Integritets- och datasäkerhetspolicy

Version 1.0

21-11-25

Huvudkontor

Avonova Hälsa AB
559093–0722

Klarastrandsleden 123
123 12 Stockholm

010–123 123 12

kontakt@avonova.se

Dataskyddsombud

gdpr@avonova.com

avonova

Innehåll

Begreppslista

Utöver de begrepp som definieras i löptext ska dessa definitioner oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges.

Behandling	En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddslagstiftning	Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den personuppgiftsbehandling som sker enligt denna Integritets- och datasäkerhetspolicy, inklusive EU-lagstiftning och lagstiftning i EUs medlemsstater.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.
Instruktion	De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av personuppgifter samt kategorier av registrerade och särskilda behov som omfattas av behandlingen.
Kundanställd	Anställd på företag, myndighet eller organisation som är kunder till Avonova och som är använder Avonovas hälso- och sjukvårdstjänster.
Logg	Logg är resultatet av Loggning. Se nedan.
Loggning	Loggning är ett kontinuerligt insamlande av uppgifter om den behandling av personuppgifter som utförs enligt denna Integritets-

	och datasäkerhetspolicy och som kan knytas till en enskild fysisk person.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
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.
Registrerad	Fysisk person vars personuppgifter behandlas.
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).
Underbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till personuppgiftsbiträdet behandlar personuppgifter för personuppgiftsansvariges räkning.
Vårdgivare	Med ”vårdgivare” avses ”statlig myndighet, landsting eller kommun i fråga om sådan hälso- och sjukvård som myndigheten, landstinget eller kommunen har ansvar för samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvård”, enligt PSL 1 kap. 3 §.
Patiensäkerhetslag (2010:659)	Med patientsäkerhet avses i denna lag, skydd mot vårdskada.

Patientdatalagen (2008:355)	Reglerna för behandling av personuppgifter inom hälso- och sjukvården finns i patientdatalagen. Patientdatalagen ska tillämpas av alla vårdgivare, både i offentlig och privat regi.
Identitetsuppgifter	Uppgifter som gör det möjligt att identifiera dig, t.ex. ditt namn.
Kontaktuppgifter	Uppgifter som gör det möjligt att kontakta dig, t.ex. adress, e-postadress och telefonnummer.
Kommunikation	Innehåll i kommunikation med oss, t.ex. innehåll i e-postmeddelanden.

1. Introduktion till Avonova

1.1 Avonovas tjänsteerbjudande

Avonova erbjuder tjänster inom företagshälsa och ledarutveckling. Med bred kunskap och stort engagemang hjälper vi organisationer och deras medarbetare att bli mer hållbara, kommunicera mer effektivt och må bättre. Våra medarbetare levererar varje dag hälsotjänster över hela Sverige.

Under "Avonova tjänster" på vår hemsida har vi samlat allt vi gör tillsammans med våra kunder för att utveckla hälso- och arbetsmiljöarbetet till att nå en hållbar nivå. Vi erbjuder tjänster med fokus på utveckling och systematik av hälso- och arbetsmiljöarbete. https://www.avonova.se/tjanster/

Avonova är tredjepartscertifierade genom Qvalify inom ISO 9001:2015 (Kvalitet), ISO 14001:2015 (Miljö), ISO 45001:2018 (Arbetsmiljö) samt Krav – ledningssystem för kvalitet inom svensk företagshälsovård, utg. 7/2016-02.

I vårt verksamhetssystem beskrivs hur vi inom kvalitet, miljö och arbetsmiljö säkrar vår verksamhet, hur vi utför våra tjänster, hur vi uppfyller krav och kriterier samt hur förbättring- och avvikelsehanteringen sker. Avonova är medlem i och följer riktlinjer från föreningen Sveriges Företagshälsor.

Genom dessa system kan vi ge en garanti att vår personal har de kvalifikationer som följer branschens riktlinjer, utför tjänster, tillämpar metoder och tekniker som grundar sig på objektivitet, vetenskap och beprövad erfarenhet.

1.2 Syftet med denna policy

Avonova värnar om er integritet. Därför har Avonova upprättat den här policyn. Den utgår från gällande dataskyddslagstiftning. Den förtydligar hur Avonova arbetar för att ta tillvara era rättigheter och er integritet. I Sverige regleras behandlingar av personuppgifter av EU:s allmänna dataskyddsförordning ("Dataskyddsförordningen" eller "GDPR") och den kompletterande svenska Dataskyddslagen (2018:218). För vårdgivare finns därutöver kompletterande bestämmelser i Patientdatalagen (2008:355). Avonova omfattas därför av alla tre regelverken.

