Bilaga
Instruktioner Behandling av personuppgifter eFrikort

Bilaga

Specifikation över behandling av personuppgifter

1. **kontaktuppgifter**

|  |  |  |
| --- | --- | --- |
|  | Leverantören | Kunden |
| Namn och organisationsnummer | CGI Sverige AB, 556337-2191 | Region Jönköpings län,232100-0057 |
| Företrädare | Anette Hägglund Sundin | Peter Lindberg |
| Dataskyddsombud, om något | Catarina Sandberg är leverantörens kontaktperson, men ej registrerat dataskydds-ombud | Johan Cederlund |

1. **Instruktioner**

 **Kortfattad beskrivning av Tjänsten och ändamålen med behandlingen**

Ange alla ändamål för vilka personuppgifter ska behandlas av Leverantören:

Ändamålet med behandlingen är att kunna tillhandahålla en elektronisk frikortstjänst för att underlätta för kassapersonal och patient vid besök inom vården.

Leverantören ska även kontinuerligt utveckla och förbättra tjänsten och för att uppfylla detta uppdrag kan Leverantören behöva behandla personuppgifter.

 **Kategorier av personuppgifter**

Ange vilka **personuppgifter** som ska behandlas av Leverantören:

Uppgifter som krävs för att beräkna en patients frikort, så som personnummer, HSA-Id för den enhet där vårdbesöket ägt rum och betald avgift för vårdbesöket samt namn och adress till patienter som uppnått frikort och skall erhålla ett fysiskt frikort med posten.

Ange vilka **särskilda kategorier** av personuppgifter som ska behandlas av Leverantören (om några):

|  |  |
| --- | --- |
| **Särskilda kategorier av personuppgifter** |  |
| Ras eller etniskt ursprung | **[ ]**  |
| Politiska åsikter | **[ ]**  |
| Religiös eller filosofisk övertygelse | **[ ]**  |
| Medlemskap i fackförening | **[ ]**  |
| Genetiska uppgifter | **[ ]**  |
| Biometriska uppgifter | **[ ]**  |
| Uppgifter om hälsa | **[x]**  |
| Uppgifter om fysisk person sexualliv eller sexuella läggning | **[ ]**  |
| Inga särskilda kategorier av personuppgifter behandlas | **[ ]**  |

Ange vilka personuppgifter som är **extra skyddsvärda**, utöver de som angivits som särskilda kategorier av personuppgifter.

* Personnummer
* HSA-id för vårdenhet där patient gjort vårdbesök anses som känslig uppgift.

 **Kategorier av registrerade**

Ange vilka kategorier av registrerade som Leverantören kommer att behandla personuppgifter om och dess omfattning:

Patienter som besöker vårdgivare som är ansluten till tjänsten eFrikort.

 **Behandlingsaktiviteter (lagring, administrering, samkörning av register osv.)**

Ange vilka behandlingar som kommer att utföras av Leverantören:

Lagring, administrering.

 **Plats för behandling av personuppgifter**

Ange alla länder där personuppgifter kan komma att lagras och/eller behandlas av Leverantören:

Sverige

**Användning i syfte att förbättra Tjänsten**

Om Leverantören ska ha rätt att behandla personuppgifter ”i syfte att utveckla och förbättra Tjänsten” ska detta uttryckligen framgå av nedanstående ifyllda tabell.

|  |
| --- |
| Specifikation över de kategorier av personuppgifter som får användas i syfte att förbättra den Tjänst som Kunden har beställt: |
| Personnummer, namn, adress, vårdbesöksinformation |
| Dessa personuppgifter ska hämtas från följande behandlingar som leverantören utför för Kundens räkning: |
| Felsökning, lagring |
| Och får endast användas av Leverantören i syfte att förbättra och/eller utveckla följande typer av Tjänster eller kategorier av Tjänster som Kunden beställt: |
| eFrikort med tillhörande stödtjänster som kunden beställt via Avtalet |

**Säkerhetsåtgärder**

Leverantören är ISO27001-certifierad och tillämpar därmed säkerhetsåtgärder för att uppfylla standarden och för att skydda våra kunders personuppgifter. Nedan finns de säkerhetsföreskrifter som Leverantören tillämpar.

För det fall att Kunden instruerar Leverantören att implementera ytterligare tekniska och organisatoriska säkerhetsåtgärder ska sådana listas nedan. För det fall inga ytterligare åtgärder har listats så är Parterna överens om att Leverantörens Säkerhetsföreskrifter nedan i så fall utgör Kundens uttömmande instruktion om de säkerhetsåtgärder som ska vidtas av Leverantören.

Ange eventuella ytterligare organisatoriska och tekniska säkerhetsåtgärder som ska implementeras av Leverantören:

*Fysisk åtkomstkontroll*

Åtgärder som förhindrar obehörigas fysiska tillgång till IT-system där behandling av personuppgifter sker:

Endast behörig personal hos Leverantören har åtkomst till servrar där personuppgifter finns lagrade. Behörighet godkänns och tilldelas av närmaste chef. Var 3:e eller var 6:e månad behöver behörigheten förnyas om behörigheten fortfarande är aktiv. Behörighet kan även plockas bort manuellt om personalen inte längre ska ha behörighet.

