

Protection des données - Information

Informations relatives à la protection des données pour le signalement et l'enquête en matière de violations de conformité

I. Responsable et finalité du traitement des données à caractère personnel

Nous, BSH Hausgeräte GmbH, Carl-Wery-Strasse 34, 81739 Munich, Allemagne (« **BSH HQ** » ou « **nous** »), ainsi que les entités BSH au sein de l'Union européenne, en Norvège, en Suisse et au Royaume-Uni (ci-après « **entité BSH** »), sommes les prestataires des services décrits dans le présent document, ce qui inclut le traitement correspondant des données à caractère personnel.

Aux fins de la gestion et de l'enquête sur les allégations de violations de la conformité (« Gestion des allégations et enquêtes de conformité »), nous et l'entité BSH concernée agissons en tant que responsables conjoints du traitement (voir art. 26 du RGPD), car nous déterminons conjointement les finalités et les moyens du traitement de vos données à caractère personnel.

Nous et l'Entité BSH proposons différents canaux de signalement pour soumettre des rapports concernant d'éventuels cas de non-conformité, tant au niveau du groupe que local :

- Le système d'alerte « Trust and Tell » (TnT)
- L'avocat de confiance (LoT)
- Le responsable local de la conformité (LCO), situé au siège social de BSH ou au sein de l'entité BSH concernée.

Les présentes informations sur la protection des données vous informent (ci-après « vous ») sur les traitements pertinents de données à caractère personnel dans le cadre de la gestion des allégations et des enquêtes de conformité.

II. Nos principes en matière de protection des données

Dans le cadre de la fourniture des services décrits dans la présente note et de l'exploitation de sites web ainsi que d'autres points de contact, nous traitons vos données à caractère personnel de différentes manières. Nous vous informons de chaque traitement de données à caractère personnel ainsi que de la base juridique et des principes respectifs sur lesquels ce traitement repose.

Nous nous engageons à protéger vos données à caractère personnel. Par conséquent, nous traitons vos données avec le plus grand soin et dans le strict respect des lois applicables en matière de protection des données et des autorisations individuelles que vous nous avez éventuellement accordées. Nous avons mis en place des mesures de sécurité organisationnelles et techniques pour protéger l'ensemble de nos sites web, applications et autres points de contact (numériques) contre les risques potentiels liés au traitement des données à caractère personnel. Les sociétés de notre groupe et nos partenaires qui nous assistent dans la fourniture des services doivent également se conformer à ces règles et principes.

Veuillez utiliser les coordonnées fournies dans la présente note d'information sur la protection des données pour nous contacter, que ce soit de manière générale ou pour toute question et/ou demande spécifique relative à la protection des données. Les lois régissant la protection des données varient en fonction du pays dans lequel vous vous trouvez. Sur la base des principes du Règlement général sur la protection des données de l'Union européenne, à savoir le RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« RGPD »), nous avons défini les principes fondamentaux suivants comme lignes directrices régissant la manière dont nous traitons et protégeons vos données à caractère personnel lorsque nous mettons à disposition nos sites web et nos services :

1. Légalité

Nous n'utilisons des données à caractère personnel que si cette utilisation est licite, ce qui, dans le cas de la gestion des allégations et de l'enquête sur les violations de conformité signalées, repose sur les bases juridiques suivantes :

- **Art. 6, al. 1, let. c) du RGPD** : en Europe, la mise en place d'un système de gestion des signalements est une obligation légale découlant de la directive européenne sur les lanceurs d'alerte (règlement (UE) 2019/1937) et des lois nationales de transposition relatives à la protection des lanceurs d'alerte. La directive autorise le traitement des données à caractère personnel nécessaire au traitement d'un signalement conformément à la législation.
- **Art. 6, al. 1, let. f) du RGPD** : Le traitement des données à caractère personnel dans le système BKMS® repose sur les intérêts légitimes de notre entreprise à détecter et prévenir les comportements répréhensibles et ainsi éviter tout préjudice à BSH, à ses employés et à ses clients, **ainsi qu'à poursuivre les infractions pénales, faire valoir des droits civils et prévenir les infractions réglementaires.**

Pour tous les traitements de données à caractère personnel que nous décrivons ici, nous indiquons également la base juridique du traitement dans la description de la relation spécifique de responsable conjoint du traitement entre nous et l'entité BSH concernée, à la section IV de la présente note d'information sur la protection des données.