Syftet med den här policyn är att ni ska få veta hur Avonova arbetar med kvalitet och hur vi behandlar era personuppgifter, vad vi använder dem till, vilka som får ta del av dem och under vilka förutsättningar samt hur ni kan ta tillvara era rättigheter när ni är kundanställd och har kontakt med oss inom ramen för våra hälso- och sjukvårdstjänster.

2. Avonovas ansvar och skyldigheter

2.1 Avonovas principer kring personuppgifter

Personuppgifter ska utformas och behandlas så att patienters och övriga registrerades integritet respekteras. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem.

Inom en vårdgivares verksamhet är det personal som deltar i vården, eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården, som är behörig att ta del av uppgifter.

2.2 Personuppgiftsansvar

Avonova Hälsa AB är en företagshälsa och i rollen som vårdgivare är Avonova personuppgiftsansvariga enligt Patientdatalagen för den behandling av personuppgifter som vi utför vid tillhandahållande av hälso- och sjukvård.

3. Behandling av Personuppgifter

3.1 Varifrån samlar vi in personuppgifter

Vi samlar in personuppgifter från:

- Dig själv (t.ex. när du kommunicerar med oss via e-post)
- Från andra vårdgivare (vid sammanhållen journalföring)
- Från din arbetsgivare (t.ex. för att vi ska kunna kontakta dig)

3.2 Varför behandlar vi dina personuppgifter?

Avonova är en privat vårdgivare och lyder under hälso- och sjukvårdslagstiftning, exempelvis Patientdatalagen (2008:355) som medför journalföringsplikt för att bidra till en god och säker vård. För detta ändamål har vi ett patient- och datasäkert journalsystem i vilket vi lagrar dina personuppgifter.

I rollen som vårdgivare behandlar vi känsliga personuppgifter (t.ex. uppgift om din hälsa) vilket är tillåtet enligt Patientdatalagen och Patientsäkerhetslagen (2010:659). Dessa lagar reglerar förebyggande hälso- och sjukvård samt arbetsmedicin. Företagshälsovården kan som rådgivare även genomföra faktaunderökningar på er arbetsplats samt att vi tillhandahåller hälsorelaterade tjänster där vi agerar som oberoende experter. För vissa av Avonovas tjänster gäller separata informationsdokument avseende behandling av personuppgifter, t.ex. om du använder Avonova Dialog eller Avonova Appen.

Inledning

Nedan listar vi närmare information om varför vi använder dina personuppgifter i olika fall. Vi kan även behandla dina personuppgifter för andra ändamål som inte är oförenliga med de ändamål som anges nedan.

Behandling av personuppgifter som inte omfattas av ändamålen som räknas upp nedan kan endast ske om vi har erhållit ditt uttryckliga samtycke

För att läsa mer om vilka kategorier av uppgifter och med stöd av vilken rättslig grund som vi använder personuppgifter för respektive syfte, se **vår detaljerade information om behandling av personuppgifter** längre ner i detta dokument.

Fullgöra de skyldigheter som åligger oss angående att föra patientjournal och upprätta annan dokumentation som behövs i och för vården av patienter

Vi behandlar dina personuppgifter för att kunna föra patientjournal och kunna upprätta annan dokumentation som behövs i vården av patienter.

Administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall

Vi behandlar personuppgifter för att kunna bedöma ditt vårdbehov och för att kunna ge vård i enskilda fall. Denna bedömning baseras på innehåll i patientjournalen och ska innehålla en första bedömning av dig och därefter återkommande

bedömningar som bygger på till exempel intervjuer med dig, observationer och olika undersökningar eller tidigare journaler.

Bedömningen bör innehålla information som gäller dels tiden före vårdtillfället dels den aktuella situationen:

- Uppgifter som bygger på din hälsa och levnadsförhållanden vilket kan ev. föranleda till vårdkontakt.
- Uppgifter som belyser ditt aktuella hälsotillstånd, situation och förhållanden som kan ev. föranleda till vårdkontakt.
- Uppgifter som har bedömts med hjälp av olika bedömningsinstrument, prover och undersökningar.

