristen nach den geltenden Gesetzen.

8. Datenschutzbeauftragter

Wenn Sie Fragen zum Datenschutz haben oder Ihre Rechte ausüben möchten, steht Ihnen unser Datenschutzbeauftragter (DSB) gerne zur Verfügung. Sie können sich einfach direkt an unseren DSB wenden, indem Sie einen Brief oder eine E-Mail an die unten angegebenen Kontaktdaten senden:

- **Wenn Sie in einem EU-/EWR-Mitgliedstaat ansässig sind, wenden Sie sich bitte an:**
BSH Hausgeräte GmbH, Datenschutzbeauftragter, Carl-Wery-Str. 34, 81739 München, Deutschland, Data-Protection-DE@bshg.com
- **Wenn Sie im Vereinigten Königreich ansässig sind, wenden Sie sich bitte an:**
BSH Home Appliances Limited, Datenschutzbeauftragter, Grand Union House, Old Wolverton Road, Wolverton, Milton Keynes, MK12 5PT, Data-Protection-UK@bshg.com
- **Wenn Sie in der Schweiz ansässig sind, wenden Sie sich bitte an:**
BSH Hausgeräte AG, Vertreter der Home Connect GmbH, BSH Hausgeräte AG, Fahrweidstrasse 80, CH-8954 Geroldswil, Data-Protection-CH@bshg.com

9. Änderungen dieser Datenschutzhinweise

Diese Datenschutzhinweise spiegeln den aktuellen Stand der Datenverarbeitung auf unserer Webseite sowie an anderen Kontaktpunkten wider. Im Falle von Änderungen der Datenverarbeitung werden diese Datenschutzhinweise entsprechend aktualisiert. Wir stellen auf unserer Webseite stets die aktuellste Version dieser Datenschutzhinweise zur Verfügung, damit Sie über den Umfang der Datenverarbeitung über diese Webseite informiert sind.

III. Beschwerdemanagement und Compliance-Untersuchungen

1. Datenverarbeitung

a. Beschwerdemanagement & Compliance-Untersuchungen

Die Stelle, die Meldungen entgegennimmt („Empfängerstelle“), kann entweder Wir oder die jeweilige BSH-Einheit sein und ist verantwortlich für die erste Entgegennahme und Dokumentation von Meldungen, die Gewährleistung der Vertraulichkeit und die Versendung einer Empfangsbestätigung an den Hinweisgeber sofern möglich, sowie für die Ermittlung des zuständigen Themenverantwortlichen und die Beurteilung der Angemessenheit einer Untersuchung unter Wahrung der Rechte von Hinweisgebern und Beschuldigten. Die Partei, die die Untersuchungen durchführt („**Untersuchende Partei**“), kann entweder Wir oder die jeweilige BSH-Einheit sein und ist für eingehende Untersuchungen verantwortlich, einschließlich der Ergreifung oder Umsetzung von Folgemaßnahmen, der ordnungsgemäßen Dokumentation und der abschließenden Berichterstattung. Beide Parteien koordinieren ihre Maßnahmen, um Transparenz und die Einhaltung der Datenschutzerfordernisse sicherzustellen.

Im Rahmen der gemeinsamen Verantwortlichkeit sind die Parteien wie folgt für die Verarbeitung personenbezogener Daten verantwortlich:

- **Maßnahme A (Empfangende Partei):** Diese Partei verwaltet die erste Entgegennahme von Whistleblower-Meldungen, einschließlich der Kommunikation mit dem Whistleblower, der Durchführung erster Plausibilitätsprüfungen und der Einstufung des Sachverhalts sowie der Dokumentation des Falls zur Übergabe.
- **Maßnahme B (Untersuchende Partei):** Diese Partei führt die eingehende Untersuchung des plausiblen Fehlverhaltens durch, einschließlich weiterer Überprüfungen und der Dokumentation aller Untersuchungsdaten und -ergebnisse.

b. Steuerung, abschließende Dokumentation und Analyse

Im Rahmen der gemeinsamen Verantwortlichkeit sind die Parteien wie folgt für die Verarbeitung personenbezogener Daten zur Steuerung, zum Abschluss und zur Analyse der eingegangenen Meldungen sowie der durchgeführten Compliance-Untersuchungen verantwortlich:

- **Maßnahme C:** Wir steuern den Gesamtprozess, indem Wir Leitlinien für Untersuchungen bereitstellen und abschließende Analyseberichte für interne und externe Stakeholder erstellen.
- **Maßnahme D:** Die jeweilige BSH-Einheit ist für das zentrale Lebenszyklusmanagement aller Daten verantwortlich, einschließlich der Erstellung, Speicherung und Löschung von Whistleblower-Meldungen und Daten aus Compliance-Untersuchungen in zentralen IT-Systemen.

