Konsekvensbedömning enligt GDPR

Bedömning av behandling Digital egenmakt för arbetsrehabilitering

2021-12-10

Konsekvensbedömning	Förhandssamråd	Inlagda i Myndighetens förteckning
☐ Underlag ☐ Genomförd ☐ Granskad av DSO[1]	☐ Underlag ☐ Granskad av DSO ☐ Godkänd av informationsägaren ☐ Genomfört	☐ Underlag ☐ Förtecknad ☐ Granskad av DSO ☐ Godkänt av informationsägaren

Versionshantering

Datum	Version	Beskrivning	Ändrat av
2021-06-11		Upprättad	Lena Thång
2021-06-14		Workshop. Kap 1–2.3	Lena Thång
2021-06-23		Workshop. Kap 2.4–4	Lena Thång
2021-06-29		Workshop. Kap 4–8	Lena Thång
2021-12-08		Sammanställning ifrån riskbedömningen och genomgång av dokumentet	Marinette Edlund

Medverkande

Namn	Roll
Karin Jacobsen	Projektledare/Verksamhetsutvecklare
Annika Angerfelt	Förbundschef, Samordningsförbundet Stockholms Stad
Malene Schmidt	Leverantör - MyIndicators
Patrik Helenius	Leverantör - MyIndicators
Lena Thång	Analysledare, Security Solutions Scandinavia AB

[1] DSO är en förkortning för dataskyddsombud, se artikel 37 GDPR.

Innehåll

1 Grundläggande uppgifter 5
1.1 Tidigare konsekvensbedömning (DPIA) 5
1.2 Uppgifter om kontaktperson för bedömningen 5
1.3 Namn på bedömningen 5
1.4 Behandlings namn 5
1.5 Ändamål med behandling 6
1.6 Bakgrund (processbeskrivning) 6
1.7 Personuppgiftsansvarig – PUA (organisation) 6
1.8 Kontaktperson (hos PUA/infoägare/processägare) 6
1.9 Ansvarig chef 6
1.10 Verksamhetsområde 6
1.11 Rättslig grund (art 6) 6
1.12 Kategorier av personuppgifter 7
1.13 Kategorier av registrerade 7
1.14 Antal registrerade 8
1.15 Publikt tillgängliga uppgifter 8
1.16 Tillgång till personuppgifter 8
1.16.1 Tillgång till personuppgifter (omfattning) 8
1.17 Lagring (Informationsredovisning) 9
1.18 Sekretess (OSL och andra bestämmelser) 9

2 Personuppgifter, känslighet och behandlingens karaktär 9
2.1 Känsliga personuppgifter (art 9) 9
2.1.1 Ange vilka känsliga personuppgifter som behandlas 9
2.1.2 Rättslig grund - känsliga (art 9) 10
2.2 Extra skyddsvärda personuppgifter 10
2.3 Beskrivning av användning av känsliga och/eller extra skyddsvärda PU 11
2.4 Utvärdering eller poängsättning 11
2.5 Automatiskt beslutfattande 11
2.6 Systematisk övervakning 12
2.7 Samkörning av uppgifter 12
2.8 Uppgifter om sårbara eller i beroendeställning 12
2.9 Ny teknik eller innovativa organisatoriska lösningar 13
2.10 Begränsning av rättigheter 13

3 Ansvarsskyldighet (efterlevnad av principer) 13
3.1 Laglighet (Ändamålsbegränsning) 13
3.1.1 Ytterligare ändamål 14
3.1.2 Automatiskt beslutfattande (rättslig grund) 14
3.2 Korrekthet 14
3.3 Öppenhet (transparens) 15
3.3.1 Kriterier för information 15
3.3.2 Åtgärder för transparens 15
3.3.3 Samtycke 16
3.4 Uppgiftsminimering 16
3.5 Riktighet och kvalitet vid insamling 16
3.6 Riktighet och kvalitet – löpande 17
3.7 Lagringsminimering 17
3.8 Integritet och konfidentialitet 17
3.8.1 Klassning 17
3.9 Proportionalitet och nödvändighet 18
3.9.1 Proportionell (nytta minus risker) 18
3.9.2 Nödvändig 18
3.9.3 Bedömning intresseavvägning 19

4 Individers rättigheter 19
4.1 Tillämpliga rättigheter 19

4.2 Administrativa åtgärder för rättigheter 19
4.3 Tekniska åtgärder för rättigheter (PbD) 19

5 Tredjelandöverföring 20
5.1 Förekomst 20
5.2 Grund för tredjelandsöverföring 20

6 Personuppgiftsbiträden (PUB) 21
6.1 Extern drift 21
6.2 Omfattning 21
6.3 Personuppgiftsbiträdesavtal (PUB-avtal) 21
6.4 Instruktioner 21
6.5 Leverantörskontroll 21
6.6 Har PUB egna syften? 21
6.7 Underbiträde 22

7 Delning 22
7.1 Informationsskyldighet (lag, förordning eller föreskrift) 22

8 Övrigt 22
8.1 Certifieringar eller uppförandekoder 22

9 Risker och åtgärder 23
9.1 Riskidentifiering 23
9.2 Riskkällor 23
9.3 Riskgrupper 24
9.4 Riskperspektiv 24
9.5 Tekniska säkerhetsåtgärder 24
9.6 Administrativa åtgärder 25
9.7 Inbyggt dataskydd – Privacy by Design (art 25, 26) 26
9.8 Sammanfattning av riskbedömning 27
9.9 Risker med högst riskvärde 28
9.9 Bedömning kvarvarande risk 38
9.10 Förhandssamråd 38

10 Bilagor 39

11 Referenser 40

12 Appendix 1 – Exempel på konsekvenser och sannolikheter 41
12.1 Konsekvenser 41
12.2 Sannolikhet 43

13 Appendix 2 – Lista på personuppgiftskategorier 44

1 Grundläggande uppgifter

Om en tröskelanalys för konsekvensbedömning har genomförts, vänligen beskriv samma svar under detta avsnitt ett som i tröskelanalysen från 1.1 till 1.15. Även kan mycket grundläggande uppgifter hämtas från personuppgiftsregistret om behandlingen redan finns beskriven där.

1.1 Tidigare konsekvensbedömning (DPIA)

Detta är en:

☒ Ny konsekvensbedömning

☐ Komplement till en tidigare konsekvensbedömning (DPIA)

Har någon annan gjort en liknande konsekvensbedömning för tekniken som används eller liknande aktiviteter?

Är behandlingens art, omfattning, sammanhang och ändamål mycket lika en behandling för vilken en konsekvensbedömning har utförts?

