19.02.2021

Behandling av personuppgifter för dig som kund & anställd hos kund

Avonova värnar om din integritet. Därför har vi upprättat den här policyn. Den utgår från gällande dataskyddslagstiftning och förtydligar hur vi jobbar för att ta tillvara dina rättigheter och din integritet.

Syftet med den här policyn är att du ska få veta hur vi behandlar dina personuppgifter, vad vi använder dem till, vilka som får ta del av dem och under vilka förutsättningar samt hur du kan ta tillvara dina rättigheter.

Avonova är personuppgiftsansvariga

Avonova Hälsa AB är en företagshälsa och i rollen som vårdgivare är vi personuppgiftsansvariga.

Avonova är personuppgiftsbiträde

När det gäller sjuk och frisk.

Med stöd av vilka rättsliga grunder behandlar vi personuppgifter om dig?

I rollen som vårdgivare behandlar vi känsliga personuppgifter vilket har en laglig grund i Patientdatalagen (2008:355) och Patientsäkerhetslagen (2010:659). Dessa lagar hör samman med förebyggande hälso- och sjukvård och arbetsmedicin. I den mån vi behandlar ytterligare uppgifter kommer vi att inhämta ditt samtycke eller säkerställa att behandlingen är tillåten med stöd av annan rättslig grund.

Företagshälsovården kan som rådgivare även genomföra faktaunderökningar på er arbetsplats samt att vi tillhandahåller hälsorelaterade tjänster där vi agerar som oberoende experter.

Patientdatalagen bygger på bland annat följande principer:

- 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 av dig, eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården, som är behörig att ta del av uppgifter om dig.

Varför behandlar vi personuppgifter om dig?

- Avonova behandlar dina personuppgifter för att kunna tillhandahålla dig våra tjänster endast för att fullgöra ett avtal med dig som kund & kundanställd
- Avonova behandlar information om din hälsa för att kunna förebygga och lindra tecken på ohälsa.
- Avonova är en 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 journalsystem
- Bedriva verksamhetsuppföljning, utveckling och forskning inom hälsa
- Framställa statistik inom företagshälsan. Statistiken är anonymiserad och går inte att härleda till en enskild individ
- Handlägga ärenden på ett effektivt och rättssäkert sätt.

19.02.2021

Vilka uppgifter samlar vi in om dig – och varför?

Vi strävar efter att inte samla in fler personuppgifter än nödvändigt för att kunna ingå eller fullgöra avtal med din arbetsgivare. För att kunna ingå samt fullgöra avtal med dig behöver vi: Personnummer, förnamn, efternamn, e-postadress, adress och arbetsplats samt ev. hälsoinformation och information som du väljer att uppge av skäl som hör samman med förebyggande hälso- och sjukvård och arbetsmedicin. Avonova får endast tillgång till dina personuppgifter genom ditt/din arbetsgivares tillhandahållande av uppgifterna till oss.

Tystnadsplikt

Avonova regeleras av tystnadsplikt och vi lämnar aldrig ut personuppgifter till obehöriga. Hälsoinformation är en känslig personuppgift och regleras.

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.

Vilka lämnar vi ut dina uppgifter till?

Vi lämnar inte ut dina uppgifter till andra företag eller organisationer om det inte krävs enligt lag eller är nödvändigt för att utföra våra lagstadgade eller avtalsenliga förpliktelser gentemot dig.

Vi kan lämna ut dina personuppgifter till någon av våra samarbetspartners, leverantörer eller underleverantörer, men endast om det behövs för att vi ska kunna uppfylla våra skyldigheter i förhållande till dig som kund. Vi lämnar aldrig ut fler personuppgifter än vad som är nödvändigt.

När det krävs enligt lag kan vi behöva lämna ut dina uppgifter till myndigheter och andra organisationer. Vi kan också behöva lämna ut dina uppgifter om det är nödvändigt för att utöva, fastställa eller bevaka våra rättsliga anspråk.

