

Informasjon om personvern

Informasjon om personvern ved rapportering og undersøkelse av brudd på regelverket

I. Ansvarlig for og formålet med behandlingen av personopplysninger

Vi, BSH Hausgeräte GmbH, Carl-Wery-Strasse 34, 81739 München, Tyskland («**BSH HQ**» eller «**vi/oss**») og BSH-enhetene innenfor EU, Norge, Sveits og Storbritannia (heretter «**BSH-enhet**»), er leverandører av tjenestene beskrevet her, inkludert den respektive behandlingen av personopplysninger.

Med henblikk på å håndtere og undersøke påstander om brudd på regelverket («håndtering av påstander og etterforskning av regelbrudd»), fungerer vi og den respektive BSH-enheten som felles behandlingsansvarlige (se art. 26 i GDPR), da vi i fellesskap fastsetter formålene med og midlene for behandlingen av dine personopplysninger.

Vi og BSH-enheten tilbyr ulike rapporteringskanaler for å sende inn rapporter om potensielle brudd på regelverket, både på sentralt og lokalt nivå:

- Varslingssystemet «Trust and Tell» (TnT)
- Lawyer of Trust (LoT)
- Lokal compliance-ansvarlig (LCO), lokalisert ved BSHs hovedkontor eller den respektive BSH-enheten.

Denne informasjonen om personvern informerer deg (heretter «du») om den relevante behandlingen av personopplysninger innenfor rammen av håndtering av anklager og etterforskning av brudd på regelverket.

II. Våre personvernprinsipper

I forbindelse med levering av tjenestene beskrevet her og driften av nettsteder og andre kontaktpunkter behandler vi dine personopplysninger på ulike måter. Vi informerer deg om hver enkelt behandling av

personopplysninger, samt det respektive rettsgrunnlaget og prinsippene som ligger til grunn for denne behandlingen.

Vi er forpliktet til å beskytte dine personopplysninger. Derfor behandler vi opplysningene dine med stor forsiktighet og i strengt samsvar med gjeldende personvernlovgivning og de individuelle samtykkene du måtte ha gitt oss. Vi har iverksatt organisatoriske og tekniske sikkerhetstiltak for å beskytte alle våre nettsteder, apper og andre (digitale) kontaktpunkter mot potensielle risikoer knyttet til behandling av personopplysninger. Våre konsernselskaper og partnere som støtter oss i leveringen av tjenestene, må også overholde disse reglene og prinsippene.

Bruk kontaktinformasjonen som er oppgitt i denne personvernerklæringen for å kontakte oss, enten generelt eller med spesifikke spørsmål og/eller henvendelser om personvern. Det finnes ulike lover som regulerer personvern, avhengig av hvilket land du befinner deg i. Basert på prinsippene i den europeiske personvernforordningen, dvs. FORORDNING (EU) 2016/679 FRA EUROPAPARLAMENTET OG RÅDET av 27. april 2016 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger, om fri utveksling av slike opplysninger og om oppheving av direktiv 95/46/EF («GDPR»), har vi definert følgende grunnleggende prinsipper som retningslinjer for hvordan vi behandler og beskytter dine personopplysninger når vi tilbyr våre nettsteder og tjenester:

1. Lovlighet

Vi bruker kun personopplysninger dersom slik bruk er lovlig, noe som i forbindelse med håndtering av påstander og etterforskning av rapporterte brudd på regelverket er basert på følgende rettslige grunnlag:

- **Art. 6 nr. 1 bokstav c) i GDPR:** I Europa er innføringen av et varslingssystem en lovpålagt forpliktelse som følger av det europeiske varslingsdirektivet (forordning (EU) 2019/1937) og avledede nasjonale gjennomføringslover om beskyttelse av varslere. Direktivet tillater behandling av personopplysninger som er nødvendig for å håndtere en anmeldelse i samsvar med lovgivningen.
- **Art. 6 nr. 1 bokstav f) i GDPR:** Behandlingen av personopplysninger i BKMS®-systemet er basert på selskapets berettigede interesser i å oppdage og forhindre uregelmessigheter og dermed unngå skade på BSH, dets ansatte og kunder, **samt å forfølge straffbare handlinger, gjøre sivile krav gjeldende og forhindre brudd på regelverket.**