☐ Ja

☒ Nej

☐ Inte säker

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

1.2 Uppgifter om kontaktperson för bedömningen

Namn:

Annika Angerfelt

Organisation/Enhet:

Samordningsförbundet Stockholms Stad

E-post:

annika.angerfelt@stockholm.se

Telefonnummer:

0850849180

1.3 Namn på bedömningen

Digital egenmakt för arbetsrehabilitering

1.4 Behandlings namn

Personuppgifter i projektet digital egenmakt

1.5 Ändamål med behandling

Arbetsrehabilitering i samverkan med digitalt stöd

1.6 Bakgrund (processbeskrivning)

Appen är utvecklad utifrån beteendevetenskaplig grund. Appen kan användas av individen under tiden för arbetsrehabilitering och för arbetscoachen finns en webbaserad plattform. Syftet med appen är för kommunikation och uppföljning mellan deltagare och arbetscoach.

1.7 Personuppgiftsansvarig – PUA (organisation)

Skriv in vilken eller vilka organisationer (gemensam personuppgiftsansvarig) som är ansvarig för den aktuella personuppgiftsbehandlingen.

Samordningsförbundet Stockholm Stad

1.8 Kontaktperson (hos PUA/infoägare/processägare)

Skriv in den som ska vara kontaktperson (informationsägaren) på myndigheten för aktuell behandling.

Karin Jacobsen, Projektledare/Verksamhetsutvecklare

1.9 Ansvarig chef

Detta kan vara verksamhetschef, enhetschef, avdelningschef, kanslichef eller förvaltningschef.

Annika Angerfelt, Förbundschef

1.10 Verksamhetsområde

Ange vid vilka avdelningar eller verksamhetsområden som behandlingen finns och, om möjligt, vilken enhet eller grupp.

Ej tillämplig

1.11 Rättslig grund (art 6)

Vilken av följande rättsliga grunder används för behandlingen?

- ☐ Myndighetsutövning och uppgift av allmänt intresse
- ☐ Rättslig förpliktelse
- ☒ Avtal med den registrerade
- ☐ Skydda grundläggande intresse
- ☐ Intresseavvägning
- ☐ Samtycke

Beskriv och kommentera ditt svar nedan:

Avtal med registrerad – anställd och deltagare

1.12 Kategorier av personuppgifter

Vilka kategorier av personuppgifter behandlas?

Se Appendix 2 – Lista på personuppgiftskategorier för detaljerad information om vad de olika kategorierna exempelvis innehåller.

☒ Anställningsinformation (HR)
☐ Information om arbetsmiljön
☐ Bakgrundskontroller
☐ Biometriska och genetiska uppgifter
☐ Inloggningsuppgifter
☐ Familjeinformation
☐ Finansiella uppgifter
☐ Kontaktinformation
☐ Myndighetsutfärdad identifikation
☒ Personlig identifikation
☐ Information om resor och kostnader
☐ Information om individer i sociala medier
☐ Sociala välfärdsdata
☐ Personliga egenskaper, utbildning och arbete
☒ Tekniska metadata
☒ Annat: i fritextfält kan eventuellt andra personuppgifter förekomma även om syftet med fritext fälten inte är avsett för detta ändamål

Beskriv och kommentera ditt svar nedan:

Anställd – Namn, typ av insats från förbundet Deltagare – Namn

1.13 Kategorier av registrerade

Vilka kategorier av registrerade finns i registret/behandlingen?

☒ Anställda (coacher)
☐ Kunder
☐ Leverantörer
☐ Besökare
☐ Elever
☐ Patienter
☐ Medlemmar
☐ Medborgare
☐ Konsulter
☐ Asylsökande
☒ Personer med funktionsvariation
☒ Deltagare

Beskriv och kommentera ditt svar nedan:

Deltagande individer i arbetsrehabiliteringen

1.14 Antal registrerade

Hur många registrerade inkluderas i behandlingen?

☒ 1–100
☐ 101–1000
☐ 1001–5000
☐ 5001–10000
☐ 10001–50000
☐ 50 001 <
☐ Annat

Beskriv och kommentera ditt svar nedan:

Anställda – minst 8 Deltagare – minst 12

1.15 Publikt tillgängliga uppgifter

Är någon data redan publikt tillgänglig?
OBS: Om personuppgifterna redan är insamlade, var de publikt tillgängliga vid tiden för insamlingen?

☐ Ja
☒ Nej

1.16 Tillgång till personuppgifter

Vilka tjänstemän och andra roller kommer ha tillgång till uppgifterna?

☐ En person
☒ Ett fåtal handläggare
☐ Personal inom enheten
☐ Personal inom förvaltningen
☐ Personal inom kommunen
☐ IT-administratörer
☒ Leverantör
☐ Annat

Beskriv och kommentera ditt svar nedan:

Coacher kommer åt sin/sina deltagare Leverantören har åtkomst men går enbart in på individnivå på begäran av PUA

1.16.1 Tillgång till personuppgifter (omfattning)

Ange hur många anställda som kommer ha tillgång till hela och de olika delarna av behandlingen om det är relevant.

Anställda – minst 8

1.17 Lagring (Informationsredovisning)

Gallringsbeslut i informationsredovisningen (eller dokumenthanteringsplanen) anger tidsgränser för data som ska bevaras, rensas eller gallras.

Ange punktnotation och rubrik enligt klassificeringsstruktur nedan.

När coachningen är avslutad raderas deltagaren och datan anonymiseras och används enbart för statistik

1.18 Sekretess (OSL och andra bestämmelser)

Innehåller behandlingen sekretessreglerade uppgifter?

Uppgifter kan vara reglerade i offentlighets- och sekretesslagen och därför extra skyddsvärda. Exempelvis en persons ekonomiska förhållanden.

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

2 Personuppgifter, känslighet och behandlingens karaktär

2.1 Känsliga personuppgifter (art 9)

Behandlas känsliga personuppgifter?

Känsliga uppgifter är sådana uppgifter som kan skada en individs integritet i stor utsträckning om de görs tillgängliga, och som därför behöver extra skydd. Det är inte tillåtet att behandla känsliga uppgifter, förutom i undantagsfall. Känsliga personuppgifter kallas "särskilda kategorier av personuppgifter" i Dataskyddsförordningen.

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

2.1.1 Ange vilka känsliga personuppgifter som behandlas

☐ Etniskt ursprung
☐ Politiska åsikter
☐ Religiös eller filosofisk övertygelse
☐ Medlemskap i fackförening
☒ Hälsa
☐ Sexualliv eller sexuell läggning
☐ Genetiska uppgifter
☐ Biometriska uppgifter

2.1.2 Rättslig grund - känsliga (art 9)

Vilken eller vilka av följande rättsliga grunder gäller för behandlingen?