Upprättande av annan dokumentation som följer av lag, förordning eller annan författning

Vi behandlar dina personuppgifter för att t.ex. kunna upprätta tjänstbarhetsintyg för arbete med bl.a. fibrosframkallande damm eller isocyanater.

Systematisk och fortlöpande utveckling och säkra kvaliteten i verksamheten

Vi behandlar dina personuppgifter för att säkerställa systematisk och fortlöpande utveckling av verksamheten och säkerställande av kvaliteten i verksamheten. Vi kan bl.a. inom ramen för vad vi kallar avancerad analys genomföra samkörning av uppgifter från olika stödsystem och statistisk analys för att förutspå sannolika sjukdoms- och friskvårdsförlopp och rehabiliteringsförlopp på gruppnivå givet kända riskfaktorer. Ändamålet med analysen är att kunna ge tydligare rådgivning och andra friskvårdsinsatser till dig samt att öka kvaliteten i verksamheten för att kunna utveckla nya och förbättrade tjänster till våra patienter.

Administration, planering, uppföljning, utvärdering och tillsyn av verksamheten

Vi behandlar dina personuppgifter t.ex. för uppföljning och kontroll av förekomst av otillbörlig inloggning i patientjournaler samt föruppföljning och kontroll av efterlevnad avseende medicinska rutiner och riktlinjer vid varje Hälsocenter.

Framställande av statistik om hälso- och sjukvården

Vi framställer statistik om vår hälso- och sjukvård bl.a. för att säkerställa systematisk och fortlöpande utveckling av verksamheten och säkerställande av kvaliteten i verksamheten, t.ex. inom ramen för avancerad analys (se punkt *"Systematisk och*

fortlöpande utveckling och säkra kvaliteten i verksamheten”).

Hantera och bemöta rättsliga krav

Vi behandlar dina personuppgifter om det är nödvändigt för att hantera och bemöta ett rättsligt krav, t.ex. i samband med en tvist eller en rättsprocess. För detta syfte kan vi dela viss information med andra mottagare, se längre ned för mer information.

Uppfylla rättsliga skyldigheter

För att uppfylla rättsliga skyldigheter som vi har hanterar vi om det är nödvändigt dina personuppgifter, t.ex. för att uppfylla krav i bokförings- eller i dataskyddslagstiftning och för att fullgöra uppgiftslämnande enligt lag eller förordning. För detta syfte kan vi dela viss information med andra mottagare, se längre ned för mer information.

3.3 Sekretess och Tystnadsplikt

All personal på Avonova arbetar under sekretess och tystnadsplikt. Det innebär att alla uppgifter som rör patientens personliga förhållanden skyddas av sekretess och får enbart lämnas ut efter särskild prövning. Sekretess innebär förbud att lämna ut uppgifter, vare sig det sker muntligen, skriftligen eller på annat sätt (skyddsvärd information). Tystnadsplikt innebär förbud mot att berätta om sekretessbelagd information. Det gäller i relation till alla utom de som är direkt inblandade i arbetet med den enskilde patienten. Tystnadsplikt och sekretess i hälso- och sjukvården regleras för privata vårdgivare av reglerna i Patientsäkerhetslagen (6 kap. 12 – 16 §§).

Se även nedan angående sammanhållen journalföring.

3.4 Rättigheter

3.4.1 Rätt till tillgång

Den registrerade har rätt att vända sig till Avonova som är personuppgiftsansvarig och begära tillgång till de personuppgifter som Avonova behandlar och information om bland annat ändamålen med behandlingen och vilka personuppgifterna har delats med.

Avonova ska i egenskap av personuppgiftsansvarig förse den registrerade med en kostnadsfri kopia på de personuppgifter som behandlas. Vid eventuella extra kopior kan Avonova komma att ta ut en administrationsavgift.

3.4.2 Rätt till rättelse, radering eller begränsning

Den registrerade har rätt att utan onödigt dröjsmål få sina personuppgifter rättade eller, under vissa förutsättningar, att behandlingen begränsas eller att uppgifterna raderas. Om den registrerade anser att Avonova behandlar personuppgifter om denne som är felaktiga eller ofullständiga, kan den registrerade kräva att få dessa rättade eller kompletterade.

Den registrerade har även rätt att få sina uppgifter raderade bland annat ifall de inte längre är nödvändiga eller om behandlingen baseras på samtycke och detta har återkallats.