2. Vertrauliche Behandlung von Meldungen und Datenübermittlung

Eingehende Meldungen werden von einem kleinen Kreis ausdrücklich befugter und speziell geschulter Mitarbeiter entgegengenommen und stets vertraulich behandelt. Im Rahmen der Bearbeitung einer Meldung kann es erforderlich sein, diese an die zuständigen Mitarbeiter in der BSH-Zentrale oder der jeweiligen BSH-Einheit weiterzuleiten. Ihre Informationen werden nur denjenigen Mitarbeitern zugänglich gemacht, die diese zur Bearbeitung Ihrer Meldung benötigen, und nur in dem Umfang, der nach den Gesetzen zum Schutz von Hinweisgebern zulässig ist. Alle Personen, die Zugang zu Ihrer Meldung erhalten, sind zur Vertraulichkeit verpflichtet. Daten können auch an andere zuständige Stellen (z. B. Behörden) weitergegeben werden, wenn Wir gesetzlich dazu verpflichtet sind und soweit dies nach den Gesetzen zum Schutz von Hinweisgebern zulässig ist.

3. Nutzung des Whistleblowing-Systems „Trust and Tell“

a. Bereitstellung der Website.

Der „Trust and Tell“-Dienst wird über eine Webseite bereitgestellt, die von einem spezialisierten externen Dienstleister, der EQS Group GmbH, in unserem Auftrag betrieben wird. Die Kommunikation zwischen Ihrem Computer und dem BKMS®-System für Compliance-Meldungen erfolgt über eine verschlüsselte Verbindung (TLS).

b. Über den Dienst

Das „Trust and Tell“-Meldesystem dient dem sicheren und vertraulichen Empfang, der Bearbeitung und der Verwaltung von Meldungen über Compliance-Verstöße innerhalb oder im Zusammenhang mit Uns und/oder der jeweiligen BSH-Einheit.

Die Nutzung des Meldesystems erfolgt auf freiwilliger Basis. Es besteht die Möglichkeit, innerhalb des Meldesystems ein Postfach einzurichten, das durch ein individuell gewähltes Pseudonym/Benutzername und ein Passwort gesichert ist. Dies ermöglicht es Ihnen, Meldungen entweder namentlich oder auf anonyme, sichere Weise an den zuständigen Mitarbeiter bei Uns oder der jeweiligen BSH-Einheit zu senden. Dieses System speichert Daten ausschließlich innerhalb des Meldesystems, was es besonders sicher macht. Es handelt sich nicht um eine Form der regulären E-Mail-Kommunikation.

Wenn Sie eine Meldung oder eine Ergänzung einreichen, können Sie gleichzeitig Anhänge an den zuständigen Mitarbeiter bei Uns oder der jeweiligen BSH-Einheit senden. Wenn Sie eine anonyme Meldung einreichen möchten, beachten Sie bitte die folgenden Sicherheitshinweise: Dateien können versteckte personenbezogene Daten enthalten, die Ihre Anonymität gefährden könnten. Entfernen Sie diese Daten vor dem Absenden. Wenn Sie diese Daten nicht entfernen können oder sich nicht sicher sind, wie Sie dies tun sollen, kopieren Sie den Text Ihres Anhangs in Ihren Meldungstext.

c. IP-Adresse, Cookies usw.

Das Meldesystem protokolliert keine IP-Adressdaten, Zeitstempel oder Metadaten im Zusammenhang mit der Nutzung durch Hinweisgeber.

Bei der Nutzung des BKMS® Incident Reporting ist der Server nicht in der Lage, den Client (den Computer des Nutzers) eindeutig zu identifizieren. Um den Client während einer Sitzung eindeutig identifizieren zu können, übermittelt die Anwendung ein Sitzungscookie an den Computer des Nutzers. Dieses Sitzungscookie wird nur für die aktuelle Verbindung verwendet und enthält lediglich eine Identifikationsnummer für die laufende Sitzung. Dieses Cookie wird gelöscht, sobald der Browser geschlossen wird. Diese Sitzungsnummer steht in keinem Zusammenhang mit dem Hinweisgeber oder den übermittelten Daten und ist nur aus technischen Gründen erforderlich.