☒ Den registrerade har lämnat ett uttryckligt samtycke
☐ Skyldigheter inom arbetsrätt, social trygghet och socialt skydd
☐ Skyldigheter inom ramen för ett kollektivavtal
☐ Skydda någons grundläggande intressen (exempelvis livshotande)
☐ Behandlingen sker inom en ideell organisation[2]
☒ En person har själv offentliggjort de känsliga uppgifterna
☐ Fastställa, göra gällande eller försvara rättsliga anspråk.
☐ Viktigt allmänt intresse
☐ Förebyggande hälso- och sjukvård och yrkesmedicin
☐ Bedömningen av en arbetstagares arbetskapacitet
☐ Kunna ställa medicinska diagnoser
☐ Tillhandahållande av hälso- och sjukvård eller behandling
☐ Social omsorg eller förvaltning av social omsorg, hälso- och sjukvårdstjänster samt deras system.
☐ Folkhälsoområdet (även förhindra smittspridning)
☐ Arkivändamål i allmänt intresse
☐ Forskningsändamål
☐ Statistiska ändamål
☐ Annat ändamål

Beskriv och kommentera ditt svar nedan:

Individen lämnar uppgifterna på frivillig basis.

2.2 Extra skyddsvärda personuppgifter

Inkluderar behandlingen någon av nedan kategorier av skyddsvärda uppgifter?

☒ Ja
☐ Nej

Om JA, Ange vilka typer av uppgifter som behandlingen omfattar:

☒ Inloggningsuppgifter
☐ Skyddad identitet
☐ Positioneringsdata
☐ Finansiella data
☐ Uppgifter om barn
☐ Löneuppgifter
☐ Uppgifter om lagöverträdelser
☒ Information som rör någons privata sfär

[2] Undantaget gäller en Ideell organisation med politiskt, filosofiskt, religiöst eller fackligt syfte i relation till sina medlemmar, tidigare medlemmar och vissa andra personer som organisationen har regelbunden kontakt med relaterat till detta syfte (till exempel kyrkobesökare, bidragsgivare och hjälpmottagare)

☒ Beteende och preferenser, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
☒ Uppgifter om sociala förhållanden
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Skyddad identitet – kommer utredas ifall det inte hanteras i insatsen.

2.3 Beskrivning av användning av känsliga och/eller extra skyddsvärda PU

Ange i vilken omfattning som känsliga personuppgifter förekommer i behandlingen:

☒ I specifika fält
☒ I löpande text
☒ I begränsad omfattning
☐ I stor omfattning

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

2.4 Utvärdering eller poängsättning

Inkluderar behandlingen utvärdering eller poängsättning?

Detta inbegriper att profilera eller förutsäga beteende, särskilt aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar.

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Aktiviteter som gör att deltagarna ska få hjälp att uppnå uppsatta mål. Deltagarna själva bedömer sin egen prestation. Typ av poäng utifrån antal genomföra aktiviteter. Instrument att skräddarsy för deltagaren. Allt är frivilligt för deltagarna.

2.5 Automatiskt beslutfattande

Inkluderar behandlingen användning av automatiskt beslutsfattande?

Behandling som har liten eller ingen påverkan på enskilda uppfyller inte detta särskilda kriterium.

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

2.6 Systematisk övervakning

Inkluderar behandlingen användning av systematisk övervakning? Systematisk övervakning innebär att observera, övervaka eller kontrollera registrerade eller samla in i situationer där de registrerade kanske inte är medvetna om vem som samlar in deras uppgifter eller hur de kommer att användas.

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

2.7 Samkörning av uppgifter

Inkluderar behandlingen en samkörning av uppgifter från två eller flera behandlingar?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

2.8 Uppgifter om sårbara eller i beroendeställning

Inkluderar behandlingen sårbara individer eller personer i beroendeställning?

Innehåller behandlingen personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter.

☒ Ja
☐ Nej

Om JA, Ange vilka sårbara individer eller personer i beroendeställning som behandlingen omfattar:

☒ Anställda
☐ Barn
☒ Personer med psykisk ohälsa
☐ Asylsökande
☐ Äldre personer
☐ Patienter
☐ Ej tillämpligt
☒ Deltagare

Beskriv och kommentera ditt svar nedan:

Deltagarna står långt från arbetsmarknaden och har komplexa behov, de kan exempelvis ha psykisk ohälsa. Varken app eller coach behandlar diagnos.

2.9 Ny teknik eller innovativa organisatoriska lösningar

Inkluderar behandlingen innovativ användning eller tillämpning av nya tekniska eller organisatoriska lösningar?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Nytt sätt att coacha med digitalt verktyg.

2.10 Begränsning av rättigheter

Hindrar behandlingen registrerade från att utöva en rättighet, använda en tjänst eller ett avtal?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3 Ansvarsskyldighet (efterlevnad av principer)

I detta avsnitt ska det beskrivas hur behandlingen tar hänsyn till de grundläggande principerna som finns för behandling av personuppgifter. Detta avsnitt syftar till att personuppgiftsansvarig ska kunna beskriva och visa hur den fullgör sin ansvarsskyldighet enligt art. 5.2 GDPR.

3.1 Laglighet (Ändamålsbegränsning)

Vilka åtgärder har utförts för att försäkra att insamlade uppgifter endast används för specifika, tydliga, och lagliga ändamål?

☒ Ändamålet för varje personuppgift identifieras innan insamlingen
☒ Det specifika ändamålet för varje personuppgift dokumenteras
☒ Personuppgifter samlas aldrig in enbart för att ”de är bra att ha”.
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Deltagarna kan själva skriva i fritextfält. De blir informerade om hur fritextfälten är avsedda att användas innan de börjar använda appen.

3.1.1 Ytterligare ändamål

För vilka ytterligare ändamål behandlas personuppgifter? Beskriv här om uppgifterna även kommer att användas inom någon annan verksamhet hos personuppgiftsansvarig.

☐ Arkivändamål av allmänt intresse
☐ Vetenskapliga eller historiska forskningsändamål
☒ Statistiska ändamål
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Om ytterligare behandlingar inte utförs, välj "Ej tillämpligt".

Beskriv och kommentera ditt svar nedan:

Personuppgifterna anonymiseras om de används för statistiska ändamål och lärande.

3.1.2 Automatiskt beslutfattande (rättslig grund)

Vilken av följande rättsliga grunder tillåter användning av data för automatiskt beslutsfattande?
(Hänvisning till fråga om automatiskt beslutsfattande ovan)

☐ Ingående eller fullgörande av ett avtal
☐ Beslutsfattandet tillåts enligt en lag som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen
☐ Den registrerades uttryckliga samtycke
☒ Ej tillämpligt

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3.2 Korrekthet

Vilka åtgärder har utförts för att försäkra att behandlingen utförts korrekt (på ett juste/rättvist sätt)?

☒ Standardinställningar för användare är från början satt till högsta skydd
☒ Användare informeras om standardinställningarna och hur man ändrar dem
☒ Integritetsfunktioner, inställningar och relaterade funktioner är tydliga, framträdande, lättillgängliga och användarvänliga
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3.3 Öppenhet (transparens)

Får registrerade individer information om behandlingen?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Individerna får information i samband med att de skriver avtal innan påbörjad behandling av personuppgifter. Information finns även att tillgå i appen.

3.3.1 Kriterier för information

Uppfyller informationen till registrerade samtliga kriterier nedan?

