Personuppgiftsbiträdesavtal för Securitas kunder

PARTER

Detta personuppgiftsbiträdesavtal ("**PUB-avtal**") har träffats mellan:

1. Securitas Sverige AB, org. nr. 556108-6082, Box 12516, 102 29 Stockholm ("**Securitas**"), och

2. _____ , org. nr. _____ , _____ (nedan "**Kund**"),
Företagsnamn *org. nr.* *Adress*

var och en "**Part**" och gemensamt "**Parterna**". Securitas är personuppgiftsbiträde och Kunden personuppgiftsansvarig.

DET/DE AVTAL MELLAN SECURITAS OCH KUND SOM REGLERAR TJÄNSTERNA OCH OMFATTAS AV DETTA PUB-AVTAL (”HUVUDAVTALET”)

Samtliga avtalsnamn inkl. avtalsnr/datum:

KUNDENS KONTAKTPERSON OCH KONTAKTUPPGIFTER

Namn & titel:
E-post, telefonnr & övrig kontaktinformation:

SECURITAS KONTAKTPERSON OCH KONTAKTUPPGIFTER

Namn & titel:
E-post, telefonnr & övrig kontaktinformation:

För meddelande till Securitas enl. Bilaga Särskilda avtalsvillkor för PUB-avtal p. 3 Dokumentation och efterlevnad, p. 6 Stöd till den personuppgiftsansvarige och p. 7 Anmälan om personuppgiftsincidenter i, ska utöver kontaktperson även kopia (cc) skickas till bitradesavtal@securitas.se

INGÅENDE DOKUMENT

Detta PUB-avtal består av följande avtalsdokument:

1. Detta dokument Personuppgiftsbiträdesavtal för Securitas kunder, som fyller ut Bilaga I till Standardavtalsklausulerna;
2. Instruktioner för behandling av personuppgifter, som utgör Bilaga II till Standardavtalsklausulerna;
3. Åtgärder för informationssäkerhet och dataskydd, som utgör Bilaga III till Standardavtalsklausulerna;
4. Särskilda avtalsvillkor för PUB-avtal; och
5. EU-kommissionens standardavtalsklausuler enligt EU-kommissionens genomförandebeslut (EU) 2021/915 av den 4 juni 2021 om standardavtalsklausuler mellan personuppgiftsansvariga och personuppgiftsbiträden enligt artikel 28.7 i GDPR, ("**Standardavtalsklausulerna**"), som finns tillgängliga i EUR-lex https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A32021D0915&locale-en.

Avseende Bilaga IV till Standardavtalsklausulerna, hänvisas till listan under punkten Underbiträden i Instruktioner för behandling av personuppgifter i detta PUB-avtal. Om innehållet är motstridiga ska dokumenten tolkas enligt företrädesordningen angiven ovan, med högsta prioritet till den första punkten.

DEFINITIONER

Följande definierade begrepp används i detta PUB-avtal, som ska äga företräde framför eventuella motsvarande definitioner i Huvudavtalet. I övrigt gäller klausul 3 i Standardavtalsklausulerna.

Definition	***Betydelse***
"**GDPR**"	betyder Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning);
"**Instruktion**"	betyder dokumenterade instruktioner som Kunden lämnar som anger föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade och eventuella särskilda krav som gäller för behandlingen, inklusive Instruktioner för behandling av personuppgifter i detta PUB-avtal;
"**Tillämplig dataskyddslagstiftning**"	betyder GDPR och all gällande dataskyddslagstiftning och förordningar, inklusive föreskrifter från berörda tillsynsmyndigheter, avseende skydd för fysiska personers grundläggande rättigheter och friheter vid behandling av deras personuppgifter som gäller för Parterna.

INLEDNING

Securitas kommer i samband med tillhandahållande av tjänsterna enligt Huvudavtalet ("**Tjänsterna**") att behandla personuppgifter som ett personuppgiftsbiträde på uppdrag av Kunden. För sådan behandling av personuppgifter gäller bestämmelserna i detta PUB-avtal. PUB-avtalet utgör en integrerad del av Huvudavtalet.

