HSB – där möjligheterna bor

HSBS POLICY FÖR HANTERING AV PERSONUPPGIFTER (INTERN)

Version 2.0

En god regelefterlevnad är en självklarhet i HSB och hela organisationen arbetar aktivt med att ständigt förbättra den. Ett stöd för HSB i arbetet med att ha en god regelefterlevnad är HSBs ansvar som är en gemensam samling av policys som antas av HSB Riksförbunds styrelse.

Förbundsstyrelsen rekommenderar HSB-föreningarna att anta beslutade policyer och stödmaterial i respektive HSB-förening. För HSB Riksförbund och dess dotterbolag gäller policyer inom HSBs ansvar när de beslutats av Förbundsstyrelsen.

Förbundsstyrelsen har den 20 oktober 2020 beslutat att HSBs policy för hantering av personuppgifter ska ingå i HSBs ansvar. Förbundsstyrelsen har utsett funktionen för regelefterlevnad på HSB Riksförbund till dokumentägare. Som dokumentägare är funktionen för regelefterlevnad på HSB Riksförbund ansvarig för att innehållet i denna policy hålls aktuell och uppdaterad i enlighet med processen för HSBs ansvar.

Om dokumentet

Dokumentägare	Funktion för regelefterlevnad, HSB Riksförbund
Fastställd av	Styrelsen för HSB Riksförbund vid styrelsemöte den 20 oktober 2020
Informationssäkerhetsklassning	Öppet internt och konfidentiellt externt

Versionshantering

Version	Datum	Sammanfattning	Beslutad av
1.0	2020-10-20	Ny policy	Förbundsstyrelsen
1.1	2021-09-17	• Tillägg av versionshantering och text om dokumentet. • Ändring av inledande text. • Språkliga justeringar. • Förtydligande i implementerings- och uppföljningsplan. • Förtydliganden i HSBs tillvägagångssätt.	Dokumentägare
2.0	2023-10-19	• Tagit bort överflödig text och genomfört språkliga justeringar. • Flyttat avsnittet ”*Implementeringsplan och Uppföljningsplan*” till Bilaga 1. • Inledning uppdaterad i förhållande till processen för HSBs ansvar. • Nytt avsnitt om ”*Gällande regelverk*” införts.	Förbundsstyrelsen

		• Förtydliganden och nya definitioner tillkommit under avsnitt ”*Vanliga begrepp*”. • Förtydliganden i avsnitt om ”*HSBs grundläggande principer vid hantering av personuppgifter*”. • Förtydliganden i avsnitt om ”*HSBs tillvägagångssätt för hantering av personuppgifter*”, där nya avsnitt om ”*Användning av personuppgiftsbiträden*”, ”*Hantering av inträffad personuppgiftsincident*” och ”*Uppföljning*” har tillkommit. • Ett omarbetat avsnitt med en ny rubrik ”*Styrning och stöddokument*”. • En del av avsnitt ”*Inventering*” har flyttats till Bilaga 2, där har en ny punkt också tillkommit.	

Gällande regelverk

Vid upprättandet av denna policy har hänsyn tagits till följande regler:

- Förordning: EU:s Dataskyddsförordning (2016/679).

Vanliga begrepp

Personuppgifter

All slags information som antingen direkt eller indirekt (det vill säga via annan information) kan kopplas till en fysisk levande person – en registrerad – såsom namn, lägenhetsnummer, IP-adress, fotografier, ljudupptagningar, beteenden, preferenser, uppgifter om störningar, löneuppgifter och uppgifter om utbildning.

Registrerad

Den registrerade är den person vars personuppgifter samlas in, innehas eller behandlas av den personuppgiftsansvarige. Om den personuppgiftsansvarige inte själv behandlar personuppgifter utförs behandlingen av ett personuppgiftsbiträde för dennes räkning.

Kategorier av registrerade

De individer som HSB behandlar personuppgifter om kan till exempel vara anställda, inhyrda konsulter, hyresgäster och bostadsrättshavare som är fysiska personer eller enskilda firmor, kontaktpersoner hos hyresgäster som är företag, anställda hos förvaltare, byggbolag, leverantörer och samarbetspartners.