2. Équité et transparence

Nous vous informons de manière équitable et transparente, dans la présente note d'information, des données à caractère personnel que nous collectons et des raisons pour lesquelles nous les collectons. Vous pouvez accéder à la note d'information sur la protection des données directement ou via un lien lors

de votre inscription et/ou lors de toute interaction avec nous. Les utilisateurs âgés de moins de 16 ans ne doivent nous transmettre des données à caractère personnel qu'avec le consentement de leurs parents ou de leur tuteur légal. La législation en matière de protection des données applicable dans votre pays peut prévoir des limites d'âge différentes à cet égard.

3. Limitation de la finalité et minimisation des données

Nous collectons et utilisons uniquement les données à caractère personnel dont nous avons réellement besoin et aux fins pour lesquelles vous nous les avez fournies. Si nous pouvons atteindre l'objectif avec moins de données à caractère personnel, nous n'utiliserons que le minimum de données requis. Néanmoins, vous êtes libre à tout moment de fournir des données à caractère personnel supplémentaires, si cela permet d'améliorer votre expérience avec les services fournis.

4. Types de traitement, y compris par des tiers

Dans les cas où nous ne traitons pas vos données à caractère personnel directement en tant que responsable du traitement (par exemple, hébergement de sites web, services techniques, etc.), nous passons des contrats avec des tiers qui fournissent ces services en notre nom en tant que sous-traitants. Ces contrats les engagent à respecter la légalité et la sécurité du traitement de vos données à caractère personnel. Cette relation est appelée « relation entre le responsable du traitement et le sous-traitant » et est définie aux articles 28 et 29 du RGPD ; dans cette relation, nous sommes le responsable du traitement et le tiers concerné est le sous-traitant. Vous trouverez une liste des sous-traitants auxquels nous faisons appel à la fin de la présente note d'information.

Le « responsable conjoint du traitement » décrit la situation dans laquelle plusieurs parties, y compris nous, collaborent pour décider de la manière dont les données seront utilisées et gérées (responsables conjoints du traitement, voir l'article 26 du RGPD). Les responsables conjoints du traitement doivent indiquer clairement qui traite quelles données à caractère personnel et quelles obligations chaque partie a assumées en ce qui concerne les règles applicables en matière de protection des données. À mesure que les responsables conjoints s'accordent sur leurs rôles et veillent à ce que les personnes concernées (les personnes sur lesquelles portent les données) soient informées de ces rôles, nous vous informons de ces rôles et de vos droits individuels pour chacune des situations de responsabilité conjointe décrites dans la présente note. Lorsque nous faisons appel à un service tiers ou à un partenaire qui traite des données à caractère personnel en tant que responsable conjoint du traitement, nous vous informons des droits et rôles correspondants dans la liste des prestataires tiers figurant à la section IV, à la toute fin du présent document.

5. Sécurité

Nous traitons vos données de manière à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre tout traitement non autorisé ou illicite et contre toute perte, destruction ou détérioration accidentelle, en recourant à des mesures techniques ou organisationnelles appropriées. Lorsque nous faisons appel à des tiers pour traiter des données à caractère personnel, nous exigeons de ces tiers qu'ils respectent un niveau approprié de mesures techniques ou organisationnelles.