☒ Koncis och transparant
☒ Begriplig och lättillgänglig
☒ Tydligt och enkelt språk
☒ Presenteras i skriftlig form eller på annat sätt
☒ Kostnadsfritt
☐ Inte säker
☐ Ej tillämpligt

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3.3.2 Åtgärder för transparens

Vilka åtgärder har införts för att försäkra att uppgifterna är behandlade på ett transparent sätt?

☒ Användare får information om vem som samlar in/använder deras uppgifter
☒ Användare har möjlighet att rapportera problem/bekymmer
☒ Användare har tillgång till en inställningspanel/funktion för sekretess
☒ Visualisering med symboler används för att hjälpa till med tydlighet
☒ Information om integritet presenteras i lager eller flikar
☐ Certifiering, sigill och märkningar används för att visa transparens
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3.3.3 Samtycke

Valde du samtycke som laglig grund för behandlingen under *0 ovan*?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3.4 Uppgiftsminimering

Vilka åtgärder har tagits för att försäkra att insamlingen är begränsad till uppgifter som enbart är lämpliga och relevanta för ändamålet?

☐ Verifikation sker på att tillräckliga och relevanta uppgifter samlas in
☒ Endast nödvändiga personuppgifter samlas in och sparas
☐ Dataöverföring begränsas till vad som är minimalt nödvändigt
☐ Rutiner för automatisk blockering och radering finns
☒ Frivilliga och obligatoriska fält är definierade i formulär
☒ Fritextfält styrs med tydlig policy
☐ Definierade fält (t.ex. färdiga svarsalternativ) används framför fritextfält
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3.5 Riktighet och kvalitet vid insamling

Vilka åtgärder har tagits för att säkerställa personuppgifternas kvalitet vid insamling?

☒ Individen lämnar själv uppgifterna och kan ändra vid behov
☐ Uppgifterna hämtas från Skatteverket eller liknande databas och anses vara korrekta
☐ Rutiner inkluderar regelbunden kontroll av att personuppgifter som insamlas är riktiga och håller god kvalitet
☐ Valideringskontroller för att upptäcka inkonsekvent, icke komplett, och felaktiga uppgifter
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3.6 Riktighet och kvalitet – löpande

Vilka åtgärder har vidtagits för att säkerställa att uppgifter kontinuerligt är riktiga och uppdaterade?

☒ Individen lämnar själv uppgifterna och kan ändra vid behov
☐ Uppgifterna uppdateras från Skatteverket eller liknande databas och anses vara korrekta
☐ Löpande kontroller av personuppgifters riktighet och kvalitet
☐ Valideringskontroller för att filtrera ut gamla personuppgifter
☒ Gamla personuppgifter raderas eller uppdateras
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Coachen hanterar när en deltagare skrivs ut.

3.7 Lagringsminimering

Vilka åtgärder har du tagit för att försäkra att personuppgifter inte lagras längre än nödvändigt?

☒ Processer finns för granskning och gallring av personuppgifter
☐ Kriterier med trigger är implementerade och radering sker systematiskt
☒ Personuppgifter begränsas eller raderas när en registrerad är inaktuell
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Coachen hanterar när en deltagare skrivs ut, personuppgifterna finns enbart kvar en begränsad tid innan radering sker.

3.8 Integritet och konfidentialitet

3.8.1 Klassning

Har ni informationssäkerhetsklassat behandlingen?

☐ Ja
☒ Nej

Om en klassning i enlighet med SKR:s KLASSA har gjorts kan nedan övergripande klassning anges. Behandlingen kan klassas utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet, i enlighet med den organisationsövergripande klassningsmodellen. Ange alltså vilken informationssäkerhetsklassning som behandlingen har och inte informationsbärarens/systemets säkerhetsklassning. Värdena ska anges för respektive fält nedan.

Värdera behandlingens Konfidentialitet (K)

☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4

Värdera behandlingens Riktighet (R)

☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4

Värdera behandlingens Tillgänglighet (T)

☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4

Beskriv eller kommentera klassningen:

Informationsklassning ska göras senast 2022

3.9 Proportionalitet och nödvändighet

Proportionalitet och nödvändighet innebär att behandlingen och dess eventuella inskränkningar i den enskildes personliga integritet – med hänsyn till skyddsåtgärder – är proportionell mot det eftersträvade syftet och att de registrerades grundläggande rättigheter och intressen säkerställs.

3.9.1 Proportionell (nytta minus risker)

Är nyttan med behandlingen proportionell mot de nackdelar, risker och problem som behandlingen leder till eller kan leda till för enskildas personliga integritet?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Nytta: genom att bidra med en strukturerad digital kommunikationsväg ges deltagarna möjlighet att kommunicera och ges motivation på ett sätt som många unga deltagare föredrar och ibland särskilt för deltagare med NPD funktionsvariation. Appen är byggd utifrån principen privacy by design. Kryptering används. Appen bidrar med ett alternativ till kommunikation och uppföljning som också kan erbjudas på ett analogt sätt om så önskas. **Nackdelar/risker/problem:** Risker finns med att fritextfält på sätt de inte är avsedda. Instruktioner och rutiner är framtagna för användandet. Behörighetsstyrning finns. Uppgiftsminimering.

3.9.2 Nödvändig

Finns det ett annat sätt att uppnå samma resultat?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

3.9.3 Bedömning intresseavvägning

Valde du intresseavvägning som svar på rättslig grund under *0 ovan*?

☐ Ja

☒ Nej

Nej är förvalt. *En myndighet kan inte använda intresseavvägning i sin myndighetsutövning. I stället används* ***allmänt intresse*** *vid exempelvis hantering av anställdas information eller behandlingar som sker säkerhetsändamål.*

4 Individers rättigheter

4.1 Tillämpliga rättigheter

I artiklarna 12–21 GDPR finns det rättigheter för den enskilde. Vilka artiklar blir aktuella av den aktuella behandlingen?

☒ Art. 12 – Informationspolicy om hur personuppgifter behandlas
☒ Art. 13 – Informationsskyldighet när enskild lämnat uppgiften
☒ Art. 14 - Informationsskyldighet när annan än enskild lämnat uppgiften
☒ Art. 15 – Registerutdrag
☒ Art. 16 – Rättelse
☒ Art. 17 – Radering
☒ Art. 18 – Begränsning av behandling
☒ Art. 19 – Anmälningsskyldighet till mottagare
☐ Art. 20 – Dataportabilitet
☒ Art. 21 – Invändning

Beskriv och kommentera ditt svar nedan:

Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter.

4.2 Administrativa åtgärder för rättigheter

Beskriv vilka administrativa åtgärder har bedömts behövas för att säkerställa att de registrerades rättigheter tillvaratas.

Informationspolicy finns framtagen Dataskyddsombud inom Samordningsförbundet Stockholms Stad är förbundets administrativa stöd i personuppgiftsfrågor som rör dataskyddsförordningen och hanterar registrerades rättigheter för förbundets räkning.