Syftet med PUB-avtalet är att säkerställa att det finns tillräckliga garantier för skydd av personuppgifter i enlighet med artikel 28 i GDPR när Securitas behandlar personuppgifter på uppdrag av Kunden i samband med tillhandahållande av tjänsterna enligt Huvudavtalet.

Vid konflikt mellan en bestämmelse i detta PUB-avtal och en bestämmelse i Huvudavtalet gäller bestämmelsen i detta PUB-avtal.

Securitas äger inte rätt till någon särskild ersättning för att uppfylla sina åtaganden som personuppgiftsbiträde enligt detta PUB-avtal om inte annat följer av detta PUB-avtal.

Detta PUB-avtal ersätter mellan Parterna tidigare ingångna PUB-avtal som avser behandling av personuppgifter som omfattas av detta PUB-avtal, dock med undantag för eventuella i förhållande till Instruktioner för behandling av personuppgifter kompletterande eller särskilda Instruktioner som omfattas av sådant tidigare ingånget PUB-avtal, vilka också ska anses utgöra ytterligare Instruktioner för behandling av personuppgifter enligt detta PUB-avtal.

* * * * * *

Detta PUB-avtal har upprättats i två exemplar av vilka vardera Parten tagit var sitt. Parterna är överens om att såväl elektroniska signaturer som egenhändigt undertecknade signaturer som har skannats in och konverterats till en bild (såsom PDF eller JPG) är giltiga och bindande.

SECURITAS SVERIGE AB	**KUND**
Ort och datum:	*Ort och datum:*
Undertecknande:	*Undertecknande:*
Namn och titel:	*Namn och titel:*

SÄRSKILDA AVTALSVILLKOR FÖR PUB-AVTAL

PARTERNAS SKYLDIGHETER

1. Dockningsklausul

Parterna är överens om att dockningsklausulen i klausul 5 i Standardavtalsklausulerna inte ska gälla mellan Parterna. Om således en part vill tillträda PUB-avtalet krävs båda Parters på förhand lämnade samtycke, samt att ett tilläggsavtal till detta PUB-avtal ingås mellan berörda parter.

2. Instruktioner

Kundens eventuella ytterligare Instruktioner för behandling av personuppgifter ska lämnas till Securitas genom möte mellan Parterna om inget annat överenskommits, samt även per e-post till Securitas kontaktperson.

Om Securitas saknar Instruktion för hur personuppgifter som omfattas av detta PUB-avtal får behandlas eller om Securitas anser att en Instruktion strider mot Tillämplig dataskyddslagstiftning ska Securitas underrätta Kunden om detta skriftligen till Kundens till Kundens kontaktperson och invänta Kundens Instruktion

Om Kunden lämnar ytterligare Instruktioner som går utöver vad som följer av Tillämplig dataskyddslagstiftning eller som inte följer av Huvudavtalet ska Securitas, om Kunden vidhåller Instruktionen, ha rätt till skälig ersättning för den ytterligare kostnad som Instruktionen innebär för Securitas eller annars enligt separat överenskommelse mellan Parterna.

3. Dokumentation och efterlevnad

En begäran om granskning eller inspektion som genomförs av Kunden (eller av Kunden utsedd oberoende revisor) enligt klausul 7.6 i Standardavtalsklausulerna ska lämnas till Securitas genom e-post till Securitas kontaktperson. För undvikande av tvivel inkluderar granskning eller inspektion även skriftliga granskningsunderlag och frågeformulär. Kunden ska lämna Securitas skäligt varsel om åtminstone en (1) månad avseende en begäran om granskning eller inspektion för att ge Parterna möjlighet att planera granskningen eller inspektionen.

För att undvika missförstånd ska en granskning eller inspektion ske i den mån tillämpliga lagar och föreskrifter tillåter. En granskning eller inspektion ska ske under normal kontorstid och så långt som möjligt utan att det stör pågående verksamhet. Sådan granskning eller inspektion ska endast omfatta sådan information som är nödvändig för att Kunden ska kunna bedöma om Securitas har uppfyllt sina skyldigheter enligt PUB-avtalet och Tillämplig dataskyddslagstiftning och ska således inte omfatta någon information som saknar betydelse för Securitas behandling av personuppgifter enligt detta PUB-avtal, inklusive information hänförlig till Securitas andra kunder eller annan information. Securitas har rutiner för att hantera granskning eller inspektion enligt denna punkt 3 som Securitas följer vid en sådan begäran från Kunden. Det kan bl.a. innebära att Securitas kan komma att tillhandahålla viss känslig eller konfidentiell information på plats i Securitas lokaler, eller på annat sätt överenskommet av Parterna.