3.4.3 Rätt att invända

Den registrerade har rätt att när som helst invända mot behandling av dennes personuppgifter om den lagliga grunden för behandlingen utgörs av Artikel 6.1 (e) ”allmänt intresse” eller 6.1 (f) ”intresseavvägning” Dataskyddsförordningen.

Ovan innebär bland annat att den registrerade har rätt att invända mot behandling av dennes personuppgifter för direktmarknadsföring.

Om den enskilde invänder mot behandlingen får Avonova endast fortsätta att behandla uppgifterna om det går att visa att det finns avgörande berättigade skäl till behandlingen eller om det är motiverat att lagra uppgifterna i syfte att kunna fastställa, utöva eller försvara rättsliga anspråk.

3.4.4 Rätt till dataportabilitet

Den registrerade har rätt till att få ut de personuppgifter som denne tillhandahållit den personuppgiftsansvarige och har rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig. Detta gäller dock under förutsättning att det är tekniskt möjligt och den lagliga grunden för behandlingen utgörs av samtycke eller att behandlingen varit nödvändig för fullgörande av avtal med den registrerade.

3.4.5 Särskilt om patientjournaler

För anteckningar i patientjournaler gäller Patientdatalagen. Dessa anteckningar är låsta (signerade) och kan inte ändras eller raderas.

Utdrag ur patientjournal

Som patient har den registrerade i regel rätt att begära utdrag ur journalen och åtkomstloggarna.

Rättelse och destruktion

Om den registrerade som patient anser att en uppgift är felaktig kan vårdgivaren införa en rättelse i journalen. En rättelse är en notering som hänvisar till den felaktiga uppgiften och ger den rätta informationen. Både den ursprungliga anteckningen och rättelsen ligger kvar i patientjournalen. Detta under förutsättning att patienten och vårdgivaren är överens om att anteckningen skall rättas. I fall där vårdgivaren och patienten är oense om journalens riktighet, eller där patienten begär destruktion av journalen kan patienten ansöka till tillsynsmyndigheten Inspektionen för vård och omsorg ("**IVO**"). Efter prövning av IVO rättas eller raderas journalen i enlighet med myndighetens beslut. Som person har den registrerade i regel rätt att begära utdrag ur journalen och åtkomstloggarna. Detta gör du genom att kontakta det lokala Hälsocenter som den registrerade besöker hos Avonova som sedan hanterar din förfrågan. Journaler hämtas personligen och ID-kontroll krävs.

Rätt att begränsa elektronisk åtkomst för vårdsyfte

Du kan motsätta dig att personuppgifter som dokumenterats för ändamål som anges i 2 kap. 4 § första stycket 1 och 2 i Patientdatalagen (uppgifter i t.ex. patientjournal) hos en vårdenhet eller inom en vårdprocess görs tillgängliga genom elektronisk åtkomst för den som arbetar vid en annan vårdenhet eller inom en annan vårdprocess hos samma vårdgivare. I sådana fall ska uppgiften genast spärras.

Information om den direktåtkomst och elektronisk åtkomst som förekommit

Du har rätt att på begäran erhålla information om den direktåtkomst och elektroniska åtkomst som förekommit.

3.4.6 Hur skyddar vi dina personuppgifter?

Din säkerhet är viktig för oss. Därför har vi säkerhetsåtgärder för att skydda dina personuppgifter från obehörig åtkomst och annan otillåten behandling. Vi analyserar och utvärderar regelbundet åtgärderna i syfte att skyddet för dina uppgifter ska vara så säkert som möjligt.

3.4.7 Hur länge lagras personuppgifterna?

Avonova strävar efter att inte lagra mer information än vad som är nödvändigt för ändamålen och enligt bestämmelser i nationell lagstiftning, exempelvis, Bokföringslagen (1999:1078). Se närmare nedan.

3.4.8 Sökbegrepp och utlämnande av uppgifter på medium för automatiserad databehandling

I journalsystemet finns fastställda sökord i enlighet med Patientdatalagen.

3.4.9 Rätt att begära skadestånd

Du har rätt att begära skadestånd om personuppgifter behandlats i strid med Patientdatalagen.

3.5 Sammanhållen journalföring

Vårdgivare får under vissa förutsättningar ha direktåtkomst till personuppgifter som behandlas av andra vårdgivare för att fullgöra de skyldigheter som åligger oss angående att föra patientjournal och upprätta annan dokumentation som behövs i och för vården av patienter samt för administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall.