4.3 Tekniska åtgärder för rättigheter (PbD)

Beskriv vilka tekniska åtgärder som behöver vara inbyggda i systemet/tjänsten för att säkerställa att de registrerades rättigheter tillvaratas.

Informationsflöde i appen, få hjälp och support

5 Tredjelandöverföring

5.1 Förekomst

Överförs personuppgifter till tredjeland eller internationell organisation?

Det finns strikta regler i dataskyddslagstiftningen för när personuppgifter får lämnas till länder utanför EU/EES, så kallat tredjeland. Detta gäller all överföring, även till personuppgiftsbiträden som inte själva använder personuppgifterna i sin verksamhet utan bara lagrar, driftar, supportar, utvecklar, underhåller eller servar systemet. Observera att ordet överföring även omfattar åtkomst till personuppgifterna i tredjeland, även om de lagras inom EU/EES.

☒ Ja
☐ Nej

Ange vilket tredjeland och mottagare

Uppgifterna lagras i Microsoft Azure på servrar inom EU, utredning pågår för flytt av lösningen till svenska servrar. Microsofts datacenter i Sverige öppnades och är tillgängliga från 16 november 2021.

Mottagaren kan vara en extern verksamhet eller ett företag inom koncernen som finns utanför EU/EES. Vem mottagaren är kan vara av intresse bland annat för vilka avtal som ska ingås. Exempel: "Biträde X i USA", "Intern verksamhet Y i Japan", "Internationell organisation Z". Exempelvis är M365 är en SaaS-tjänst som levereras av Microsoft. Lagring sker inom EU men överföring av vissa data sker till tredjeland, dvs. Microsoft i USA samt Microsofts underbiträden.

5.2 Grund för tredjelandsöverföring

På vilka grunder sker överföringen till tredjeland eller internationell organisation?

☒ EU-kommissionens standardavtalsklausuler (SCC)
☐ Bindande företagsbestämmelser (Binding Corporate Rules, BCR)
☐ EU-kommissionen har godkänt mottagandet som har ansetts ha en godkänd skyddsnivå
☐ Godkänd certifieringsmekanism
☐ Godkänd uppförandekod
☐ Eget avtal mellan parterna som godkänts av tillsynsmyndigheten
☐ Viktigt allmänintresse
☐ Avtal med den registrerade
☐ Rättsliga anspråk
☐ Samtycke
☐ Annat

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

6 Personuppgiftsbiträden (PUB)

6.1 Extern drift

Sköts delar av driften av behandlingen externt för informationsbärare (system)?

☒ Ja
☐ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

6.2 Omfattning

Anlitas personuppgiftsbiträde för hela eller delar av behandlingen?
☒ Ja
☐ Nej

Om Ja beskriv kort i vilka delar av behandlingen.

Klicka eller tryck här för att ange text.

6.3 Personuppgiftsbiträdesavtal (PUB-avtal)

Bifoga det avtal alt. det förslag som finns mellan personuppgiftsansvarig och personuppgiftsbiträdet.

Ska tas fram

6.4 Instruktioner

Bifoga de instruktioner alt. det förslag som finns mellan personuppgiftsansvarig och personuppgiftsbiträdet.

Tas fram i samband med PUB-avtal

6.5 Leverantörskontroll

Har en egen leverantörskontroll genomförts för att granska leverantörens efterlevnad av informationssäkerhet och dataskydd?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

6.6 Har PUB egna syften?

Beskriv om personuppgiftsbiträdet avser att behandla uppgifterna för något eget syfte, både som rådata, eller efter anonymisering av personuppgifterna.

Nej

6.7 Underbiträde

Har PUB redovisat vilka underbiträdesavtal som är tecknade?

☐ Ja
☒ Nej – Tas fram i samband med PUB-avtal

7 Delning

Utlämnande till tredje part
Lämnas några personuppgifter ut till tredje part?

☐ Ja
☒ Nej

Om Ja, Ange mottagare:

(Microsoft under utredning)

7.1 Informationsskyldighet (lag, förordning eller föreskrift)

Finns det någon skyldighet för personuppgiftsansvarig att lämna uppgifter till någon annan myndighet eller organisation enligt lag, förordning eller föreskrift?

☐ Ja
☒ Nej

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

8 Övrigt

8.1 Certifieringar eller uppförandekoder[3]

Känner du till några godkända certifieringar eller branschspecifika uppförandekoder som leverantören följer? (Code of conduct)

☐ Ja
☒ Nej

Nej är förvalt. Det är mycket ovanligt med godkända certifieringar uppförandekoder.

[3] Certifieringar och branschspecifika uppförandekoder är utarbetade av organisationer eller andra representativa organ och är giltiga om de är godkända av en tillsynsmyndighet i EU, europeiska dataskyddsnämnden (EDPB) eller EU-kommissionen för att uppfylla GDPR-efterlevnad.

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

9 Risker och åtgärder

Risker beskrivs nedan i en övergripande dokumentation av identifierade risker, samt tekniska och organisatoriska åtgärder. Nedan steg från 9.1 till 9.7 skall alltså ses som ett resultat av riskhanteringsprocessen och ger en övergripande tydlighet av risker som hanterats och är samtidigt ett stöd till de aspekter som riskhanteringen behöver omfatta. 9.8 ger en sammanfattning av de viktigaste riskerna som bedömts, åtgärder och kvarvarande risker.

Själva riskbedömningen kan också genomföras och dokumenteras i en bilaga (Excel eller annat dokument). Referera då till det aktuella riskdokumentet och summera de viktigaste riskerna under 9.8

Infoga riskdokument:

Riskidentifiering och riskanalys för Digital egenmakt

9.1 Riskidentifiering

Riskerar den registrerade att utsättas för någon eller några av följande skador som orsakats av behandlingen eller som konsekvens av en personuppgiftsincident?

☐ Diskriminering
☐ Identitetsstöld
☐ Bedrägeri
☐ Ekonomisk förlust
☒ Påverkan på rykte
☒ Förlust av konfidentialitet
☐ Anonymisering röjs av obehörig
☐ Betydande påverkan på det ekonomiska och sociala förhållandet
☐ Förlust av mänskliga fri- och rättigheter
☐ Förhindra individers kontroll över sina uppgifter
☒ Sannolikt sker ingen skada till följd av behandlingen
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

9.2 Riskkällor

Vilka potentiella källor finns som kan orsaka dessa skador?

☐ Dataintrång
☒ Antagonist
☐ Kriminalitet

☐ Bristande övervakning
☒ Bristfällig policy/tillvägagångsätt
☐ Oskyddad lagring
☐ Brist på ansvarsskyldighet
☐ Brist på experter inom ämnet/ämneskompetens
☐ Otillräcklig testning
☒ Otillräcklig utbildning/övning/träning
☐ Driftstörning, haveri
☐ Inte säker
☐ Ej tillämpligt
☐ Annat – Brist på resurser och tid

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text vid behov.