6. Droits des utilisateurs

Vous disposez des droits suivants à notre égard, auxquels nous nous conformons de manière rapide et adéquate dès réception de votre demande, comme indiqué ci-dessous :

- **Votre droit d'accéder à vos données à caractère personnel conformément à l'article 15 du RGPD** : nous vous indiquons si nous détenons des données à caractère personnel vous concernant et, le cas échéant, nous vous donnons accès à ces données et vous fournissons des informations à leur sujet.
- **Votre droit de demander la rectification de vos données conformément à l'article 16 du RGPD** : nous corrigeons les informations inexactes ou complétons les données à caractère personnel incomplètes, à condition que ces données soient nécessaires à la finalité prévue du traitement de vos données.
- **Votre droit de demander l'effacement de vos données conformément à l'article 17 du RGPD** : nous effaçons les données à caractère personnel que nous détenons à votre sujet, sauf si ces données sont soumises à des délais de conservation ou à des droits de conservation, par exemple parce que nous devons conserver vos données pour remplir nos obligations contractuelles ou conformément à la loi.
- **Votre droit de demander la limitation du traitement de vos données conformément à l'article 18 du RGPD** : dans les cas prévus à l'article 18, paragraphe 1, du RGPD, vous pouvez nous demander de bloquer vos données. Nous ne traitons les données bloquées que dans une mesure très limitée et si cela est nécessaire pour fournir les services ou remplir les obligations dont l'exécution est nécessaire après le blocage de vos données que vous avez demandé.
- **Votre droit de retirer votre consentement conformément à l'article 7, paragraphe 3, du RGPD** : pour les traitements de données nécessitant votre consentement, vous pouvez retirer votre consentement à tout moment afin d'empêcher tout traitement futur de vos données. Les traitements de données effectués sur la base de votre consentement avant son retrait restent valides et licites.
- **Votre droit d'opposition au traitement de vos données conformément à l'article 21 du RGPD** : vous pouvez vous opposer au traitement futur de vos données si nous traitons vos données sur la base de l'une des justifications légales énoncées à l'article 6, paragraphe 1, points e) ou f), du RGPD. Si vous vous opposez, nous cessons de traiter vos données, à moins que nous n'ayons des motifs légitimes et impérieux de poursuivre le traitement qui prévalent sur vos intérêts et vos droits, ou pour la constatation, l'exercice ou la défense de droits en justice. Le traitement de vos données à des fins de marketing direct ne constitue jamais pour nous un motif légitime et impérieux.
- **Votre droit à la portabilité des données conformément à l'article 20 du RGPD** : lorsque le traitement des données est effectué par des moyens automatisés et repose sur un consentement ou un contrat, nous pouvons vous fournir les données que vous nous avez communiquées dans un format structuré, couramment utilisé et lisible par machine.
- **Votre droit de saisir une autorité de contrôle** : vous pouvez introduire une réclamation relative à la protection des données auprès d'une autorité de protection des données. Pour ce faire, contactez l'autorité de protection des données compétente pour votre lieu de résidence ou l'autorité de protection des données dont nous relevons (mentionnée ci-dessous dans la liste des autorités de protection des données).

7. Principes de suppression

En principe, nous conservons vos données aussi longtemps que nécessaire pour enquêter sur l'incident de conformité auquel se rapporte votre signalement. Une fois l'enquête terminée et le délai de conservation applicable écoulé, nous supprimons vos données à caractère personnel, à l'exception des données dont la conservation est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice. La suppression de ces données est régie par les délais de prescription légaux maximaux prévus par les lois applicables.