En vårdgivare får inte ha direktåtkomst till personuppgifter som behandlas av en annan vårdgivare i en utredning enligt lagen (2018:744) om försäkringsmedicinska utredningar. I den lagen finns särskilda bestämmelser om direktåtkomst vid sådana utredningar.

Om en patient motsätter sig det får inte andra uppgifter om patienten än att det finns spärrade uppgifter om en patient samt uppgift om vilken vårdgivare som har spärrat uppgifterna göras tillgängliga för andra vårdgivare genom sammanhållen journalföring. En annan vårdgivare får ta del av uppgift om vilken vårdgivare som har spärrat uppgifterna endast under särskilda omständigheter.

Innan uppgifter om en patient görs tillgängliga för andra vårdgivare genom sammanhållen journalföring ska patienten informeras om vad den sammanhållna journalföringen innebär och om att patienten kan motsätta sig att andra uppgifter än dem som anges i andra stycket görs tillgängliga för andra vårdgivare genom sammanhållen journalföring.

Om en patient motsätter sig att uppgifter görs tillgängliga för andra vårdgivare genom sammanhållen journalföring ska uppgifterna genast spärras. En patient kan när som helst begära att den vårdgivare som har spärrat uppgifterna häver spärren.

Ospärrade uppgifter om patienten ska göras tillgängliga för de vårdgivare som är anslutna till systemet med sammanhållen journalföring. Det ska vidare införas en uppgift i systemet om att det finns ospärrade uppgifter om patienten. Andra vårdgivare ska kunna ta del av denna uppgift utan att ta del av uppgift om vilken vårdgivare som har gjort uppgiften tillgänglig och övriga uppgifters innehåll.

Om det finns spärrade uppgifter om en patient och det föreligger fara för dennes liv eller det annars föreligger allvarlig risk för dennes hälsa, får vårdgivaren i vissa fall ta del av uppgift om vilken eller vilka vårdgivare som har spärrat uppgifterna. Om vårdgivaren med ledning av denna uppgift bedömer att de spärrade uppgifterna kan antas ha betydelse för den vård som patienten oundgängligen behöver, får vårdgivaren begära hos den vårdgivare som har spärrat uppgifterna att denne häver spärren.

3.6 Utlämnande av personuppgifter

Vi delar dina personuppgifter med olika mottagare.

Tjänsteleverantörer (personuppgiftsbiträden). För att hantera personuppgifter delar vi personuppgifter med tjänsteleverantörer som vi har anlitat. Dessa tjänsteleverantörer tillhandahåller exempelvis IT-tjänster. När tjänsteleverantörerna behandlar personuppgifter på vårt uppdrag och enligt våra instruktioner är de personuppgiftsbiträden till oss och vi ansvarar för hanteringen av dina personuppgifter. Tjänsteleverantörerna får inte använda dina personuppgifter för sina egna ändamål och de är skyldiga enligt lag och avtal med oss att skydda dina uppgifter och att iaktta sekretess.

Andra Vårdgivare. Vi lämnar ut personuppgifter om dig inom ramen för reglerna rörande sammanhållen journalföring.

Din Arbetsgivare. Med ditt samtycke kan vi dela tjänstbarhetsintyg med din arbetsgivare genom vår webbportal.

Övriga mottagare. I vissa fall, när det är nödvändigt, delar vi dina personuppgifter med andra mottagare för vissa syften:

- hantera och bemöta rättsliga krav,
- uppfylla rättsliga skyldigheter,
- svara på en förfrågan, och

Exempel på mottagare är externa rådgivare, myndigheter, domstol, polisen. Vi lämnar aldrig ut dina personuppgifter till andra företag eller verksamheter för marknadsföringsändamål.

3.7 Gallring

Vi behandlar dina personuppgifter så länge det är nödvändigt med hänsyn till ändamålet med behandlingen. Detta innebär normalt sett att vi sparar dina personuppgifter så länge vi har en pågående vårdrelation med dig och därefter för den period som är nödvändig för att vi ska kunna fullgöra våra rättsliga förpliktelser (t.ex. ska en journalhandling bevaras i minst tio (10) år efter det att den sista uppgiften fördes in i handlingen).