9.3 Riskgrupper

Vilka specifika grupper av individer risker att skadas?

☒ Brukare
☐ Entreprenörer
☒ Anställda/Medarbetare
☐ Arbetssökande
☐ Asylsökande
☐ Patienter/Vårdboende
☐ Besökare
☐ Studenter
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv och kommentera ditt svar nedan:

Klicka eller tryck här för att ange text.

9.4 Riskperspektiv

Hur kan dessa potentiella skador uppfattas av de registrerade?

Klicka eller tryck här för att ange text.

Om detta inte kan förutses, bör en de registrerades tillfrågas för att ge sin uppfattning om behandlingen.

9.5 Tekniska säkerhetsåtgärder

Vilka tekniska åtgärder har införts i syfte att minska eller eliminera de risker som identifierats under *Riskidentifiering* ovan?

☐ Autentisering
☐ Anti-malware

☐ Detekteringsverktyg för personuppgiftsincidenter (Data Breach)
☒ Säkerhetskopiering (backup)
☒ Kryptering vid överföring
☒ Kryptering vid vila
☐ Brandväggar (blockering av vissa portar)
☐ Informationsskydd (Microsoft Information Protection) i 365
☐ Loggning
☐ Logisk kontroll av åtkomst
☐ Flerfaktorsautentisering (MFA)
☐ Managerade enheter
☐ Nätverksautentisering
☐ Pseudonymisering (Anonymisering)
☒ Regelbundna mjukvaruuppdateringar (Patchning)
☐ Detekteringsverktyg för sårbarheter
☐ Mobile Application management (MAM)
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv eller kommentera vilka tekniska skyddsåtgärder som behövs för att säkerställa en lämplig säkerhetsnivå:

Klicka eller tryck här för att ange text.

9.6 Administrativa åtgärder

Vilka administrativa åtgärder har genomförts för att reducera eller eliminera de risker som identifierats under *Riskidentifiering* ovan?

☒ Riktlinjer för dator- och mobilanvändning
☒ Utbildning och informationsinsatser
☐ Kontinuitetsplan
☒ Incidenthanteringsplan
☐ Katastrofberedskap (Disaster recovery plan)
☐ Behovsenlig behörighet (Need-to-know)
☐ Sekretessavtal
☒ Avtalsmässiga åtgärder (Instruktioner etc)
☐ Lösenordspolicy
☐ Penetrationstestning
☐ Säkra lokaler
☐ Tillsyn/interna kontroller
☐ Övervakning
☐ Simulerings- och krisövningar
☐ Bakgrundskontroller
☐ Säker radering
☒ Åtkomstkontroll
☒ Personuppgiftsbiträdesavtal
☐ Leverantörskontroller
☐ Inte säker
☐ Ej tillämpligt
☐ Annat

Beskriv eller kommentera vilka administrativa skyddsåtgärder som behövs för att säkerställa en lämplig säkerhetsnivå:

Klicka eller tryck här för att ange text.

9.7 Inbyggt dataskydd – Privacy by Design (art 25, 26)

Beskriv hur behandlingen tar hänsyn till principen om inbyggt dataskydd i artiklarna 25 och 26?

Inbyggt dataskydd och dataskydd som standard med mål att säkerställa att processer och system är utformade så att inhämtande och behandling (inklusive användning, utlämnande, bevarande, överföring och radering) begränsas till det som är nödvändigt för det identifierade ändamålet.

I bilaga Myli Architechture beskrivs inbyggt dataskydd på följande sätt under stycket *Data security*:

Data security

Users will be logged in via BankId as a 2-way authentication. All communication between Myli components are encrypted with SHA-2 SSL encryption. Person identified data is stored only in Identity and Patient databases. In all other Micro services and databases the user is identified as a unique guid. Person identified Columns in Identity and Patient are protected by encryption or Dynamic Data Masking.

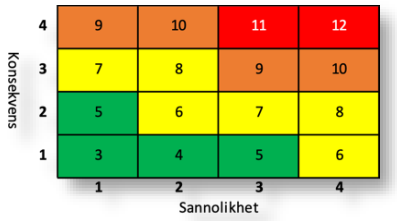
9.8 Sammanfattning av riskbedömning

Riskhanteringen ger en bedömning av konsekvenser av risker och sannolikhet för att de ska inträffa.

Den påverkan för individen som kan bli följden av en situation bör bedömas med hänsyn tagen till konsekvenser som förlust av konfidentialitet, riktighet eller tillgänglighet rörande tillgångarna. Sannolikheten är hur frekventa hoten är och hur enkelt sårbarheterna kan utnyttjas.

Bedömning av konsekvens sker i en skala mellan 1 till 4.
Bedömning av sannolikhet sker i en skala mellan 1 till 4.
Riskvärdet räknas ut i analysen och sker enligt formeln Sannolikhet + konsekvens x 2.

Det är detta riskvärde som används vid prioritering av åtgärder i riskbehandlingen.



Sammanfattning av risker:

14 risker har identifierats. Två av dessa risker värderades inte eftersom den ena risken inte ansågs vara en risk i nuläget på grund av att funktionen radering inte ännu är framtagen och den andra risken angående PUB avtal med Microsoft inte ansågs vara aktuell.

Generellt värderades de identifierade riskerna relativt lågt. Utav de 12 värderade riskerna var det sju risker som hamnade i kategorien gul, vilket generellt innebär att riskerna ska bevakas och planeras åtgärder för. Fem av riskerna hamnade i kategorin grön, vilket generellt innebär att risker som anses hanterade eller inte behöver hanteras.

Av de sju risker som hamnade på ett riskvärde mellan sex och åtta (riskvärde gul) fastslogs åtgärder och ytterligare en riskvärdering gjordes. Riskvärde efter åtgärd hamnade på mellan 3–5 vilket är i kategorin grön, vilket innebär att åtgärderna ansågs minska på sannolikhet eller konsekvensen av själva risken.

De risker som från början värderades till ett lågt riskvärde (grön), valdes att inte gå vidare med under workshoppen. Några risker finns det planer för åtgärder, vilket framkom i diskussionen vid första riskvärderingen.

För några av de identifierade riskerna har projektet redan tagit fram åtgärder vilket gör att risken inte längre kvarstår.

9.9 Risker med högst riskvärde

Nedan är en sammanfattning av de riskerna med högst riskvärde.