Kunden står för egna och oberoende revisors kostnader och ska ersätta Securitas för skälig kostnad som belastar Securitas för resurser som går åt för att ledsaga revisor i lokal och tillhandahålla revisorn med efterfrågat material. I övrigt står vardera Parten sin egen kostnad för genomförande av granskning eller en inspektion, om inte annat framgår av denna punkt 3. Om en granskning utvisar att Securitas har brustit i sina åtaganden enligt detta PUB-avtal eller Tillämplig dataskyddslagstiftning ska Securitas utan dröjsmål åtgärda sådan brist på egen bekostnad.

På Securitas begäran ska Kundens personal och eventuell oberoende revisor som Kund utsett och bemyndigat för att genomföra en granskning eller inspektion ingå en sekretessförbindelse med Securitas avseende den information som sådana personer får del av i samband med granskningen eller inspektionen.

Parterna är införstådda med att Securitas bedriver verksamhet av säkerhetskänslig natur, och att Securitas har rätt att erbjuda alternativ till en granskning eller inspektion enligt denna punkt 3 exempelvis genom att tillhandahålla rapport eller annan dokumentation från en granskning som Securitas eller tredje part genomfört för att kontrollera att Securitas implementerat tillräckliga tekniska och organisatoriska åtgärder för att uppfylla sina skyldigheter enligt Tillämplig dataskyddslagstiftning. Med hänsyn till Securitas särskilda verksamhet kan en oberoende revisor som Kunden utsett behöva godkännas av Länsstyrelsen innan revisorn påbörjar granskningen eller inspektionen. Kunden ansvarar för eventuell kostnad för sådant godkännande.

4. Användning av underleverantörer

Parterna är överens om att alternativ 2 i klausul 7.7 i Standardavtalsklausulerna ska tillämpas.

Securitas ska informera Kunden om eventuella ändringar till listan genom att underbiträde läggs till eller byts ut åtminstone en vecka i förväg genom e-post till Kundens kontaktperson, via prenumeration eller fakturaunderlag eller på annat sätt Securitas finner lämpligt.

Om Kunden inte invänder mot ändringen äger Securitas rätt att anlita det aktuella underbiträden för att behandla personuppgifter på uppdrag av Kunden. Om Kunden vill utöva sin rätt att invända mot ett nytt underbiträde ska Kunden skriftligen underrätta Securitas om detta inom en vecka från informationsgivning. Sådan skriftlig underrättelse ska lämnas till Securitas genom e-post till Securitas kontaktperson.

Om Kunden invänder mot anlitandet av ett underbiträde enligt ovan ska Parterna diskutera en lösning som båda Parter kan acceptera. Om Parterna inte kommer överens om en lösning inom en vecka (eller den längre period som Parterna skriftligen kommer överens om) räknat från Kundens skriftliga invändning så är Kunden införstådd att det innebär att Securitas förhindras att fullgöra sina avtalsenliga förpliktelser i den utsträckning det relaterar till underbiträdet i fråga. Åsidosättandet att fullgöra sådana förpliktelser utgör inte avtalsbrott och begränsar inte andra skyldigheter enligt Avtalet och Kunden ska fortsatt ersätta Securitas som om fullt fullgörande av Tjänsten i enlighet med Avtalet skett.

5. Internationella överföringar

Under förutsättning att Securitas iakttar bestämmelserna i klausul 7.8 i Standardavtalsklausulerna får Securitas härmed ett generellt samtycke av Kunden till att överföra personuppgifter till tredje land som är nödvändigt för Securitas att tillhandahålla Tjänsterna förutsatt att det följer Tillämplig dataskyddslagstiftning och sker i enlighet med kapitel 5 GDPR.