8. Délégué à la protection des données

Si vous avez des questions concernant la protection des données ou si vous souhaitez exercer vos droits, notre délégué à la protection des données (DPO) est là pour vous aider. Vous pouvez facilement contacter notre DPO directement en envoyant un courrier ou un e-mail à l'aide des coordonnées fournies ci-dessous :

- **Si vous résidez dans un État membre de l'UE/EEE, veuillez contacter :**
BSH Hausgeräte GmbH, Délégué à la protection des données, Carl-Wery-Str. 34, 81739 Munich, Allemagne, Data-Protection-DE@bshg.com
- **Si vous résidez au Royaume-Uni, veuillez contacter :**
BSH Home Appliances Limited, Délégué à la protection des données, Grand Union House, Old Wolverton Road, Wolverton, Milton Keynes, MK12 5PT, Data-Protection-UK@bshg.com
- **Si vous résidez en Suisse, veuillez contacter :**
BSH Hausgeräte AG, représentant de Home Connect GmbH, BSH Hausgeräte AG, Fahrweidstrasse 80, CH-8954 Geroldswil, Data-Protection-CH@bshg.com

9. Modifications apportées à la présente politique de confidentialité

La présente politique de confidentialité reflète l'état actuel du traitement des données sur notre site web et nos autres points d'interaction. En cas de modifications apportées au traitement des données, la présente politique de confidentialité sera mise à jour en conséquence. Nous mettons toujours à disposition la dernière version de la présente politique de confidentialité sur notre site web afin que vous puissiez être informé de l'étendue du traitement des données via ce site web.

III. Gestion des allégations et enquêtes de conformité

1. Traitement des données

a. Gestion des allégations et enquêtes de conformité

La partie recevant les signalements (« **partie destinataire** ») peut être soit nous, soit l'entité BSH concernée. Elle est chargée de la réception initiale et de la documentation des signalements, de garantir la confidentialité et de veiller à ce qu'un accusé de réception soit envoyé au lanceur d'alerte dans la mesure du possible, ainsi que de déterminer le responsable du dossier et l'opportunité de mener une enquête tout en préservant les droits des lanceurs d'alerte et des personnes mises en cause. La partie menant les enquêtes (« **partie enquêtante** ») peut être soit nous, soit l'entité BSH concernée, et est chargée de mener des enquêtes approfondies, y compris le traitement ou la mise en œuvre de mesures de suivi, la documentation appropriée et le rapport final. Les deux parties coordonnent leurs actions afin de garantir la transparence et le respect des exigences en matière de protection des données.

Dans le cadre du contrôle conjoint, les parties sont responsables du traitement des données à caractère personnel comme suit :

- **Action A (Partie réceptrice) :** cette partie gère la réception initiale des signalements, y compris la communication avec le lanceur d'alerte, la réalisation de vérifications préliminaires de plausibilité et la classification de l'objet du signalement, ainsi que la documentation du dossier en vue de son transfert.
- **Action B (Partie chargée de l'enquête) :** cette partie mène l'enquête approfondie sur les fautes présumées, y compris les vérifications complémentaires et la documentation de toutes les données et conclusions de l'enquête.

b. Pilotage, documentation finale et analyse

Dans le cadre de la responsabilité conjointe, les parties sont responsables du traitement des données à caractère personnel pour la pilotage, la clôture et l'analyse des signalements reçus et des enquêtes de conformité menées comme suit :

- **Action C** : Nous pilotons l'ensemble du processus en fournissant des orientations sur les enquêtes et en établissant des rapports analytiques finaux à l'intention des parties prenantes internes et externes.
- **Action D** : L'entité BSH concernée est responsable de la gestion centralisée du cycle de vie de toutes les données, y compris la préparation, le stockage et la suppression des signalements et des données d'enquêtes de conformité sur les systèmes informatiques centraux.

2. Traitement confidentiel des signalements et transfert des données

Les signalements reçus sont traités par un petit cercle d'employés expressément autorisés et spécialement formés, et sont toujours traités de manière confidentielle. Dans le cadre du traitement d'un signalement, il peut s'avérer nécessaire de le transmettre aux employés responsables au siège de BSH ou à l'entité BSH concernée. Vos informations ne seront accessibles qu'aux employés qui en ont besoin pour traiter votre signalement et uniquement dans la mesure autorisée par les lois sur la protection des lanceurs d'alerte. Toutes les personnes ayant accès à votre signalement sont tenues de respecter la confidentialité. Les données peuvent également être transférées à d'autres organismes compétents (par exemple, des autorités publiques) si nous y sommes légalement tenus et dans la mesure autorisée par les lois sur la protection des lanceurs d'alerte.