IV. Liste der Drittanbieter und gemeinsam Verantwortlichen sowie deren Einsatz

Die Stelle, die Meldungen entgegennimmt, kann entweder Wir oder die jeweilige BSH-Einheit sein und ist verantwortlich für die erste Entgegennahme und Dokumentation von Meldungen, die Gewährleistung der Vertraulichkeit und die Versendung einer Empfangsbestätigung an den Hinweisgeber, soweit möglich, sowie für die Ermittlung des zuständigen Themenverantwortlichen und die Beurteilung der Angemessenheit einer Untersuchung unter Wahrung der Rechte von Hinweisgebern und Beschuldigten. Die Partei, die Untersuchungen durchführt, kann entweder wir oder die jeweilige BSH-Einheit sein und ist für eingehende Untersuchungen verantwortlich, einschließlich der Ergreifung oder Umsetzung von Folgemaßnahmen, der ordnungsgemäßen Dokumentation und der abschließenden Berichterstattung. Beide Parteien koordinieren ihre Maßnahmen, um Transparenz und die Einhaltung der Datenschutzanforderungen sicherzustellen.

Im Rahmen der gemeinsamen Verantwortlichkeit sind die Parteien wie folgt für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Vorfallmanagement und der Compliance-Untersuchung verantwortlich:

Verpflichtungen gemäß der EU-DSGVO, der britischen DSGVO und dem Schweizer DSG <i>Die verantwortliche Partei kreuzt in der Tabelle unter ihrer jeweiligen Zuständigkeit an</i>	Handlungsbereich A, B, C (BSH-Zentrale)	Handlungsbereich A, B, D (BSH-Einheit)
Erfordernis einer Rechtsgrundlage für die gemeinsame Verarbeitung (Artikel 6 EU-DSGVO und UK-DSGVO, Artikel 6 Schweizer DSG),	[x] in Bezug auf die eigenen Verarbeitungen	[x] bezüglich der eigenen Verarbeitungen
Bereitstellung von Informationen zur gemeinsamen Verarbeitung personenbezogener Daten (Artikel 13, 14 EU-DSGVO und UK-DSGVO, Artikel 19 Schweizer DSG)	[x] bezüglich der eigenen Verarbeitungen	[x] bezüglich der eigenen Verarbeitungen
Bereitstellung des wesentlichen Inhalts dieser gemeinsamen Verarbeitung (Artikel 26 Absatz 2 EU-DSGVO und UK-DSGVO)	[x]	[x]

Verpflichtungen gemäß der EU-DSGVO, der britischen DSGVO und dem Schweizer DSG <i>Die verantwortliche Partei kreuzt in der Tabelle unter ihrer jeweiligen Zuständigkeit an</i>	Handlungsbereich A, B, C (BSH-Zentrale)	Handlungsbereich A, B, D (BSH-Einheit)
	in Bezug auf die eigenen Verarbeitungen	in Bezug auf die eigenen Verarbeitungen
Rechte der betroffenen Person in Bezug auf die von den Parteien nach der gemeinsamen Verarbeitung gespeicherten personenbezogenen Daten (Artikel 15–20 EU-DSGVO und UK-DSGVO, Artikel 25–29 Schweizer DSG)	[x] als zentraler Koordinator auch für die jeweilige BSH-Einheit	
Widerspruchsrecht, soweit die gemeinsame Verarbeitung auf einem berechtigten Interesse beruht (Artikel 21 EU-DSGVO und UK-DSGVO)	[x] als zentraler Koordinator auch für die jeweilige BSH-Einheit	
Sicherheit der gemeinsamen Verarbeitung (Artikel 32: EU-DSGVO und UK-DSGVO, Artikel 8 Schweizer DSG)	[x] für von uns verwaltete IT-Systeme	[x] für von einer BSH-Einheit verwaltete IT-Systeme
Verstöße gegen den Datenschutz bei der gemeinsamen Verarbeitung (Artikel 33, 34 EU-DSGVO und UK-DSGVO, Artikel 24 Schweizer DSG)	[x] für von uns verwaltete IT-Systeme	[x] für von einer BSH-Einheit verwaltete IT-Systeme

Darüber hinaus können personenbezogene Daten zu folgenden Zwecken an diese Dritten übermittelt werden:

- Das Meldesystem „Trust and Tell“ wird von einem spezialisierten externen Dienstleister, der EQS Group GmbH, Karlstraße 47, D-80333 München, Deutschland, betrieben, der als Auftragsverarbeiter für die BSH tätig ist. Die Daten werden in einer von der EQS Group GmbH betriebenen Datenbank in einem Hochsicherheitsrechenzentrum in der Europäischen Union gespeichert. Der Dienstleister hat keinen Zugriff auf die Daten. Dies wird durch ein zertifiziertes Verfahren sowie umfassende technische und organisatorische Maßnahmen sichergestellt.
- Der Ombudsmann Dr. Karl Sidhu (SvS Rechtsanwälte), Widenmayerstr. 36, 80538 München, Deutschland, fungiert als Vertrauensanwalt und ist einer der Anlaufstellen für Hinweisgeber.
- Externer Rechtsbeistand zur Unterstützung der Untersuchung und Abhilfe.
- Weitergabe an die Robert Bosch GmbH (unsere Muttergesellschaft), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, zur technischen Verarbeitung von Daten auf IT-Systemen, die im Auftrag von Uns und der jeweiligen BSH-Einheit betrieben werden.