6. Stöd till den personuppgiftsansvarige

Information och begäran enligt klausul 8 i Standardavtalsklausulerna ska lämnas genom e-post till respektive Parts kontaktperson. Securitas äger rätt till skälig ersättning för den kostnad som biståndet till Kunden medför för Securitas eller annars enligt överenskommelse mellan Parterna.

7. Anmälan av personuppgiftsincidenter

En underrättelse till Kunden om en personuppgiftsincident som rör Kundens personuppgifter enligt klausul 9 i Standardavtalsklausulerna ska lämnas till Kunden via e-post till Kundens kontaktperson.

Kunden åtar sig att hålla affärshemligheter eller konfidentiell information som Kunden erhåller från Securitas avseende en inträffad personuppgiftsincident strikt konfidentiell. Detta ska inte förhindra Kunden från att lämna ut sådan information till berörd tillsynsmyndighet. Kunden ska dock vid tillgängliggörandet av sådan information till tillsynsmyndigheten begära att sådan information omfattas av sekretess.

SLUTBESTÄMMELSER

8. Sekretess för personuppgifter

Utan att det påverkar tillämpningen av sekretessåtaganden i Huvudavtalet ska Securitas ej hålla alla personuppgifter som omfattas av PUB-avtalet och som Securitas behandlar som personuppgiftsbiträde för Kundens räkning med mindre säkerhet än så som Securitas tillämpar för sin egen konfidentiella information.

9. Avtalstid och uppsägning

Detta PUB-avtal gäller under samma avtalstid som Huvudavtalet och för sådan ytterligare tid som Securitas (eller ett anlitat underbiträde) behandlar personuppgifter på uppdrag av Kunden.

Om någon av Parterna säger upp detta PUB-avtal med omedelbar verkan av något av de skäl som anges i klausul 10 i Standardavtalsklausulerna ska också Huvudavtalet upphöra med omedelbar verkan.

10. Upphörande av behandlingen av personuppgifter

Med hänvisning till klausul 10 (d) i Standardavtalsklausulerna ska Kunden genom e-post till Securitas kontaktperson lämna anvisning om Kunden vill att de personuppgifter som Securitas (eller underbiträde) behandlar på uppdrag av Kunden ska: (i) raderas; eller (ii) återlämnas till Kunden.

11. Bestämmelser som gäller efter avtalets upphörande

Punkten 8 (*Sekretess för personuppgifter*), punkten 10 (*Upphörande av behandlingen av personuppgifter*), punkten 12 (*Ansvar*) och punkten 13 (*Övrigt*) ska gälla efter PUB-avtalets upphörande oavsett anledning därtill.

12. Ansvar

Respektive Part ska vara ansvarig för administrativa sanktionsavgifter som har påförts Parten i fråga på grund av att Parten inte har uppfyllt sina skyldigheter enligt detta PUB-avtal eller Tillämplig dataskyddslagstiftning eller har behandlat personuppgifter i strid med Tillämplig dataskyddslagstiftning.

Vad gäller ansvar för krav på skadestånd från berörda registrerade gäller artikel 82 i GDPR. Utan att det påverkar ovanstående ska ansvarsbegränsningen i Huvudavtalet gälla.

13. Övrigt

Ändringar. För det fall ändringar i tillämplig lag, lagakraftvunnen dom som rör tolkningen av tillämplig lag eller om Tjänsterna förändras på ett sätt som kräver förändring till detta PUB-avtal ska Parterna samråda om detta och i god anda samarbeta för att göra nödvändiga ändringar till PUB-avtalet.

Hela avtalet. PUB-avtalet utgör hela avtalet mellan Parterna avseende alla frågor som PUB-avtalet berör.

Överlåtelse. Ingen av Parterna ska äga rätt att helt eller delvis överlåta sina rättigheter eller skyldigheter enligt detta PUB-avtal utan den andra Partens skriftliga samtycke.

Tillämplig lag. På detta PUB-avtal ska svensk lag tillämpas utan beaktande av bestämmelser om motstridiga regler om lagval.

Tvist. Bestämmelsen om tvistelösning i Huvudavtalet ska gälla för eventuella tvister och anspråk som uppstår till följd av eller i samband med PUB-avtalet, eller brott mot, uppsägning eller ogiltigförklaring av det.