For all behandling av personopplysninger som vi beskriver her, vil vi også oppgi det rettslige grunnlaget for behandlingen i beskrivelsen av det konkrete forholdet mellom oss og den respektive BSH-enheten som felles behandlingsansvarlige i avsnitt IV i denne personvernerklæringen.

2. Rettferdighet og åpenhet

Vi vil informere deg om hvilke personopplysninger vi samler inn og hvorfor vi samler dem inn, på en rettferdig og transparent måte i denne personvernerklæringen. Du kan få tilgang til personvernerklæringen direkte eller via en lenke når du registrerer deg og/eller ved ethvert kontaktpunkt der du samhandler med oss. Brukere under 16 år bør kun overføre personopplysninger til oss med samtykke fra en forelder eller foresatt. Personvernlovgivningen som gjelder i ditt land kan medføre andre aldersgrenser i denne sammenheng.

3. Formålsbegrensning og dataminimering

Vi samler inn og bruker kun personopplysninger som vi virkelig trenger, og til det formålet du oppga personopplysningene til oss for. Hvis vi kan oppnå formålet med færre personopplysninger, vil vi kun

bruke det minste nødvendige antallet opplysninger. Du står likevel fritt til når som helst å oppgi ytterligere personopplysninger, dersom dette vil forbedre din opplevelse av de tilbudte tjenestene.

4. Typer av behandling, inkludert tredjeparter

I tilfeller der vi ikke behandler dine personopplysninger direkte som behandlingsansvarlig (f.eks. webhotell, tekniske tjenester osv.), inngår vi avtaler med tredjeparter som leverer disse tjenestene på våre vegne som databehandlere. Disse avtalene forplikter dem til å behandle dine personopplysninger på en måte som sikrer lovligheten og sikkerheten ved behandlingen. Dette kalles et forhold mellom behandlingsansvarlig og databehandler og er definert i artikkel 28 og 29 i GDPR, der vi er den behandlingsansvarlige og den respektive tredjeparten er databehandleren. Du finner en liste over databehandlerne vi benytter, på slutten av denne personvernerklæringen.

Felles databehandlingsansvar beskriver situasjonen der flere parter, hvorav vi er en av dem, samarbeider om å bestemme hvordan data skal brukes og forvaltes (felles databehandlingsansvarlige, se artikkel 26 i GDPR). Felles databehandlingsansvarlige må gi tydelig informasjon om hvem som behandler hvilke personopplysninger og hvilke forpliktelser hver part har påtatt seg med hensyn til gjeldende personvernregler. I den grad de felles behandlingsansvarlige blir enige om sine roller og sørger for at de registrerte (personene opplysningene gjelder) blir informert om disse rollene, vil vi informere deg om disse rollene og dine individuelle rettigheter for hver av situasjonene med felles behandlingsansvar som er beskrevet her. Når vi bruker en tredjepartstjeneste eller -partner som behandler personopplysninger som felles behandlingsansvarlig, vil vi informere deg om rettighetene og rollene i henhold til oversikten over tredjepartsleverandører i avsnitt IV helt på slutten av dette dokumentet.

5. Sikkerhet

Vi vil behandle opplysningene dine på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder beskyttelse mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved hjelp av egnede tekniske eller organisatoriske tiltak. Der vi bruker tredjeparter til å behandle personopplysninger, forplikter vi disse tredjepartene til å følge et passende nivå av tekniske eller organisatoriske tiltak.