- Übermittlung an die Robert Bosch GmbH (unsere Muttergesellschaft), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, zur Erbringung von E-Discovery-Dienstleistungen (insbesondere zum Betrieb von Tools zur strukturierten Überprüfung und Analyse von E-Mails) im Auftrag von Uns und der jeweiligen BSH-Einheit.

V. Liste der Datenschutzbehörden gemäß DSGVO

Gemäß der Datenschutz-Grundverordnung (DSGVO) haben natürliche Personen das Recht auf den Schutz ihrer personenbezogenen Daten und können sich an die zuständigen Datenschutzbehörden (DPAs) wenden. Die nachstehende Liste soll Ihnen einen Überblick über die Datenschutzbehörden im Geltungsbereich der DSGVO geben. Bitte beachten Sie, dass betroffene Personen je nach Standort des Anbieters entweder die Datenschutzbehörde ihres Wohnsitzes oder die für den Anbieter der Website zuständige Datenschutzbehörde kontaktieren können. Bitte beachten Sie, dass diese Liste nicht vollständig ist und es weitere Datenschutzbehörden innerhalb des DSGVO-Raums oder, falls Sie sich nicht im DSGVO-Raum befinden, in Ihrem Land geben kann.

- **Österreich:** 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:** Kommission für den Schutz personenbezogener Daten, <https://www.cdpd.bg/>
- **Kroatien:** Kroatische Datenschutzbehörde, <http://www.azop.hr/>
- **Zypern:** Beauftragter für den Schutz personenbezogener Daten, <http://www.dataprotection.gov.cy/>
- **Tschechische Republik:** Amt für den Schutz personenbezogener Daten, <http://www.uouu.cz/>
- **Dänemark:** Datatilsynet, <http://www.datatilsynet.dk/>
- **Estland:** Estnische Datenschutzbehörde (Andmekaitse Inspeksioon), <http://www.aki.ee/>
- **Finnland:** Amt des Datenschutzbeauftragten, <http://www.tietosuoja.fi/en/>
- **Frankreich:** Commission Nationale de l'Informatique et des Libertés – CNIL, <http://www.cnil.fr/> <https://www.cnil.fr/en/contact-cnil>
- **Deutschland/Bayern:** Bayerische Landesdatenschutzbehörde (BayLDA), <http://www.baylda.de>
- **Griechenland:** Griechische Datenschutzbehörde, <http://www.dpa.gr/>
- **Ungarn:** Ungarische Nationale Behörde für Datenschutz und Informationsfreiheit, <http://www.naih.hu/>
- **Island:** Persónuvernd, <https://www.personuvernd.is>, <https://www.dpa.is>
- **Irland:** Datenschutzkommission, <http://www.dataprotection.ie/>
- **Italien:** Garante per la protezione dei dati personali, <http://www.garanteprivacy.it/>
- **Lettland:** Staatliche Datenschutzinspektion, <https://www.dvi.gov.lv/>
- **Liechtenstein:** Datenschutzbehörde, Fürstentum Liechtenstein, <https://www.datenschutzstelle.li>
- **Litauen:** Staatliche Datenschutzinspektion, <https://vdai.lrv.lt/>
- **Luxemburg:** Nationale Kommission für den Datenschutz, <http://www.cnpd.lu/>
- **Malta:** Amt des Informations- und Datenschutzbeauftragten, <http://www.idpc.org.mt/>
- **Niederlande:** Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>
- **Norwegen:** Datatilsynet, <https://www.datatilsynet.no>
- **Polen:** Urząd Ochrony Danych Osobowych (Amt für den Schutz personenbezogener Daten), <https://uodo.gov.pl/>
- **Portugal:** Comissão Nacional de Proteção de Dados – CNPD, <http://www.cnpd.pt/>
- **Rumänien:** Nationale Aufsichtsbehörde für die Verarbeitung personenbezogener Daten, <http://www.dataprotection.ro/>
- **Slowakei:** Amt für den Schutz personenbezogener Daten der Slowakischen Republik, <http://www.dataprotection.gov.sk/>
- **Slowenien:** Datenschutzbeauftragter der Republik Slowenien, <https://www.ip-rs.si/>
- **Spanien:** Agencia Española de Protección de Datos (AEPD), <https://www.aepd.es/>

- **Schweden:** Integritetsskyddsmyndigheten, <http://www.imy.se/>

Gültig ab: Juni 2026