4. Datasäkerhet, kontroller och incidenthantering

För att skydda våra kunders data använder Avonova sig av säkerhetslösningar från internationellt välkända leverantörer inom säkerhetsbranschen. Lösningarna är konfigurerade enligt branschpraxis och placerade hos Avonovas ISO-27001 certifierade driftpartner i Sverige. Vid användning av SaaS tjänster väljs leverantörer ut som kan påvisa ett åtagande i linje med internationellt erkända standarder (ISO-27001 eller liknande) och som lyder under GDPR. Avonova utvärderar löpande sina leverantörer, partners och processer för att säkerställa fullgod säkerhet till våra tjänster.

4.1 Riskhantering

Vår verksamhet strävar alltid efter ständiga förbättringar, som är till nytta för våra kunder och vår verksamhet. För att vara konkurrenskraftiga arbetar vi mycket med att leta möjligheter där vi kan erbjuda mervärde till våra kunder. Möjligheterna innebär dock även risker som måste hanteras för att vi ska uppfylla våra åtaganden om att skydda våra kunders information. Vi arbetar löpande med riskbedömningar i vår verksamhet och vidtar åtgärder i förebyggande syfte. Därför genomför vi risk- och sårbarhetsanalyser vid införandet av nya lösningar.

4.2 Incidenthantering

Avonova jobbar aktivt med incidenthantering tillsammans med sin driftpartner för att skyndsamt lösa incidenter och minimal påverkan för Avonova och dess kunder. Vid avslutad incident drar Avonova lärdom av den för att arbeta förebyggande mot framtida incidenter. Vid kritiska incidenter skapas en incidentrapport och genomgång av de lärdomar vi fått av den kritiska incidenten.

4.3 Åtkomsthantering

Att skydda våra kunders information mot obehörig åtkomst är av största vikt för oss på Avonova. Vi arbetar med personliga konton, där varje konto endast har de nödvändiga

rättigheterna (”least-privilege” principen) för att vi ska kunna utföra våra åtaganden.

4.4 Datasäkerhet

På Avonova använder vi kryptering av data vid förflyttning över osäkra medium och vid vila baserat på informationens känslighet och bedömd risk.

4.5 Förändringshantering

På Avonova arbetar vi efter förändringsprocesser med tester och testmiljöer. Genom kontrollerade och testade ändringar säkerställer vi säkerheter och tillgängligheten på våra tjänster.

4.6 Konsekvensbedömning

Avonova arbetar med konsekvensbedömningar enligt Dataskyddsförordningen i de fall där den planerade behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Vid utveckling eller förändring av tjänster utför Avonova en bedömning baserat på kriterier i enlighet med tillsynsmyndighetens vägledning, för att fastställa om behandlingen, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter och vilka risksänkande åtgärder som i förekommande fall bör vidtas.

4.7 Överföring av personuppgifter till tredje land

Vi sparar dina personuppgifter inom EU/EES-området.

****

avonova

Detaljerad information om behandlingar av personuppgifter

Se nedan för detaljerad information om vilka kategorier av personuppgifter som vi behandlar med stöd av vilken rättslig grund.

Ändamål	***Personuppgifter***	***Rättslig grund***
Fullgöra de skyldigheter som åligger oss angående att föra patientjournal och upprätta annan dokumentation som behövs i och för vården av patienter	• Identitetsuppgifter • Hälsouppgifter • Kontaktuppgifter • Övrig i journal och annan dokumentation förekommande uppgifter	Rättslig förpliktelse (artikel 6.1 c) i GDPR) Känsliga personuppgifter (artikel 9.2 h) i GDPR)
Administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall	• Identitetsuppgifter • Hälsouppgifter • Kontaktuppgifter • Övrig i journal och annan dokumentation förekommande uppgifter	Rättslig förpliktelse (artikel 6.1 c) i GDPR) eller Allmänt intresse (artikel 6.1 e) i GDPR) Känsliga personuppgifter (artikel 9.2 h) i GDPR)
Upprättande av annan dokumentation som följer av lag, förordning eller annan författning	• Berörda kategorier av personuppgifter som är nödvändiga för att upprätta dokumentation som krävs enligt lag, förordning eller författning i det enskilda fallet.	Rättslig förpliktelse (artikel 6.1 c) i GDPR) Känsliga personuppgifter (artikel 9.2 h) i GDPR)
Systematisk och fortlöpande utveckling och säkra kvaliteten i verksamheten	• Identitetsuppgifter • Hälsouppgifter • Kontaktuppgifter • Övrig i journal och annan dokumentation förekommande uppgifter	Rättslig förpliktelse (artikel 6.1 c) i GDPR) eller Allmänt intresse (artikel 6.1 e) i GDPR) Känsliga personuppgifter (artikel 9.2 h) i GDPR)
Administration, planering, uppföljning, utvärdering och tillsyn av	• Identitetsuppgifter • Hälsouppgifter • Kontaktuppgifter	Rättslig förpliktelse (artikel 6.1 c) i GDPR) eller Allmänt