Personuppgiftsbehandling

Är en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning,

läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Personuppgiftsansvarig (PUA)
Den som bestämmer ändamålen och medlen för en personuppgiftsbehandling och därmed är ansvarig för att behandlingen sker i enlighet med gällande rätt. Det är ofta ett företag eller en organisation, inte en fysisk person, som avses.

Det kan inom en organisation eller inom ramen för ett samarbete finnas flera personuppgiftsansvariga och dessa kan även ha ett delat personuppgiftsansvar.

Personuppgiftsbiträde (PUB)
Ett företag eller organisation som behandlar personuppgifter på uppdrag av den personuppgiftsansvarige och för dennes räkning. Ett exempel på detta är när HSB behandlar personuppgifter åt bostadsrättsföreningarna inom den tekniska och administrativa förvaltningen. Om personuppgiftsbiträdet utför någon behandling för egna ändamål är leverantören personuppgiftsansvarig för sådan behandling.

Känsliga personuppgifter (så kallade särskilda kategorier av personuppgifter)
Personuppgifter som till exempel avslöjar etniskt ursprung, medlemskap i fackförening, sexuell läggning, sexualliv, genetiska uppgifter, religiös eller filosofisk övertygelse, hälsa, biometriska uppgifter som används för att entydigt identifiera en person eller uppgifter om hälsa är att betrakta som känsliga personuppgifter.

En uppgift om att någon behöver ett anpassat boende pga. funktionshinder är ett exempel på en känslig personuppgift.

Extra skyddsvärda personuppgifter
Extra skyddsvärda personuppgifter är sådana uppgifter som i regel är mer integritetskänsliga än andra och som ofta kräver en högre nivå av säkerhet. Exempel:

- löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala förhållanden

Personuppgiftsincident
En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

HANTERING AV PERSONUPPGIFTER INOM HSB

Denna policy har som syfte att inom HSB skapa en gemensam grund och ett gemensamt arbetssätt för att hantera personuppgifter. Ett gemensamt arbetssätt är en förutsättning för att HSBs gemensamma nationella organisation ska kunna erbjuda ett effektivt stöd. Denna policy beskriver därför hur HSB internt samverkar kring hantering av personuppgifter.

HSBs grundläggande principer vid hantering av personuppgifter

- HSB följer innehållet i för var tid gällande personuppgiftslagstiftning.

- HSB ska upprätthålla en god personuppgiftshantering. Detta innebär att HSB vid tolkning och tillämpning av för var tid gällande personuppgiftslagstiftning ska ta hänsyn till de kooperativa principerna och HSBs kärnvärderingar ETHOS samt att åtgärder står i proportion till ändamål och risker för människors fri och rättigheter.
- HSB behandlar endast personuppgifter om det finns laglig grund.
- HSB behandlar personuppgifter på ett rättvist och korrekt sätt.
- HSBs personuppgiftsbehandling är transparent och öppen.
- HSB behandlar endast personuppgifter utifrån de särskilda och uttryckligt angivna ändamålen.
- HSB behandlar endast personuppgifter som är adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.
- HSB lagrar endast personuppgifter så länge det är nödvändigt för att uppfylla det ändamål för vilka de samlades in.
- De personuppgifter som HSB behandlar är korrekta och uppdaterade.
- HSB vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda insamlade personuppgifter.
- HSB tillmötesgår de registrerades rättigheter.
- HSB beaktar ovan angivna grundläggande principer vid utveckling av nya produkter och tjänster. Vilket innebär att HSB tar hänsyn till integritetsskyddsreglerna när man anskaffar/utformar verksamhet och rutiner samt säkerställer att behandling av personuppgifterna inte sker i onödig omfattning.
- HSB i egenskap av personuppgiftsansvarig måste påvisa efterlevnaden av de grundläggande principerna i dataskyddsförordningen. HSB dokumenterar sitt arbete med att säkerställa en god personuppgiftshantering och har upprättat en förteckning över all personuppgiftsbehandling inom organisationens verksamhet.

HSBs tillvägagångssätt för hantering av personuppgifter

1. Utse en dataskyddsansvarig

Dataskyddsansvarig är en person eller funktion som har det övergripande operativa samordnings- och uppföljningsansvaret för hantering av personuppgifter inom HSB-föreningen/bolaget.