3. Utilisation du système d'alerte « Trust and Tell »

a. Mise à disposition du site web.

Le service « Trust and Tell » est fourni via un site web exploité pour notre compte par un prestataire de services externe spécialisé, EQS Group GmbH. La communication entre votre ordinateur et le système BKMS® de signalement de non-conformité s'effectue via une connexion cryptée (TLS).

b. À propos du service

Le système de signalement « Trust and Tell » a pour objectif de recevoir, traiter et gérer de manière sécurisée et confidentielle les signalements concernant des violations de conformité au sein de notre entreprise et/ou de l'entité BSH concernée, ou en rapport avec celles-ci.

L'utilisation du système de signalement est facultative. Il est possible de créer une boîte aux lettres au sein du système de signalement, sécurisée par un pseudonyme / nom d'utilisateur et un mot de passe choisis individuellement. Cela vous permet d'envoyer des signalements au collaborateur responsable au sein de notre entreprise ou de l'entité BSH concernée, soit en indiquant votre nom, soit de manière anonyme et sécurisée. Ce système stocke les données uniquement au sein du système de signalement, ce qui le rend particulièrement sûr. Il ne s'agit pas d'une forme de communication par e-mail classique.

Lorsque vous soumettez un signalement ou un complément d'information, vous pouvez simultanément envoyer des pièces jointes au collaborateur responsable chez nous ou au sein de l'entité BSH concernée. Si vous souhaitez soumettre un signalement anonyme, veuillez tenir compte des conseils de sécurité suivants : les fichiers peuvent contenir des données personnelles cachées susceptibles de compromettre votre anonymat. Supprimez ces données avant l'envoi. Si

vous ne parvenez pas à supprimer ces données ou si vous ne savez pas comment procéder, copiez le texte de votre pièce jointe dans le corps de votre signalement.

c. Adresse IP, cookies, etc.

Le système de signalement n'enregistre pas les données d'adresse IP, les horodatages ou les métadonnées relatives à son utilisation par les lanceurs d'alerte.

Lors de l'utilisation du système BKMS® Incident Reporting, le serveur n'est pas en mesure d'identifier de manière unique le client (l'ordinateur de l'utilisateur). Afin de pouvoir identifier clairement le client pendant une session, l'application transmet un cookie de session à l'ordinateur de l'utilisateur. Ce cookie de session n'est utilisé que pour la connexion en cours et ne contient qu'un numéro d'identification pour la session en cours. Ce cookie est supprimé dès la fermeture du navigateur. Ce numéro de session n'a aucun lien avec le lanceur d'alerte ou les données transmises et n'est nécessaire que pour des raisons techniques.

IV. Liste des prestataires tiers et des responsables conjoints du traitement et de leur utilisation

La partie recevant les signalements peut être soit nous, soit l'entité BSH concernée ; elle est chargée de la réception initiale et de la documentation des signalements, de garantir la confidentialité et d'envoyer, dans la mesure du possible, un accusé de réception au lanceur d'alerte, ainsi que de déterminer le responsable du dossier et l'opportunité de mener une enquête tout en préservant les droits des lanceurs d'alerte et des personnes mises en cause. La partie menant les enquêtes peut être soit nous, soit l'entité BSH concernée, et est chargée de mener des enquêtes approfondies, y compris le traitement ou la mise en œuvre de mesures de suivi, la documentation appropriée et le rapport final. Les deux parties coordonnent leurs actions afin de garantir la transparence et le respect des exigences en matière de protection des données.