6. Brukerrettigheter

Du har følgende rettigheter overfor oss, som vi etterkommer på en rettidig og tilstrekkelig måte så snart vi mottar din henvendelse, slik det er beskrevet nedenfor:

- **Din rett til å be om innsyn i dine personopplysninger i henhold til artikkel 15 i GDPR:** Vi vil informere deg om vi har personopplysninger om deg, og i så fall gi deg innsyn i og informasjon om disse opplysningene.
- **Din rett til å be om retting av dine opplysninger i henhold til artikkel 16 i GDPR:** Vi vil rette uriktige opplysninger eller komplette ufullstendige personopplysninger, forutsatt at disse opplysningene er nødvendige for det tiltenkte formålet med behandlingen av dine opplysninger.
- **Din rett til å be om sletting av dine opplysninger i henhold til artikkel 17 i GDPR:** Vi vil slette de personopplysningene vi har om deg, med mindre slike opplysninger er underlagt oppbevaringsfrister eller oppbevaringsrettigheter, for eksempel fordi vi må beholde opplysningene dine for å oppfylle våre kontraktsmessige forpliktelser eller i henhold til lovkrav.
- **Din rett til å be om begrensning av behandlingen av dine personopplysninger i henhold til artikkel 18 i GDPR:** I tilfeller som beskrevet i artikkel 18 (1) i GDPR kan du be oss om å blokkere dine personopplysninger. Vi vil kun behandle blokkerte personopplysninger i svært begrenset

omfang og dersom det er nødvendig for å yte tjenester eller oppfylle forpliktelser som må utføres etter at du har bedt om blokkering av dine personopplysninger.

- **Din rett til å trekke tilbake samtykke i henhold til artikkel 7 nr. 3 i GDPR:** For databehandlinger som krever ditt samtykke, kan du når som helst trekke tilbake samtykket ditt for å forhindre fremtidig behandling av dine opplysninger. Databehandlinger basert på ditt samtykke før tilbaketrekkingen forblir gyldige og lovlige.
- **Din rett til å gjøre innsigelse mot behandlingen av dine opplysninger i henhold til artikkel 21 i GDPR:** Du kan gjøre innsigelse mot fremtidig behandling av dine opplysninger dersom vi behandler opplysningene dine på grunnlag av en av de rettsligebegrunnelsene som er angitt i artikkel 6 nr. 1 bokstav e eller f i GDPR. Dersom du gjør innsigelse, vil vi stanse behandlingen av dine personopplysninger, med mindre vi har tvingende berettigede grunner for videre behandling som veier tyngre enn dine interesser og rettigheter, eller for å fastsette, utøve eller forsvare rettskrav. Behandlingen av dine personopplysninger for formål knyttet til direkte markedsføring utgjør aldri tvingende og berettigede grunner for oss.
- **Din rett til dataportabilitet i henhold til artikkel 20 i GDPR:** Når databehandlingen utføres automatisk og er basert på samtykke eller avtale, kan vi gi deg opplysningene du har gitt oss i et strukturert, alminnelig brukt og maskinlesbart format.
- **Din rett til å klage til en tilsynsmyndighet:** Du kan inngi en klage vedrørende personvern til en personvernmyndighet. For å gjøre dette må du kontakte den relevante personvernmyndigheten som har ansvar for ditt bosted, eller den personvernmyndigheten som har jurisdiksjon over oss (oppført nedenfor i listen over personvernmyndigheter).

7. Prinsipper for sletting

Som hovedregel lagrer vi opplysningene dine så lenge det er nødvendig for å undersøke den bruddhendelsen som din rapport gjelder. Etter at undersøkelsen er fullført og den gjeldende oppbevaringsperioden er utløpt, vil vi slette dine personopplysninger, med unntak av opplysninger som må lagres videre for å fastsette, utøve eller forsvare rettskrav. Sletting av slike opplysninger er underlagt de maksimale lovbestemte foreldelsesfristene i henhold til gjeldende lovgivning.