Varje HSB-förening/bolag bör utse en dataskyddsansvarig. Utses ingen dataskyddsansvarig anses vd inom HSB-föreningen/bolaget vara dataskyddsansvarig. Att man utser en dataskyddsansvarig fråntar inte vd/styrelsen dess ansvar som personuppgiftsansvarig.

2. Styrning och interna regelverk

Varje HSB-förening/bolag ska upprätta en struktur för den interna ansvarsfördelningen avseende personuppgiftshantering som sker i den egna organisationen. Det vill säga identifiera ansvaret utifrån befintliga befattningar uppifrån ledningen och ner i organisationen. Strukturen för ansvarsfördelningen ska spegla organisationens utformning. Detta för att åstadkomma en tydlig och ansvarsfull personuppgiftshantering i den egna organisationen.

Vidare ska varje HSB-förening/bolag som hanterar personuppgifter upprätta riktlinjer, instruktioner och rutiner för att beskriva vad organisationen gör för att uppnå HSBs grundläggande principer för hantering av personuppgifter. Utgångspunkt vid framtagande av riktlinjer, rutiner och instruktioner är respektive HSB-förening/bolagsverksamhet.

3. Struktur och inventering

Dataskyddsanasvarig ska tillsammans med verksamheten identifiera all personuppgifts-behandling som sker och dokumentera detta i ett register.

Varje HSB-förening/bolag som hanterar eller avser att hantera personuppgifter ska inventera vilka personuppgifter som behandlas. Inventeringen ska uppdateras löpande, dock med ett lägsta intervall om två år. Vid inventering ska information dokumenteras enligt bilaga 2.

4. Utbildning

Alla medarbetare och konsulter inom HSB ska få information och utbildning om hur HSB arbetar för att säkra en god personuppgiftshantering. Utbildning bör vara relevant för den särskilda kategorin anställda. Till exempel behöver anställda på kund- och medlemservice information om interna rutiner medan styrelseledamöter snarare behöver övergripande information om regelverkets risker.

Varje HSB-förening/bolag ansvarar för att utbildning sker i lämplig omfattning.

5. Användning av personuppgiftsbiträden

HSB ska endast använda personuppgiftsbiträden som ger tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna policy och andra interna regler samt säkerställer skyddet av de registrerades rättigheter enligt dataskyddsförordningen.

Ett personuppgiftsbiträdesavtal och instruktion för aktuell behandling måste upprättas med externa personuppgiftsbiträden.

6. Hantering av inträffad personuppgiftsincident

Om en personuppgiftsincident skulle inträffa ska:

HSB (som personuppgiftsansvarig) utan onödigt dröjsmål dock senast inom 72 timmar efter att det inträffade upptäckts, anmäla incidenten till Integritetsskyddsmyndigheten (IMY), i de fall incidenten bedöms föranleda risk för registrerade personers rättigheter och friheter. I de fall incidenten inte bedöms föranleda risk för registrerade personers rättigheter och friheter behöver ingen anmälan göras till IMY. En sådan bedömning genomförs och dokumenteras av dataskyddsansvarig.

HSB som personuppgiftsbiträde ska tillse att, utan onödig fördröjning, anmäla det inträffade till berörd personuppgiftsansvarig enligt upprättat personuppgiftsbiträdesavtal mellan HSB och aktuell personuppgiftsansvarig. HSB som underleverantör åtar sig att delta i förebyggande, felsökning och felavhjälpning av samt informationsgivning om personuppgiftsincidenter.

7. Dokumentation

Arbetet med HSBs tillvägagångssätt för hantering av personuppgifter ska dokumenteras. Dokumentationen ska redovisas på begäran inom ramen för uppföljning av HSBs ansvar.

8. Uppföljning

Varje HSB-förening/bolag som hanterar personuppgifter ska årligen medverka till HSB Riksförbunds uppföljning av efterlevnaden av denna policy.

HSB-föreningen/bolaget ska i den mån det är möjligt kontrollera och följa upp hur väl HSB-föreningen/bolaget efterlever denna policy och dataskyddsförordningen.

HSB – där möjligheterna bor

Bilaga 1

IMPLEMENTERINGS- OCH UPPFÖLJNINGSPLAN

Målgrupp

Primär: dataskyddsansvariga, dataskyddsombud, regelefterlevnadsansvariga och/eller verkställande direktörer inom HSB-föreningar och bolag.

Sekundär: anställda, förtroendevalda och konsulter inom HSB-föreningar och bolag.