Dans le cadre de la responsabilité conjointe, les parties sont responsables du traitement des données à caractère personnel aux fins de la gestion des allégations et des enquêtes de conformité comme suit :

Obligations au titre du RGPD de l'UE, du RGPD britannique et de la LPD suisse) <i>La partie responsable coche la case correspondante dans le tableau sous sa responsabilité respective</i>	Champ d'action A, B, C (Siège du BSH)	Champ d'application A, B, D (Entité BSH)
Exigence d'une base légale pour le traitement conjoint (article 6 du RGPD de l'UE et du RGPD britannique, article 6 de la LPD suisse),	[x] concernant ses propres traitements	[x] concernant ses propres traitements
Fournir des informations sur le traitement conjoint des données à caractère personnel (Articles 13 et 14 du RGPD de l'UE et du RGPD britannique, article 19 de la LPD suisse)	[x] concernant ses propres traitements	[x] concernant ses propres traitements

Obligations au titre du RGPD de l'UE, du RGPD britannique et de la LPD suisse) <i>La partie responsable coche la case correspondante dans le tableau sous sa responsabilité respective</i>	Champ d'action A, B, C (Siège du BSH)	Champ d'application A, B, D (Entité BSH)
Mise à disposition de l'essentiel de la présente JCA (Article 26, paragraphe 2, du RGPD de l'UE et du RGPD du Royaume-Uni)	[x] concernant ses propres traitements	[x] concernant ses propres traitements
Droits de la personne concernée sur les données à caractère personnel conservées par les parties après le traitement conjoint (Articles 15 à 20 du RGPD de l'UE et du RGPD britannique, articles 25 à 29 de la LPD suisse)	[x] en tant que coordinateur central également pour l'entité BSH concernée	
Droit d'opposition dans la mesure où le traitement conjoint est fondé sur un intérêt légitime (Article 21 du RGPD de l'UE et du RGPD britannique)	[x] en tant que coordinateur central également pour l'entité BSH concernée	
Sécurité du traitement conjoint (Article 32 du RGPD de l'UE et du RGPD britannique, article 8 de la LPD suisse)	[x] pour les systèmes informatiques que nous gérons	[x] pour les systèmes informatiques gérés par une entité BSH
Violations de données à caractère personnel concernant le traitement conjoint (articles 33 et 34 du RGPD de l'UE et du RGPD britannique, article 24 de la LPD suisse)	[x] pour les systèmes informatiques gérés par nous	[x] pour les systèmes informatiques gérés par une entité BSH

En outre, les données à caractère personnel peuvent être transférées à ces tiers aux fins suivantes :

- Le système de signalement « Trust and Tell » est géré par un prestataire de services externe spécialisé, EQS Group GmbH, Karlstraße 47, D-80333 Munich, Allemagne, agissant en tant que sous-traitant pour le compte de BSH. Les données sont stockées dans une base de données gérée par EQS Group GmbH au sein d'un centre de données hautement sécurisé situé dans l'Union européenne. Le prestataire de services n'a pas accès aux données. Cette protection est garantie par une procédure certifiée et des mesures techniques et organisationnelles exhaustives.
- Le médiateur, Dr Karl Sidhu (cabinet d'avocats SvS), Widenmayerstr. 36, 80538 Munich, Allemagne, agit en tant qu'avocat de confiance et constitue l'un des canaux de signalement pour les lanceurs d'alerte.
- Conseiller juridique externe chargé de soutenir l'enquête et la mise en œuvre des mesures correctives.

- Transfert à Robert Bosch GmbH (notre société mère), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, pour le traitement technique des données sur des systèmes informatiques exploités pour notre compte et celui de l'entité BSH concernée.
- Transfert à Robert Bosch GmbH (notre société mère), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, pour la fourniture de services d'e-discovery (en particulier l'exploitation d'outils permettant d'examiner et d'analyser les e-mails de manière structurée) pour notre compte et celui de l'entité BSH concernée.