8. Databeskyttelsesansvarlig

Hvis du har spørsmål om personvern eller ønsker å utøve dine rettigheter, står vårt personvernombud (DPO) til rådighet for å hjelpe deg. Du kan enkelt ta kontakt med vårt personvernombud direkte ved å sende et brev eller en e-post ved hjelp av kontaklinformasjonen nedenfor:

- **Hvis du er bosatt i et EU-/EØS-medlemsland, kan du kontakte:**
BSH Hausgeräte GmbH, personvernansvarlig, Carl-Wery-Str. 34, 81739 München, Tyskland, Data-Protection-DE@bshg.com
- **Hvis du er bosatt i Storbritannia, kan du kontakte:**
BSH Home Appliances Limited, personvernansvarlig, Grand Union House, Old Wolverton Road, Wolverton, Milton Keynes, MK12 5PT, Data-Protection-UK@bshg.com
- **Hvis du er bosatt i Sveits, kan du kontakte:**
BSH Hausgeräte AG, representant for Home Connect GmbH, BSH Hausgeräte AG, Fahrweidstrasse 80, CH-8954 Geroldswil, Data-Protection-CH@bshg.com

9. Endringer i denne personvernerklæringen

Denne personvernerklæringen gjenspeiler den nåværende tilstanden for databehandlingen på vår nettside og andre kontaktpunkter. Ved endringer i databehandlingen vil denne personvernerklæringen bli oppdatert

tilsvarende. Vi legger alltid ut den nyeste versjonen av denne personvernerklæringen på vår nettside, slik at du kan holde deg informert om omfanget av databehandlingen via denne nettsiden.

III. Håndtering av påstander og etterforskning av brudd på regelverket

1. Databehandling

a. Håndtering av anklager og etterforskning av brudd på regelverket

Den som mottar varsler («**mottaker**») kan være enten oss eller den respektive BSH-enheten og er ansvarlig for den innledende mottakelsen og dokumentasjonen av varsler, for å sikre konfidensialitet og at en bekreftelse på mottakelse sendes til varsleren der det er mulig, samt for å fastslå hvem som er ansvarlig for saken og om det er hensiktsmessig å iverksette en undersøkelse, samtidig som rettighetene til varslere og de anklagede ivaretas. Den som gjennomfører undersøkelsene («**undersøkelsesparten**») kan være enten oss eller den respektive BSH-enheten, og er ansvarlig for grundige undersøkelser, herunder håndtering eller iverksettelse av oppfølgingstiltak, korrekt dokumentasjon og sluttrapportering. Begge parter skal koordinere sine tiltak for å sikre åpenhet og overholdelse av personvernkrav.

Innenfor rammen av felles kontrollansvar er partene ansvarlige for behandlingen av personopplysninger som følger:

- **Tiltak A (mottakerparten):** Denne parten håndterer den innledende mottakelsen av varslerrapporter, herunder kommunikasjon med varsleren, gjennomføring av innledende plausibilitetskontroller og klassifisering av saken, samt dokumentering av saken for overlevering.
- **Tiltak B (etterforskende part):** Denne parten gjennomfører en grundig etterforskning av sannsynlig uredlig oppførsel, herunder ytterligere kontroller og dokumentasjon av alle etterforskningsdata og funn.

b. Styring, sluttdokumentasjon og analyse

Innenfor rammen av felles kontrollansvar er partene ansvarlige for behandlingen av personopplysninger for styring, avslutning og analyse av mottatte varsler og gjennomførte etterforskninger som følger:

- **Tiltak C:** Vi styrer den overordnede prosessen ved å gi veiledning om undersøkelser og utarbeide endelige analyserapport for interne og eksterne interessenter.
- **Tiltak D:** Den respektive BSH-enheten er ansvarlig for den sentrale livssyklusforvaltningen av alle data, inkludert utarbeidelse, lagring og sletting av varslerrapporter og data fra etterlevelsesundersøkelser i sentrale IT-systemer.