INSTRUKTIONER FÖR BEHANDLING AV PERSONUPPGIFTER

Denna bilaga utgör en integrerad del av PUB-avtalet, och anger Kundens instruktioner för Securitas (och dess anlitade underbiträdens) behandling av personuppgifter i samband med tillhandahållandet av Tjänsterna enligt Huvudavtalet.

En separat instruktion gäller för Securitas Digitala tjänster, vilken finns tillgänglig genom följande länk: https://www.securitas.com/securitas-digital-services--legal-documents

BESKRIVNING AV BEHANDLINGEN

Securitas behandlar personuppgifter för Kundens räkning för att tillhandahålla Tjänsterna enligt Huvudavtalet och för att uppfylla sina skyldigheter enligt PUB-avtalet. Nedan beskrivs närmare den behandling av personuppgifter som Securitas utför som personuppgiftsbiträde på uppdrag av Kunden i förhållande till de tjänster som Securitas tillhandahåller. Vilken behandling av personuppgifter som Securitas utför för Kundens räkning beror på vilka tjänster som ingår i Huvudavtalet.

Bevakningstjänster

Behandlingens ändamål och art:
Personuppgifter behandlas av Securitas för Kundens räkning för att *hantera bevakningstjänst*, inklusive för att upprätthålla kontaktpersonlistor och instruktioner, genomföra behörighetskontroller, samt för att upprätta och dela kundrapporter.

Kategorier av personuppgifter:	*Kategorier av registrerade:*
• Kontaktuppgifter • Identifieringsuppgifter • Lokaliseringsuppgifter • Iakttagelser och åtgärder	• Kundens anställda och andra anlitade personer • Övriga personer som vistas behörigt eller obehörigt inom Kundens bevakningsområde

Brandskydd

Behandlingens ändamål och art:
Personuppgifter behandlas av Securitas för Kundens räkning för att *hantera brandskydd* och för att *genomföra utbildningar*, inklusive för att upprätthålla kontaktpersonlistor och instruktioner, hantera deltagarlistor för utbildningar och utbildningsresultat samt för att upprätta och dela kundrapporter.

Kategorier av personuppgifter:	*Kategorier av registrerade:*
• Kontaktuppgifter • Identifieringsuppgifter • Iakttagelser och åtgärder • Utbildningsuppgifter	• Kundens anställda och andra anlitade personer • Deltagare i utbildningar

Larmcentraltjänster, Personlarm och Fastighetsjour

Behandlingens ändamål och art:
Personuppgifter behandlas av Securitas för Kundens ändamål för att *tillhandahålla larmcentraltjänster/personlarm/fastighetsjour,* inklusive för att hantera larmmottagning, förmedla larm, upprätthålla kontaktpersonlistor och instruktioner, genomföra behörighetskontroller, samt för att upprätta och dela kundrapporter.

Kategorier av personuppgifter:	*Kategorier av registrerade:*
• Kontaktuppgifter • Identifieringsuppgifter • Lokaliseringsuppgifter • Iakttagelser och åtgärder • Teknisk användaridentifikation & användargenererad data (Alarm.com) • Bild- och ljudmaterial	• Kundens anställda och andra anlitade personer • Övriga personer som vistas behörigt eller obehörigt inom Kundens bevakningsområde, inklusive lägenhetsinnehavarare.

Parkeringstjänster

Behandlingens ändamål och art:
Personuppgifter behandlas av Securitas för att *hantera parkeringstjänster*, inklusive för att hantera parkeringstillstånd, elektroniska nycklar, utfärda och hantera kontrollavgifter eller parkeringsanmärkningar samt administrera bortförande av felparkerade fordon.