*Åtkomstkontroll avseende system*

Åtgärder som förhindrar obehöriga att använda IT-system:

Web-service

Kommunikation mellan anropande system och Tjänsten ska ske genom 2-vägs SSL/TLS. Om den anropande aktören ej använder klientcertifikat ska behörighet till tjänsten ej medges. Tjänsterna ska följa RIV Tekniska Anvisningar. Tjänsten skall även konfigureras att lita på det anropande systemet. Leverantören får endast göra denna konfiguration efter instruktion av Kunden.

Webgränssnitt

Tjänstens webbgränssnitt skall skyddas av ett autentiseringsfilter som säkerställer att aktören är behörig. Tvåfaktorsautentisering skall användas. Endast personer med behörig systemroll och medarbetaruppdrag skall ges tillträde till tjänsten.

Den personal som arbetar med tjänstens utveckling, förvaltning och support skall ges tillträde till tjänsten för att kunna uppfylla avtalet.

*Åtkomstkontroll avseende personuppgifter*

Åtgärder för att säkerställa att personer som är behöriga att använda IT-systemet endast bereds tillgång till personuppgifter som omfattas av personernas fastställda behörigheter:

När det gäller personal hos Kunden eller dess vårdgivare tilldelas behörighet till tjänstens webbgränssnitt av Kunden eller dess vårdgivare. Personal hos Leverantören tilldelas behörighet av någon av tjänstens Kunder eller Inera.

*Åtkomstkontroll vid överföringar*

Åtgärder för att säkerställa att personuppgifter inte obehörigen kan läsas, kopieras, ändras eller raderas vid elektronisk överföring eller vid överföring eller lagring på lagringsenheter samt att mottagare kan identifieras och kontrolleras då överföring av personuppgifter sker via elektronisk överföring:

Kommunikation mellan anropande system och efrikortstjänsten skall ske genom 2-vägs SSL/TLS.

Filer som skickas till printavdelningen för distribuering av fysiska frikort skall överföras via sftp.

*Kontroll över inmatning av personuppgifter*

Leverantören implementerar nedan listade åtgärder för att säkerställa att det i relevanta delar i efterhand går att granska och avgöra om personuppgifter har matats in, ändrats eller raderats i IT-systemet och vem som har vidtagit åtgärden:

Allt som utförs och som rör personuppgiftsbehandling i tjänsten ska loggas så att kunden kan följa upp. Uppföljning ska kunna kan ske utifrån personidentitet på patient, identitet på användare eller angivet frikort.

*Tillgänglighetskontroll*

Åtgärder för att säkerställa att personuppgifter skyddas mot oavsiktlig förstörelse eller förlust:

Personuppgifterna ska regelbundet överföras till säkerhetskopior. Kopiorna ska förvaras avskilt och väl skyddade så att personuppgifterna kan återskapas efter en störning. Personuppgiftsbiträdet ska ha en rutin för test av återläsning.

*Lagringsregler*

Åtgärder för att tillse att personuppgifter gallras under och efter avtalstiden när användningen inte längre är nödvändig för det ursprungliga ändamålet:

Under avtalstiden: Enligt Patientdatalagen skall alla loggar lagras i minst 5 år. Så snart som möjligt och senast inom 2 månader efter att 5 år passerats skall loggarna raderas.

Frikortsdata för respektive patient skall lagras i 24 månader för att kunna hantera aktuell frikortsperiod samt se historik över frikort.

Ostrukturerat data i servicedesken/funktionsbrevlåda skall raderas inom 1 månad från att ärendet inkommit.

Filer för distribuering av fysiska frikort får lagras i maximalt 2 månader.

Efter att avtalet har upphört att gälla: se punkten **Fel! Hittar inte referenskälla.** i Biträdesavtalet.

*Leverantörens säkerhetsföreskrifter*

Ange Leverantörens Säkerhetsföreskrifter som ska gälla för personuppgiftsbehandlingen:

Leverantören skall, för att åstadkomma i detta avtal föreskriven säkerhetsnivå, tillse:

* att arbetsrutiner och arbetsuppgifter är utformade på ett sådant sätt att det blir möjligt för personalen att arbeta och tänka säkerhetsmedvetet,
* att personalen informeras om vikten av att följa gällande säkerhetsrutiner,
* att IT-utrustning som används för behandling av personuppgifter har ett tillfredsställande skydd mot stöld och händelser som kan förstöra utrustningen,
* att nödvändiga åtgärder vidtas för att förhindra att personuppgifter förstörs, ändras eller förvanskas vid överföring via nät och för att skydda anslutna tjänster mot obehörigåtkomst
* att utrustningen som är ansluten till Internet eller annat öppet nät skyddas från obehörig trafik.

**på förhand Godkända underbiträden**

Leverantören har rätt att använda följande underbiträden för att behandla personuppgifter inom ramen för Biträdesavtalet:

|  |  |
| --- | --- |
| **Namn** | **Plats för behandling (land)** |
| --- | --- |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_