verksamheten	• Övrig i journal och annan dokumentation förekommande uppgifter	intresse (artikel 6.1 e) i GDPR) Känsliga personuppgifter (artikel 9.2 h) i GDPR)
Framställande av statistik om hälso- och sjukvården	• Identitetsuppgifter • Hälsouppgifter • Kontaktuppgifter • Övrig i journal och annan dokumentation förekommande uppgifter Framtagen statistik innehåller inte personuppgifter.	Rättslig förpliktelse (artikel 6.1 c) i GDPR) eller Allmänt intresse (artikel 6.1 e) i GDPR) Känsliga personuppgifter (artikel 9.2 h) i GDPR)
Hantera och bemöta rättsliga krav	• Berörda kategorier av personuppgifter som är nödvändiga för att hantera och bemöta det rättsliga kravet i det enskilda fallet.	Berättigat intresse (artikel 6.1 f) i GDPR). Behandlingen är nödvändig för att tillgodose vårt berättigade intresse av att hantera och bemöta rättsliga krav. Känsliga personuppgifter (artikel 9.2 f) i GDPR)
Uppfylla övriga rättsliga skyldigheter	• Berörda kategorier av personuppgifter som är nödvändiga för att uppfylla respektive rättslig skyldighet.	Rättslig förpliktelse (artikel 6.1 c) i GDPR)

När vi delar personuppgifter

Se nedan för detaljerad information om vilka kategorier av personuppgifter vi delar med olika kategorier av mottagare för olika syften och med stöd av vilken laglig grund.

Mottagare	***Ändamål***	***Personuppgifter***	***Rättslig grund***
Andra vårdgivare	Sammanhållen journalföring	• Hälsouppgifter • Identitetsuppgifter • Kontaktuppgifter • Personnummer • I övrigt i journal förekommande personuppgifter	Rättslig förpliktelse (artikel 6.1 c) i GDPR) eller Allmänt intresse (artikel 6.1 e) i GDPR) Känsliga personuppgifter (artikel 9.2 h) i GDPR)
Din Arbetsgivare	Delning av tjänstbarhetsintyg	• Hälsouppgifter • Identitetsuppgifter • Kontaktuppgifter	Samtycke (artikel 6.1 a) och artikel 9.2 a) i GDPR)
Din Arbetsgivare	Personlighetstest	• Hälsouppgifter • Kontaktuppgifter • Personnummer	Samtycke (artikel 6.1 a) och artikel 9.2 a) i GDPR)

Övriga mottagare

Ändamål	***Rättslig grund***
Hantera och bemöta rättsliga krav Endast de kategorier av personuppgifter som är nödvändiga för att hantera och bemöta det rättsliga kravet i det enskilda fallet.	Berättigat intresse (artikel 6.1 f) i GDPR). Behandlingen är nödvändig för att tillgodose vårt berättigade intresse av att hantera och bemöta rättsliga krav. Känsliga personuppgifter (artikel 9.2 f)) i GDPR)
Uppfylla rättsliga skyldigheter Endast de kategorier av personuppgifter som är nödvändiga för att uppfylla respektive rättslig skyldighet.	Uppfylla rättslig skyldighet (artikel 6.1 c) i GDPR). Behandlingen är nödvändig för att uppfylla rättsliga skyldigheter som vi har. Känsliga personuppgifter (artikel 9.2 f)) i GDPR)
Svara på en förfrågan	Berättigat intresse (artikel 6.1 f) i GDPR) eller uppfylla rättslig skyldighet (artikel 6.1

Endast de kategorier av personuppgifter som är nödvändiga för att svara på förfrågan.	c) i GDPR). I den utsträckning vi är skyldiga att besvara en förfrågan behandlas personuppgifter för att uppfylla den rättsliga skyldigheten. I annat fall sker behandlingen med stöd av en intresseavvägning när det är nödvändigt för att tillgodose vårt och förfrågarens berättigade intresse av att vi svarar på förfrågan.