Kategorier av personuppgifter:	*Kategorier av registrerade:*
• Kontaktuppgifter • Identifieringsuppgifter • Lokaliseringsuppgifter • Parkeringsrelaterade uppgifter • Fordonsuppgifter • Bild- och ljudmaterial	• Kundens anställda och andra anlitade personer • Parkör

UNDERBITRÄDEN OCH LAGRINGSTID

För information om vilka underbiträden som Securitas anlitar för att tillhandahålla Tjänsterna samt lagringstid för personuppgifterna, se följande länk: https://www.securitas.se/om-oss/vart-integritetsarbete-gdpr/pub-avtal/. Om MySecuritas Guarding används se även https://www.securitas.se/om-oss/vart-integritetsarbete-gdpr/sub-processors-tracktik/. Information om ändringar av underbiträden kan även tillhandahållas på andra sätt som föreskrivet i punkt 4.

KATEGORIER AV PERSONUPPGIFTER

I tabellen nedan anges vilka typer av uppgifter som omfattas av respektive kategori av personuppgifter som används i denna Instruktion.

Kategori av personuppgifter	***Exempel på typer av personuppgifter***
Kontaktuppgifter	Namn, adress, e-post, telefonnummer, titel (tex säkerhetschef) och/eller befogenhet (tex nyckelansvarig).
Identifieringsuppgifter	Namn, personnummer, födelsedatum, samordningsnummer, anställningsnummer eller personlig kod. Vid iakttagelser kan åtgärden vara att göra en behörighetskontroll där det kan det föreligga behov av att identifiera och säkerställa identitet av personen på platsen. Vid Larmcentralenstjänster kan det föreligga behov av att identifiera en person via personlig kod. För parkeringstjänster kan det föreligga behov av att identifiera ägare till fordon eller nyttjande av elektroniska nycklar. För Brandtjänster finns behov av att säkerställa identitet för vissa utbildningar och diplomeringar.
Lokaliseringsuppgifter	Uppgift om plats eller position, GPS-positioner eller andra tekniska lokaliseringsuppgifter.
Iakttagelser och åtgärder	Beskrivning av iakttagelse och eventuell vidtagen åtgärd. Kan innehålla beskrivning av signalement på en person, *Fordonsuppgifter* och *Identifieringsuppgifter*.
Parkeringsrelaterade uppgifter	Parkeringstid och längd, parkeringskostnad (vid parkeringsservice), fordonsrelaterade skulder (vid fordonsflytt).
Teknisk användaridentifikation & användargenererad data	IT-relaterad information såsom IP-adress, användardata, uppgifter från cookies, navigationsuppgift på hemsida. Information för personalisering, såsom enhetsbeskrivning, lokalstorlek, systemkonfiguration, sensornamn, apparater eller andra enheter som övervakas av Alarm.com, kontoinformation, schema, läge, automationsinställningar och enhetsinställningar. Användningsdata, såsom prestanda för säkerhetsenhet som övervakas av Alarm.com, elanvändning eller förbrukning, information om värme och kyla, ljus- eller andra armaturinställningar samt användnings- och varningsloggar. Uppgifter som genereras genom användning och interaktion med Alarm.com-tjänster, såsom aktivering/avaktivering, dörröppning, på- och avslagning av ljus.
Utbildningsuppgifter	Namn, uppgift om resultat på genomförd utbildning, datum för genomförd utbildning i vissa fall *Identifieringsuppgifter*.
Fordonsuppgifter	Registreringsnummer, beskrivning av fordon, ägaruppgifter, fordonsrelaterade skulder (vid tjänsten bortförande av fordon).
Bild- och ljudmaterial	Bilder och/eller ljudupptagning där personuppgifter förekommer.

Åtgärder för informationssäkerhet och dataskydd

Inledning
Securitas Sverige AB (”Securitas”) har som mål att upprätthålla en god säkerhet för sin egen samt sina kunders information. För att uppnå detta bedrivs ett strukturerat arbete för att ständigt kunna förbättra informationssäkerheten, detta arbete utgår från ISO27000-Ledningssystem för informationssäkerhet.

Securitas Sverige AB är ett auktoriserat bevakningsföretag enligt Lag (1974:191) om bevakningsföretag, vilket innebär att företaget ska bedriva verksamhet på ett sakkunnigt och omdömesgillt sätt.

Securitas Sverige AB:s larmcentralverksamhet är certifierad enligt SSF 136, Norm avseende larmcentraler samt SSF1101, Norm avseende SSF Cybersäkerhet.