Vi lämnar aldrig ut dina personuppgifter till andra företag eller verksamheter för marknadsföringsändamål.

För journalanteckningar i din journaler, där gäller Patientdatalagen. Dessa anteckningar är låsta (signerade) och kan inte ändras eller raderas. Som person har du i regel rätt att begära utdrag ur journalen och åtkomstloggarna. Detta gör du genom att kontakta det lokala Hälsocenter som du besöker hos Avonova som sedan hanterar din förfrågan. Journaler hämtas personligen och ID-kontroll krävs.

19.02.2021

Tredjelandsöverföring

Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området.

Microsoft paketet Microsoft Molndesign för Offentlig Sektor (MSMD) Syftet är att förenkla för den offentliga sektorn i Sverige att använda sig av molntjänster i Microsoft Azure. MSMD lanseras den 1 december 2020 i samarbete med ett antal utvalda partnerföretag i Sverige. Bland annat CGI som Avonova arbetar med.

Microsoft Molndesign för Offentlig Sektor lanseras den 1 december i samarbete med Atea, TietoEVRY, TrueSec, OneVinn, B3 Consulting Group, NordCloud, Asurgent, ***CGI****, Sogeti och Certezza.*

Hur MSMD hjälper offentlig sektor att upprätthålla GDPR

- ***Azure Blueprint för svensk offentlig sektor*** *som baseras på MSB:s metodstöd för systematiskt informationssäkerhetsarbete ISO 27001.*
- ***Microsoft Compliance-paket för GDPR*** *som gör det möjligt att verifiera organisationens och Microsoft Azure's regelefterlevnad av GDPR.*
- ***Azure Data Subject Request*** *gör det möjligt att svara på förfrågningar om åtkomst, rättelse, radering och export av personuppgifter i Azure.*

Hur MSMD hjälper offentlig sektor att upprätthålla OSL
Förutom alla delar som ingår kopplat till GDPR så ingår dessutom:

- ***Azure Customer Lockbox*** *(extra kostnader kan tillkomma) som inför ett extra steg för sekretessprövning innan någon kan ges tillgång till kunddata vid support.*
- ***Double Key Encryption (eller motsvarande)*** *som hindrar tillgång till kunddata för alla som inte har tillgång till krypteringsnycklarna, inklusive Microsoft.*

Hur MSMD hjälper offentlig sektor att upprätthålla säkerhetsskyddslagen
Förutom komponenter som finns beskrivna i avsnitten ovan avseende GDPR och OSL så erbjuder Microsoft:

- ***Azure Stack Hub****. Ett eget privat Azure som man kan köra helt eller delvis bortkopplat från Internet och det offentliga molnet.*[1]

Webbportalen (CGI)

- *Vi överför inte själva eller genom våra underleverantörer personuppgifter till tredje land*
- *Det finns inga andra mottagare heller som för över personuppgifter i tredje land.*
- *Vi använder oss av Microsoft Azure för lagring av data. Då MS är baserat i USA är de underställda amerikansk lag. Amerikanska myndigheter har alltså möjlighet att begära ut denna data.*

Två-faktorautentisering

- *Autentisering sker via inlogg med organisationskonto från Microsoft eller Microsoft Live-konto och det sker följdaktligen antingen mot användarens organisations AD eller mot live.com (dvs Microsofts server som hanterar personliga konton).*
- *Säkerhetsnivån beror alltså på policies som satts upp inom användarens organisation eller på inställningar på live-kontot. Dvs finns det en policy inom kundens organisation att två-faktorautentisering ska användas för att logga in gäller detta även inloggning i webbportalen.*

[1] https://news.microsoft.com/sv-se/2020/11/24/microsoft-molndesign-for-offentlig-sektor/?fbclid=IwAR0_SJPjEbYrBg0Nptf9EcaDV2FKF9TTVzQXb8v-_I0XBf2r8T0hEjD8k3o

19.02.2021

Samma sak gäller live kontot; om kontot är konfigurerat att använda två-faktorautentisering så gäller det även inloggningen mot Avonova.