2. Konfidensiell håndtering av varsler og dataoverføring

Innkommende varsler mottas av en liten krets av uttrykkelig autoriserte og spesialutdannede medarbeidere og behandles alltid konfidensielt. Som en del av behandlingen av en varsel kan det være nødvendig å videresende den til de ansvarlige medarbeiderne ved BSHs hovedkontor eller den respektive BSH-enheten. Opplysningene dine vil kun gjøres tilgjengelige for de medarbeiderne som trenger dem for å behandle varselet ditt, og kun i den utstrekning det er tillatt i henhold til lovgivningen om beskyttelse av varslere. Alle personer som får tilgang til varselet ditt, er forpliktet til å opprettholde konfidensialitet. Data kan også overføres til andre ansvarlige instanser (f.eks. offentlige myndigheter) dersom vi er lovpålagt å gjøre dette, og i den grad det er tillatt i henhold til lovgivningen om beskyttelse av varslere.

3. Bruk av varslingssystemet «Trust and Tell»

a. Tilgjengeliggjøring av nettstedet.

«Trust and Tell»-tjenesten tilbys via et nettsted som drives av en spesialisert ekstern tjenesteleverandør, EQS Group GmbH, på våre vegne. Kommunikasjonen mellom datamaskinen din og BKMS®-systemet for rapportering av brudd på regelverket skjer via en kryptert forbindelse (TLS).

b. Om tjenesten

«Trust and Tell»-rapporteringssystemet har til formål å motta, behandle og håndtere rapporter om brudd på regelverket innenfor eller knyttet til oss og/eller den respektive BSH-enheten på en sikker og konfidensiell måte.

Bruk av rapporteringssystemet skjer på frivillig basis. Det er mulig å opprette en mailboks i rapporteringssystemet som er sikret med et individuelt valgt pseudonym/brukernavn og passord. Dette gjør at du kan sende rapporter til den ansvarlige medarbeideren hos oss eller den respektive BSH-enheten, enten ved navn eller på en anonym og sikker måte. Dette systemet lagrer kun data inne i selve rapporteringssystemet, noe som gjør det særlig sikkert. Det er ikke en form for vanlig e-postkommunikasjon.

Når du sender inn en rapport eller et tillegg, kan du samtidig sende vedlegg til den ansvarlige medarbeideren hos oss eller den aktuelle BSH-enheten. Hvis du ønsker å sende inn en anonym rapport, må du ta hensyn til følgende sikkerhetsråd: Filer kan inneholde skjulte personopplysninger som kan kompromittere din anonymitet. Fjern disse opplysningene før du sender. Hvis du ikke klarer å fjerne disse opplysningene eller er usikker på hvordan du skal gjøre det, kan du kopiere teksten i vedlegget inn i rapportteksten.

c. IP-adresse, informasjonskapsler osv.

Rapporteringssystemet logger ikke IP-adressedata, tidsstempler eller metadata knyttet til bruken av systemet av varslere.

Når du bruker BKMS® Incident Reporting, kan ikke serveren entydig identifisere klienten (brukerens datamaskin). For å kunne identifisere klienten entydig under en økt, sender applikasjonen en øktcookie til brukerens datamaskin. Denne øktcookie brukes kun for den aktuelle tilkoblingen og inneholder kun et identifikasjonsnummer for den pågående økten. Denne cookien slettes når nettleseren lukkes. Dette øktnummeret har ingen tilknytning til varslere eller opplysningene som sendes inn, og er kun nødvendig av tekniske årsaker.

IV. Liste over tredjepartsleverandører og felles behandlingsansvarlige samt deres bruk

Den som mottar varsler kan være enten oss eller den respektive BSH-enheten, og er ansvarlig for den innledende mottakelsen og dokumentasjonen av varsler, for å sikre konfidensialitet og at en mottaksbekreftelse sendes til varsleren der det er mulig, samt for å fastslå den ansvarlige temaansvarlige og hensiktsmessigheten av å iverksette en undersøkelse, samtidig som rettighetene til varslere og de anklagede ivaretas. Den som gjennomfører undersøkelser kan være enten oss eller den respektive BSH-enheten, og er ansvarlig for grundige undersøkelser, herunder håndtering eller iverksettelse av oppfølgingstiltak, korrekt dokumentasjon og sluttrapportering. Begge parter vil koordinere sine tiltak for å sikre åpenhet og overholdelse av personvernkrav.