Detta dokument syftar till att beskriva de säkerhetsåtgärder som Securitas Sverige AB vidtagit för att hantera information och personuppgifter som omfattas av kundavtal på ett godtagbart sätt utifrån relevant lagstiftning samt Securitas egna riktlinjer.

Definition
I detta dokument används begreppet ”kunddata” vilket innefattar både kundinformation och personuppgifter relaterat till kundavtalet.

Organisatoriska säkerhetsåtgärder

Område	Praxis
Policyer	**Informationssäkerhetspolicy** Securitas har i ledningssystemet ett regelverk för informationssäkerhet, inkluderat en informationssäkerhetspolicy som anger målen för Securitas informationssäkerhetsarbete. Securitas övergripande mål med informationssäkerheten är: • Tillgänglighet – Information ska vara tillgänglig när behörig användare behöver den. • Riktighet – Information som hanteras ska vara tillförlitlig och endast kunna skapas och ändras av behörig personal. • Konfidentialitet – Information ska endast vara tillgänglig för den som är behörig att ta del av informationen. För att nå de övergripande målen fastställs årligen delmål med tillhörande säkerhetsåtgärder som tillsammans bidrar till den överordnade måluppfyllelsen. Uppföljning sker årligen och rapporteras i enlighet med fastslagna processer.

	Integritetspolicy Securitas integritetspolicy anger hur organisationen behandlar och skyddar personuppgifter i verksamheten och hur dataskyddsförordningens bestämmelser efterlevs. Integritetspolicyn finns publicerad på Securitas hemsida.
Organisation av informationssäkerhetsarbetet	**Ledning** Securitas ledning har det yttersta informationssäkerhetsansvaret. Det operativa och praktiska ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret. Det innebär att verksamhetsansvarig, oavsett nivå, ansvarar för informationssäkerheten inom det utpekade verksamhetsområdet. **Informationssäkerhetsansvarig** Informationssäkerhetsansvarig ansvarar för att driva det systematiska informationssäkerhetsarbetet. I detta uppdrag ingår att tillse att organisationen har interna rutiner som möjliggör uppfyllnad av informationssäkerhetsmålen. Informationssäkerhetsansvarig ska också tillse att Securitas ledning, enligt fastställd process, informeras om måluppfyllnad. **Dataskyddsombud (DPO)** Dataskyddsombudet övervakar att organisationen följer dataskyddsförordningen. **Säkerhetschef/säkerhetsskyddschef** Säkerhetschefen ansvarar för att övergripande övervaka och upprätthålla säkerheten inom Securitas, genom att tillse att tillämpliga lagar och regelverk efterlevs samt att beslutade säkerhetsåtgärder och rutiner införs och tillämpas. Säkerhetschefen är även säkerhetsskyddschef med ansvar för säkerhetsskyddet utifrån säkerhetsskyddslagen samt i relation till kunder inom säkerhetskänslig verksamhet.

Integration i verksamheten	**Informationssäkerhet i verksamheten** Säkerhet ingår som en naturlig och central del i Securitas verksamhet och omfattar såväl personalsäkerhet som IT-säkerhet och fysiskt skydd. Alla delar av verksamheten omfattas av bestämmelser om informationssäkerhet. Centrala delar specificeras ytterligare här nedan.
Klassificering och riskhantering	**Informationsvärdering** Securitas värderar kunddata för att säkerställa att informationen omfattas av lämpliga organisatoriska och tekniska säkerhetsåtgärder. **Riskbedömning** Securitas riskbedömer och genomför konsekvensbedömningar av relevanta behandlingar.
Hantering av tillgångar	**Implementering av skydd** Securitas har utsedda roller som ansvarar för informationstillgångar och att de skyddas genom tekniska och organisatoriska åtgärder. **Förteckning över tillgångar** Securitas upprätthåller en förteckning över alla informationssystem på vilka personuppgiftsdata lagras. Rutiner finns för hur informationstillgångar ska och får hanteras.
Styrning av åtkomst	**Åtkomstrutiner** Securitas har rutiner för behörighetsstyrning som säkerställer att endast de personer som behöver åtkomst till informationssystem för att kunna utföra sina arbetsuppgifter ges behörighet till dessa. Rutinerna säkerställer att begränsat antal personer har behörighet att bevilja, ändra eller avsluta behörig åtkomst till data. Teknisk supportpersonal kan endast bereda sig åtkomst till kunddata vid behov. Rutiner finns för ändring och avslut av behörigheter.
Lösenordshantering	**Lösenordspolicy** Securitas har en lösenordspolicy som omfattar samtliga konton som är knutna till registrerade användare. Policyn omfattar krav på komplexitet samt regelbundna byten av lösenord utifrån branschpraxis.