Säkerhet - Dokument i dokumentarkivet och bilagor till meddelanden

- *Alla filer och bilagor lagras krypterade i Azure.*
- *Informationen skickas över en krypterad kanal (krypterad med TLS 1.2) mellan klient och server.*

In och utloggning

- *Webbportalen har in- och utloggningsmöjlighet. Användaren ansvarar för aktiv in- och utloggning från Webbportalen.*

Cookies - Avonova

- *Avonovas webbportal använder cookies för insamlande av telemetri-data. Detta är data som används för att avhjälpa fel och för att ta fram statistik runt användandet av tjänsten. Avonova använder ingen typ av tracking cookies eller andra tredjeparts cookies.*

Cookies - Microsoft

- *Sajten bygger på Sharepoint Online, en plattform som levereras och driftas av Microsoft. Microsoft använder cookies för att plattformen ska fungera som den ska. Denna data är endast för internt bruk hos Microsoft enligt "Microsoft Online Services Data Protection Addendum". Mer info om hur microsoft använder data kopplad till deras onlinetjänster hittas här.*
  (https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67)

Avonova Dialog (CGI)

Se ovan

Compodium- videotjänst (office mangement)

Datan är placerad i Sverige

Hubspot (CRM)

- För att kunna behandla förfrågningar du sänder till oss via formuläret på avonova.se lagrar vi denna information i vårt CRM-System, Hubspot
- Hubspot lagra i dag sin data i USA.

Hur länge behandlar vi dina personuppgifter?

Avonova lagrar inte mer information än vad som är nödvändigt för ändamålen och enligt bestämmelsen i nationell lagstiftning. Uppgifter i din journal arkiveras under minst 10 år enligt patientdatalagen (2008:355).

Dina rättigheter

När vi behandlar personuppgifter om dig har du som registrerad flera rättigheter. Du har rätt att när som helst ta kontakt med oss gällande dessa, och om du vill utöva någon av rättigheterna som beskrivs nedan når du oss enklast på gdpr@avonova.se

19.02.2021
Vi förbehåller oss rätten att vidta lämpliga skydds- och säkerhetsåtgärder i syfte att säkerställa att du är den du utger dig för att vara när du tar kontakt med oss. Om du inte kan visa din identitet på ett trovärdigt sätt är det inte säkert att vi kan tillmötesgå din begäran.

Tillgång till personuppgifter
Du har rätt att få veta vilka personuppgifter vi behandlar om dig. Om du vill veta det kan du få ett sammanställt registerutdrag av oss som innehåller de personuppgifter vi behandlar om dig.

Rättelse och radering
Om vi behandlar dina personuppgifter på ett felaktigt sätt eller om vi inte längre behöver uppgifterna har du rätt att få dem raderade. Om uppgifterna är ofullständiga har du rätt att få dem kompletterade. Tänk på att det inte är säkert att vi kan utföra våra tjänster till dig om du begär att få dina personuppgifter raderade. Om du 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 journalen. Detta under förutsättning att du och vårdgivaren är överens om att anteckningen skall rättas. I fall där vårdgivaren och du är oense om journalens riktighet, eller där du begär destruktion av journalen kan du ansöka till tillsynsmyndigheten Inspektionen för vård och omsorg ("IVO"). Efter prövning av IVO rättas eller raderas journalen i enlighet med myndighetens beslut.

Rätt att inge klagomål
Du har rätt att inge klagomål till Datainspektionen om du anser att vi behandlar dina personuppgifter på ett felaktigt sätt. Du kan läsa mer om detta på Datainspektionens hemsida www.datainspektionen.se.

Avonova förbehåller sig rätten att uppdatera eller ändra denna policy när som helst utan föregående meddelande, och ni bör regelbundet besöka denna webbplats för den senaste versionen.

Definition	Betydelse
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
Dataskyddsförordningen (GDPR)	till att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter
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 §.