Implementeringsplan

Denna policy ska implementeras hos den primära målgruppen genom att:

- HSB Riksförbund håller denna policy tillgänglig på HSBs gemensamma intranät
- HSB Riksförbund kommunicerar innehållet i denna policy till den primära målgruppen via e-postutskick.
- HSB Riksförbund ska kommunicera innehållet i denna policy till den primära målgruppen i samband med den årliga genomgången av nya, ändrade och befintliga policyer som hålls i T3 varje år.
- HSB-förening/bolag utser en dataskyddsansvarig.

Denna policy ska implementeras hos den sekundära målgruppen genom att:

- HSB Riksförbund tillhandahåller en grundläggande utbildning i dataskyddsförordningen.

Uppföljning

HSB Riksförbund ska inom ramen för den årliga verksamhetsuppföljningen kontrollera anslutningsgrad, riskområdestäckningsgrad, implementeringsgrad och uppföljningsgrad genom att ställa följande frågor till HSB-föreningar och bolag:

Kategori	Mål	Fråga	Svarsalt.	Poäng
Anslutningsgrad/risk-områdestäckningsgrad	1	Har HSB-föreningen/bolaget antagit HSBs policy för hanterings av personuppgifter?	Ja/nej	Ja=1 p
Anslutningsgrad/risk-områdestäckningsgrad	1	Om nej, har HSB-föreningen/bolaget antagit en liknande policy som täcker samma riskområde?	Ja/nej	Ja=1p
Implementeringsgrad	4	Har 80 % av HSB-föreningen/bolagets medarbetare genomfört HSBs gemensamma grundutbildning i GDPR?	Ja/nej	Ja=2 p
Implementeringsgrad	4	Har HSB-föreningen/bolaget utsett en dataskyddsansvarig?	Ja/nej	Ja=1p
Implementeringsgrad	4	Har HSB-föreningen/bolaget antagit riktlinjer, rutiner, instruktioner eller andra styrande dokument för att säkerställa implementering av denna policy?	Ja/nej	Ja=1 p
Implementeringsgrad	4	Har HSB-föreningen vidtagit annan åtgärd för att säkerställa implementering av denna policy?	Ja/nej	Ja=1p
Uppföljningsgrad	4	Har HSB-föreningen/bolaget antagit rutiner för att följa upp efterlevnaden av GDPR?	Ja/nej	Ja=1p

Uppföljningsgrad	4	Har det inträffat fler än två personuppgiftsincidenter i HSB-föreningen/bolaget under det senaste året?	Ja/nej	Ja=1p
Uppföljningsgrad	4	Genomför HSB-föreningen/bolaget stickprovskontroller av efterlevnaden av GDPR?	Ja/nej	Ja=1p
Uppföljningsgrad	4	Genomför HSB-föreningen/bolaget någon form av periodiserad uppföljning av efterlevnaden av GDPR utöver den som sker inom ramen för HSB Riksförbunds verksamhetsuppföljning?	Ja/nej	Ja=1p
Uppföljningsgrad	4	Genomför HSB-föreningen/bolaget någon annan typ av uppföljning?	Ja/nej	Ja=1p

Bilaga 2

Inventering av befintliga personuppgiftsbehandlingar och identifiering av nya personuppgiftsbehandling i HSBs registerförteckning

Varje HSB-förening/bolag som hanterar eller avser att hantera personuppgifter ska inventera vilka personuppgifter som behandlas. Inventeringen ska uppdateras löpande, dock med ett lägsta intervall om två år.

Vid inventering bör det för varje kategori av personuppgift beaktas:

- Typ av personuppgift
- Kategori av behandling
- Intern ägare
- Intressenter inom organisationen
- Syfte och ändamål med behandling
- Kategori av registrerade
- Kategori av personuppgifter
- Kategori av mottagare
- Rättslig grund
- Allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna
- Applikation där lagring sker
- Lagringstid
- Beskrivning av överföring till tredje land
- Namn på personuppgiftsbiträde som anlitats för behandlingen
- Förekomst av samtycke
- Beskrivning av hur den registrerade informeras om behandlingen
- Beskrivning om behandlingen kräver utförande av analyser såsom konsekvensbedömning (PIA/DPIA), TIA (Transfer Impact Assessment) eller annat.