Hantering av informationssäkerhets- och personuppgiftsincidenter	**Process för informationssäkerhetsincidenter** Securitas har processer för att hantera informationssäkerhetsincidenter och informera kunder vid behov eller enligt avtal. **Process för personuppgiftsincidenter** Securitas har processer för att hantera personuppgiftsincidenter och informera personuppgiftsansvariga (kunder) utan dröjsmål.
Kontinuitet för informationssäkerhet	**Kris- och beredskapsplanering** Securitas upprätthåller kris- och beredskapsplaner för anläggningar där Securitas informationssystem som behandlar kunddata finns. **Redundans och dataåterställning** Securitas har rutiner för redundant lagring och dataåterställning. Återläsningstester genomförs.
Personalsäkerhet	**Utbildning** Securitas informerar och utbildar sin personal löpande om hur kunddata ska hanteras samt om relevanta säkerhetsförfaranden för personalens respektive roller. **Bakgrundskontroll** Securitas Sverige AB är ett auktoriserat bevakningsföretag enligt Lag (1974:191) om bevakningsföretag vilket innebär att all personal är godkänd vid prövning med avseende på laglydnad, medborgerlig pålitlighet samt lämplighet i övrigt för anställning. Med personal förstås samtliga anställda men även annan personal som deltar i bolagets verksamhet, har tillträde till bolagets lokaler eller på annat sätt kan bereda sig tillträde till kundinformation. Alla anställda som har åtkomst till kunddata och/eller har behörighet att behandla personuppgifter omfattas av tystnadsplikt i kollektivavtal samt har undertecknat sekretessavtal. Vid säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) genomgår angiven personal för uppdraget säkerhetsprövning enligt fastställda rutiner.

Tekniska säkerhetsåtgärder

Område	Praxis
Driftsäkerhet	**Skydd mot skadlig kod** Securitas har skydd mot skadlig programvara som omfattar skydd av kunddata. **Säkerhetskopiering och dataåterställning** Securitas gör regelbundet kopior av kunddata från vilka sådana data kan återställas. Lagring av kopior av kunddata och dataåterställningsrutiner sker fysiskt avskilt från den primära datorutrustningen, enligt Securitas interna regelverk. Securitas har rutiner som reglerar vem som har åtkomst till kopior av kunddata. Securitas loggar insatser för dataåterställning.
Händelseloggning	**Loggning och spårbarhet** Securitas säkerställer spårbarhet av aktiviteter i informationssystem genom loggning för att kunna identifiera och utreda incidenter och händelser.
Kryptering	**Kryptering** Securitas använder särskilda krypteringsmetoder vilka används vid behov.

Fysiska säkerhetsåtgärder

Område	Praxis
Skydd av utrustning	**Skydd av utrustning** Securitas lokaler skyddas mot obehörigt tillträde med skalskydd, larm- och passersystem, enligt fastställda säkerhetsnivåer utifrån lagkrav och branschstandard. Tillträde till lokaler registreras på individnivå och spårbarhet säkerställs genom loggar. Rutiner för styrning av tillträdesbehörigheter finns. Hantering och skydd av mobil utrustning som lämnar Securitas lokaler omfattas av internt regelverk. Rutiner finns för automatisk inaktivering av sessioner enligt ett givet tidsintervall om personal lämnar datorer utan uppsikt.
Skydd mot störningar	**Skydd mot störningar** Securitas har vidtagit åtgärder för skydd mot förlust av data på grund av elavbrott eller kommunikationsstörningar. Lokaler med informationssystem som behandlar kunddata är försedda med brandlarm.