Innenfor rammen av felles kontrollansvar er partene ansvarlige for behandlingen av personopplysninger i forbindelse med håndtering av anklager og etterforskning av etterlevelse som følger:

Forpliktelser i henhold til EUs GDPR, Storbritannias GDPR og den sveitsiske FADP) <i>Den ansvarlige parten setter et kryss i tabellen under sitt respektive ansvarsområde</i>	Handlingsområde A, B, C (BSH HQ)	Handlingsområde A, B, D (BSH-enhet)
Krav om rettslig grunnlag for felles behandling (artikkel 6 i EUs GDPR og Storbritannias GDPR, artikkel 6 i sveitsiske FADP),	[x] når det gjelder egne behandlinger	[x] angående egne behandlinger
Informasjon om felles behandling av personopplysninger (Artikkel 13 og 14 i EUs og Storbritannias GDPR, artikkel 19 i det sveitsiske FADP)	[x] angående egne behandlinger	[x] angående egne behandlinger
Tilgjengeliggjøring av innholdet i denne JCA (Artikkel 26(2) i EUs GDPR og Storbritannias GDPR)	[x] angående egne behandlinger	[x] angående egne behandlinger
Den registrertes rettigheter med hensyn til personopplysningene som er lagret av partene etter den felles behandlingen (Artikkel 15–20 i EUs GDPR og Storbritannias GDPR, artikkel 25–29 i det sveitsiske FADP)	[x] som sentral koordinator også for den respektive BSH-enheten	
Rett til å gjøre innsigelse i den grad den felles behandlingen er basert på berettiget interesse (artikkel 21 i EUs GDPR og Storbritannias GDPR)	[x] som sentral koordinator også for den respektive BSH-enheten	
Sikkerhet ved felles behandling (Artikkel 32 i EUs GDPR og Storbritannias GDPR, artikkel 8 i det sveitsiske FADP)	[x] for IT-systemer som forvaltes av oss	[x] for IT-systemer som forvaltes av BSH-enheten
Brudd på personvernet knyttet til felles behandling (artikkel 33 og 34 i EUs og Storbritannias GDPR, artikkel 24 i det sveitsiske FADP)	[x] for IT-systemer som forvaltes av oss	[x] for IT-systemer som forvaltes av en BSH-enhet

I tillegg kan personopplysninger overføres til disse tredjepartene for følgende formål:

- Rapporteringssystemet «Trust and Tell» drives av en spesialisert ekstern tjenesteleverandør, EQS Group GmbH, Karlstraße 47, D-80333 München, Tyskland, som fungerer som databehandler for BSH. Dataene lagres i en database som drives av EQS Group GmbH i et datasenter med høy sikkerhet i Den europeiske unionen. Tjenesteleverandøren har ikke tilgang til dataene. Dette sikres gjennom en sertifisert prosedyre og omfattende tekniske og organisatoriske tiltak.
- Ombudsmannen Dr. Karl Sidhu (SvS Attorneys at Law), Widenmayerstr. 36, 80538 München, Tyskland, fungerer som tillitsadvokat og er en av mottakskanalene for varslere.
- Ekstern juridisk rådgiver for å støtte etterforskningen og avhjelpende tiltak.
- Overføring til Robert Bosch GmbH (vårt morselskap), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, for teknisk behandling av data på IT-systemer som drives på vegne av oss og den respektive BSH-enheten.
- Overføring til Robert Bosch GmbH (vårt morselskap), Robert-Bosch-Platz 1, D-70839 Gerlingen-Schillerhöhe, for levering av e-discovery-tjenester (spesielt drift av verktøy for å gjennomgå og analysere e-post på en strukturert måte) på vegne av oss og den respektive BSH-enheten.