V. Liste des autorités de protection des données au titre du RGPD

Conformément au Règlement général sur la protection des données (RGPD), les personnes physiques ont le droit de protéger leurs données à caractère personnel et peuvent solliciter l'aide des autorités de protection des données (APD) compétentes. La liste ci-dessous a pour but de vous fournir une liste des APD au sein de la zone d'application du RGPD. Il est important de noter que les personnes concernées ont la possibilité de contacter soit l'APD de leur lieu de résidence, soit l'APD compétente pour le fournisseur du site web, en fonction de la localisation de ce dernier. Veuillez noter que cette liste n'est pas exhaustive et qu'il peut exister d'autres autorités de protection des données au sein de la zone d'application du RGPD ou, si vous ne vous trouvez pas dans cette zone, dans votre pays.

- **Autriche** : Österreichische Datenschutzbehörde, <http://www.dsb.gv.at/>
- **Belgique** : Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA), <https://www.autoriteprotectiondonnees.be> <https://www.gegevensbeschermingsautoriteit.be>
- **Bulgarie** : Commission pour la protection des données à caractère personnel, <https://www.cdpd.bg/>
- **Croatie** : Agence croate de protection des données à caractère personnel, <http://www.azop.hr/>
- **Chypre** : Commissaire à la protection des données à caractère personnel, <http://www.dataprotection.gov.cy/>
- **République tchèque** : Office pour la protection des données à caractère personnel, <http://www.uoou.cz/>
- **Danemark** : Datatilsynet, <http://www.datatilsynet.dk/>
- **Estonie** : Inspection estonienne de la protection des données (Andmekaitse Inspektsioon), <http://www.aki.ee/>
- **Finlande** : Bureau du médiateur chargé de la protection des données, <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>
- **Allemagne/Bavière** : Autorité bavaroise de protection des données (BayLDA), <http://www.baylda.de>
- **Grèce** : Autorité hellénique de protection des données, <http://www.dpa.gr/>
- **Hongrie** : Autorité nationale hongroise pour la protection des données et la liberté d'information, <http://www.naih.hu/>
- **Islande** : Persónuvernd, <https://www.personuvernd.is> , <https://www.dpa.is>
- **Irlande** : Commission de protection des données, <http://www.dataprotection.ie/>
- **Italie** : Garante per la protezione dei dati personali, <http://www.garanteprivacy.it/>
- **Lettonie** : Inspection nationale des données, <https://www.dvi.gov.lv/>
- **Liechtenstein** : Autorité chargée de la protection des données, Principauté du Liechtenstein, <https://www.datenschutzstelle.li>
- **Lituanie** : Inspection nationale de la protection des données, <https://vdai.lrv.lt/>
- **Luxembourg** : Commission nationale pour la protection des données, <http://www.cnpd.lu/>
- **Malte** : Bureau du commissaire à l'information et à la protection des données, <http://www.idpc.org.mt/>
- **Pays-Bas** : Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>
- **Norvège** : Datatilsynet, <https://www.datatilsynet.no>

- **Pologne** : Urząd Ochrony Danych Osobowych (Office de protection des données à caractère personnel), <https://uodo.gov.pl/>
- **Portugal** : Comissão Nacional de Proteção de Dados – CNPD, <http://www.cnpd.pt/>
- **Roumanie** : Autorité nationale de contrôle du traitement des données à caractère personnel, <http://www.dataprotection.ro/>
- **Slovaquie** : Office pour la protection des données à caractère personnel de la République slovaque, <http://www.dataprotection.gov.sk/>
- **Slovénie** : Commissaire à l'information de la République de Slovénie, <https://www.ip-rs.si/>
- **Espagne** : Agencia Española de Protección de Datos (AEPD), <https://www.aepd.es/>
- **Suède** : Integritetsskyddsmyndigheten, <http://www.imy.se/>

Valable à partir de : juin 2026