V. Liste over personvernmyndigheter i henhold til GDPR

I henhold til personvernforordningen (GDPR) har enkeltpersoner rett til å beskytte sine personopplysninger og kan søke hjelp fra de relevante datatilsynsmyndighetene (DPA-er). Listen nedenfor har til hensikt å gi deg en oversikt over datatilsynsmyndigheter innenfor GDPR-området. Det er viktig å merke seg at de registrerte har muligheten til å kontakte enten datatilsynsmyndigheten i sitt bostedsland eller den datatilsynsmyndigheten som har ansvar for nettstedets leverandør, avhengig av leverandørens beliggenhet. Vær oppmerksom på at denne listen ikke er uttømmende, og at det kan finnes flere datatilsynsmyndigheter innenfor GDPR-området eller, hvis du ikke befinner deg i GDPR-området, i ditt eget land.

- **Østerrike:** Österreichische Datenschutzbehörde, <http://www.dsb.gv.at/>
- **Belgia:** 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.cdpd.bg/>
- **Kroatia:** Kroatisk personvernbyrå, <http://www.azop.hr/>
- **Kypros:** Commissioner for Personal Data Protection, <http://www.dataprotection.gov.cy/>
- **Tsjekkia:** Kontoret for personvern, <http://www.uoou.cz/>
- **Danmark:** Datatilsynet, <http://www.datatilsynet.dk/>
- **Estland:** Estlands datatilsyn (Andmekaitse Inspektsioon), <http://www.aki.ee/>
- **Finland:** Datatilsynet, <http://www.tietosuoja.fi/en/>
- **Frankrike:** Commission Nationale de l'Informatique et des Libertés – CNIL, <http://www.cnil.fr/> <https://www.cnil.fr/en/contact-cnil>
- **Tyskland/Bayern:** Bayerske datatilsynet (BayLDA), <http://www.baylda.de>
- **Hellas:** Den greske datatilsynsmyndigheten, <http://www.dpa.gr/>
- **Ungarn:** Ungarsk nasjonal myndighet for personvern og informasjonsfrihet, <http://www.naih.hu/>
- **Island:** Persónuvernd, <https://www.personuvernd.is>, <https://www.dpa.is>
- **Irland:** Datatilsynet, <http://www.dataprotection.ie/>
- **Italia:** Garante per la protezione dei dati personali, <http://www.garanteprivacy.it/>
- **Latvia:** Statens datatilsyn, <https://www.dvi.gov.lv/>
- **Liechtenstein:** Datatilsynet, Fyrstedømmet Liechtenstein, <https://www.datenschutzstelle.li>
- **Litauen:** Statens datatilsyn, <https://v dai.lrv.lt/>
- **Luxembourg:** Commission Nationale pour la Protection des Données, <http://www.cnpd.lu/>

- **Malta:** Kontoret for informasjons- og personvernkommissæren, <http://www.idpc.org.mt/>
- **Nederland:** Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>
- **Norge:** Datatilsynet, <https://www.datatilsynet.no>
- **Polen:** Urząd Ochrony Danych Osobowych (Kontoret for personvern), <https://uodo.gov.pl/>
- **Portugal:** Comissão Nacional de Proteção de Dados – CNPD, <http://www.cnpd.pt/>
- **Romania:** Den nasjonale tilsynsmyndigheten for behandling av personopplysninger, <http://www.dataprotection.ro/>
- **Slovakia:** Kontoret for personvern i Den slovakiske republikk, <http://www.dataprotection.gov.sk/>
- **Slovenia:** Informasjonskommissæren for Republikken Slovenia, <https://www.ip-rs.si/>
- **Spania:** Agencia Española de Protección de Datos (AEPD), <https://www.aepd.es/>
- **Sverige:** Integritetsskyddsmyndigheten, <http://www.imy.se/>

Gjelder fra: juni 2026