Beskrivning av tabell:

Sannolikhet (Sa) 1–4, Osannolikt, Möjlig, Sannolik, Mycket Sannolik (se Appendix 7.2 för definitioner)
Konsekvens (Ko) 1–4, Försumbar, Måttlig, Allvarlig, Mycket allvarlig (se Appendix 7.1 för definitioner)
Riskvärde (Rv) är en sammanlagd bedömning av sannolikhet och konsekvens och är ett stöd för prioritering av risker

#	**Beskrivning**	Riskvärde före åtgärd	Åtgärder för riskhantering	Kvarvarande risk
R1	Namn på risk **Coach råkar skriva till fel deltagare** *Risk för …* Coach skriver till fel deltagare och råkar avslöja uppgifter om en annan deltagare *…på grund av…* Det är inte tydligt vem man skriver med eftersom deltagarna kan namnge sig med ett smeknamn och det finns ingen profil-bild. Blandar ihop namnen, fysiskt svårt se vart information hör till - visuell osäkerhet *… vilket leder till …* Coachen råkar avslöja information om en annan deltagare, för-troendetapp, sekretessbrott	Sa: 2 Ko: 3 Rv: 8	Har gjort tydligare: visuellt i appen – det står deltagares namn hela tiden i chatten, chattar med namn	Sa: 1 Ko: 2 Rv: 5

R2	Namn på risk **Deltagare "Lättar på sitt hjärta"** *Risk för …* Deltagare skriver om mycket personliga saker som ligger utanför behandlingens ändamål. *…på grund av…* Det finns inga tekniska begränsningar för vad en deltagare kan skriva om *… vilket leder till …* Det finns ingen rättslig grund för att behandla uppgifterna och personuppgifterna ges inte tillräckligt skydd	Sa: 3 Ko: 2 Rv: 7	Informera coacher, ge tydliga instruktioner, muntlig och skriftlig instruktion, som ett "körkort". Funktion att ta bort chatt som deltagare Funktion ta bort chatt - inte först, slutet av 2022 Instruktion - inför införandet	Sa: 1 Ko: 1 Rv: 3
R3	Namn på risk ***Otydligt hur appen kan användas i efterhand*** *Risk för …* *…på grund av…* *… vilket leder till …* Fel info är kvar, kontot är stängt och inte tillgängligt för coachen. Manuell hantering av My indicators idag,	Sa: 1 Ko: 3 Rv: 7	Lista med avslutade coacher, påminnelser att avsluta konto/koppling till deltagare. Rutin för uppstart och avslut	Sa: 1 Ko: 2 Rv: 5

R4	Namn på risk **Avbrott i appen/appens funktioner** *Risk för …* Appen fungerar inte när deltagare och coacher behöver använda den *…på grund av…* Överbelastning - för dålig kapacitet och mobilens täckning *… vilket leder till …* Deltagare blir irriterade. Deltagare vill inte längre använda appen	Sa: 2 Ko: 2 Rv: 6	Övervakar löpande - och anpassar efter behov. Prestandadimension	Sa: 1 Ko: 1 Rv: 3
R5	Namn på risk **Oklart om appen innehåller hälso- och sjukvårdsuppgifter** *Risk för …* Krav på säkerhet och lagring enligt patientdatalagen inte uppfylls *…på grund av…* Otydligt om informationen klassificeras som hälso- och sjukvårdsuppgifter *… vilket leder till …* Personuppgifter ges inte tillräckligt skydd och lagras felaktigt	Sa: 2 Ko: 2 Rv: 6	Informera coacher, ge tydliga instruktioner, muntlig och skriftlig instruktion, som ett "körkort". Funktion att ta bort chatt som deltagare	Sa: 1 Ko: 2 Rv: 5

R6	Namn på risk **Ändamålet med behandlingen förändras** *Risk för …* **Ändamålet förändras i och med att användningsområdena i appen utökas** *…på grund av…* Ytterligare apputveckling sker efter testperioden *… vilket leder till …* Behandlingen sker inte enligt ändamål, de grundläggande principerna i dataskyddsförordningen uppfylls ej	Sa: 2 Ko: 2 Rv: 6	Vara transparent, uppdatera informationsmaterialet regelbundet och inför nya uppdateringar. Informera deltagare om nya/utökade behandlingar. Gör en riskbedömning inför uppdateringar som ändrar personuppgiftsbehandling	Sa: 1 Ko: 2 Rv: 5

R7	Namn på risk **Byte av coach skulle kunna innebära informationsförlust** *Risk för …* Inte få med information när deltagare byter coach *…på grund av…* Oklart hur deltagare får med sig sin information när de byter coach – idag finns ingen automatisk överföring av konversationer och anteckningar i appen *… vilket leder till …* Information inte är tillgänglig via appen	Sa: 2 Ko: 2 Rv: 6	En överlämning mellan coacher - lämpligt ta fram en rutin för detta, informera om vad som händer vid byte av coach, instruktion för coacher – informationsmaterial (en för coach och en för deltagare, med tydliga syften, för olika processer och tips för hur appen ska användas)	Sa: Ko: Rv:

R8	Namn på risk **Datatrafiken avlyssnas av obehörig aktör** *Risk för …* Obehöriga kan ta del av uppgifter i appen *…på grund av…* Molnlösningar, webbaserat system *… vilket leder till …* Personuppgifter blir röjda och deltagarna kan känna sig kränkta. Det blir en personuppgiftsincident	Sa: 1 Ko: 2 Rv: 5	kryptering på trafik och lagring, alternativa lösningar on prem – kostnads åtgärder.	Sa: Ko: Rv:
R9	Namn på risk **Historik kring aktivtiter försvinner** *Risk för …* Historiken över deltagares resultat från aktiviteter försvinner *…på grund av…* Tekniska brister, haveri, servrar som kraschar *… vilket leder till …* Deltagare förlorar dokumentation över sin prestation.	Sa: 1 Ko: 2 Rv: 5	Diskussion: I molntjänst är risken liten - hög redundans, risken blir större om driften måste flyttas till on prem	Sa: Ko: Rv:

R10	Namn på risk **Inaktiva deltagare sparas för länge** *Risk för …* Inaktiv deltagare har inte tagits bort efter att coachningen är klar *…på grund av…* Oklart hur radering av inaktiva deltagare ska fungera *… vilket leder till …* Uppgifter om den inaktiva deltagaren lagras för länge	Sa: 1 Ko: 2 Rv: 5	Diskussion och åtgärder: dela upp risken: aktiv/inaktiv deltagare: finns inte funktion nu för att radera deltagare. Fokus på inaktiva deltagare - efter hur lång tid ska uppgifter sparas? Återaktivering ska vara en möjlighet. Aktivera/inaktivera coachning - ta del av uppgifterna efter deltagandet - radering från appen, aktiviteter - sammandrag för utvecklingssyften - anonymiserade data kvar - informera om detta till deltagare innan start	Sa: Ko: Rv:

R11	Namn på risk **Uppgifter delas hemligt med amerikanska myndigheter** *Risk för …* Uppgifter delas hemligt med amerikanska myndigheter *…på grund av…* Amerikanskt ägt bolag används (Azure) *… vilket leder till …* Amerikanska myndigheter kan begära ut uppgifter baserat på Cloud Act och FISA	Sa: 1 Ko: 2 Rv: 5		Sa: Ko: Rv:
R12	Namn på risk **Telefon blir stulen/borttappad** *Risk för …* Obehöriga kommer åt uppgifter i appen *…på grund av…* Deltagare och coacher kan vara inloggade på appen när telefonen försvinner *… vilket leder till …* Personuppgifter blir röjda och deltagarna kan känna sig kränkta. Det blir en personuppgiftsincident	Sa: 2 Ko: 1 Rv: 4	Diskussion: Ska det vara enkelt att logga in i appen? Enkelhet i användandet av appen är viktig för målguppen. En avvägning. Många har lås på telefonen vilket påverkar sannolikheten. Åtgärder: Informera deltagare: Meddela coachen om att mobil är stulen - kan spärra kontot. I informationen: om man väljer "kom ihåg mig" kan rekommendera skalskydd på mobilen	Sa: Ko: Rv:

R13	Namn på risk **Coach kan ej försäkra att det är rätt person** *Risk för …* Familjemedlem eller annan anhörig skriver i deltagarens ställe och "styr" hens aktiviteter och kommunikation med coachen *…på grund av…* Det finns inget sätt att försäkra att coachen chattar med rätt person *… vilket leder till …* Deltagaren får inte det stöd hen behöver, felaktiga uppgifter samlas in	Sa:1 Ko: 1 Rv: 3	Diskussion: Anhöriga tror de hjälper, kanske egen app för anhörig? Deltagare kanske ber om hjälp, viktigt att informera om hur appen bör användas. Inga komplikationer om aktivitet/coachning inte följs, appen är inte enda kommunikationsvägen. MyIndicators har valt att inte nyttja BankID då de värderar möjligheten att vara anonym högre. Konsekvensen om denna risk värderas lättare i förhållande till anonymiteten. Detta då det även förs regelbundet analog dialog mellan coach och deltagare. Myli's avsedda användning är inte att behandla utan ett verktyg för egenmakt.	Sa: Ko: Rv:

9.9 Bedömning kvarvarande risk

Är de identifierade planerade åtgärderna som föreslås tillräckliga för att minska de identifierade riskerna till en nivå så att behandlingen *inte sannolikt leder till en hög risk för fysiska personers fri- och rättigheter*?

☒ Ja
☐ Nej

9.10 Förhandssamråd

Vid nej ovan så är den kvarvarande risken hög och IMY bör rådfrågas (artikel 36.1). För det fall ni inte lyckas avhjälpa alla allvarliga risker behöver ni söka förhandssamråd hos IMY innan behandlingen kan påbörjas. För förhandssamråd kräver IMY att verksamheten gjort en konsekvensbedömning och arbetat med riskminimering.

Har eller kommer ni begära förhandssamråd hos IMY[4]?

☐ Ja
☒ Nej

Om Nej, motivera

Klicka eller tryck här för att ange text.

[4] Integritetsskyddsmyndigheten (IMY), tidigare Datainspektionen

10 Bilagor

Här kan du ange om det utöver denna rapport finns ytterligare handlingar som har legat till grund för bedömningarna samt de handlingar som blir bilagor till denna rapport.

☐ Beskrivning av verksamhet,

Se bilaga Klicka eller tryck här för att ange text vid behov.

☒ Beskrivning av IT-system och/eller IT-säkerhet,

Myli Architechture

☐ Överenskommelse om direktåtkomst,

Se bilaga Klicka eller tryck här för att ange text vid behov.

☐ Personuppgiftsbiträdesavtal,

Se bilaga Klicka eller tryck här för att ange text vid behov.

☐ Registervårdsplan,

Se bilaga Klicka eller tryck här för att ange text vid behov.

☐ Informationsklassning av personuppgifterna.

Se bilaga Klicka eller tryck här för att ange text vid behov.

☐ Annat:

Se bilaga Klicka eller tryck här för att ange text vid behov.

☐ Specifika säkerhetsåtgärder:

Se bilaga Klicka eller tryck här för att ange text vid behov.

11 Referenser

Artikel 29-gruppen (2017) WP 248 rev. 01, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, antagna den 4 april 2017, senast reviderade och antagna den 4 oktober 2017 Länk

Artikel 29-gruppen (2018) WP251rev.01 Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679, antagna den 3 oktober 2017, senast reviderade och antagna den 6 februari 2018

Artikel 29-gruppen (2018) WP260rev.01 Riktlinjer om öppenhet enligt förordning (EU) 2016/679 Antagna den 29 november 2017, senast granskade och antagna den 11 april 2018

Artikel 29-gruppen (2013) WP 203 Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013

Artikel 29-gruppen (2014) WP 217, Yttrande 6/2014 om begreppet den registeransvariges berättigade intressen i artikel 7 i direktiv 95/46/EG, antaget den 9 april 2014

CNIL Commission Nationale de l'Informatique et des Libertés (2018) *Privacy Impact Assessment (PIA) 3 : knowledge bases* Länk

Integritetsmyndighetens (IMY) hemsida om konsekvensbedömning. Länk

European Data Protection Supervicer (EDPS) (2019) *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation*, v1.3 July 2019 Länk

International Standard Organisation -ISO (2017) *ISO/IEC 29134:2017 1 Information technology -- Security techniques -- Guidelines for privacy impact assessment.* Länk

12 Appendix 1 – Exempel på konsekvenser och sannolikheter

12.1 Konsekvenser [5]

Konsekvens-nivå	Generisk beskrivning	Exempel på skada		
		Fysisk	**Materiell**	**Moralisk**
1. Försumbar	Registrerade är inte påverkade eller har små besvär, som de kan komma över utan problem. T.ex personuppgifter som är allmänt tillgänglig (t.ex. i telefonböcker, adressböcker eller listor)	• Bristande omvårdnad (barn, en person beroende av hjälp) • Huvudvärk	• Tidsförlust på grund av formaliteter • Spam • Direktmarknadsföring • Riktad annonsering som konsument	• Ren skär irritation • Rädsla att tappa data • Känsla av obehag av närgångenhet • Smärre tidsförlust • Bristande respekt • Missade erbjudanden
2. Måttlig	Registrerade kan påverkas med tydliga besvär, som de kan komma över, trots vissa svårigheter. T.ex personuppgifter som kräver ett legitimt intresse för åtkomst (t.ex. begränsade offentliga filer eller medlemmarna i en distributionslista)	• Mindre fysisk påverkan (illamående, ångest) • Bristande omvårdnad som orsakar skada • Förtal som resulterar i psykisk eller fysiska symptom.	• Oväntade kostnader (böter, avgifter) • Ej access till tjänster • Missade möjligheter (karriär, semester) • Oönskad post som orsakar skada • Kostnadsökningar • Inkorrekt profilering • Exponering av hemliga uppgifter (graviditet, rehabilitering)	• Avstängning från en tjänst • Ärekränkning och försämrat rykte • Problem med professionella eller personliga relationer (bilder, skamfilning) • Känsla av intrång i privatlivet • Förolämpning på sociala medier
3. Allvarlig	Registrerade påverkas med betydande besvär, som de bör kunna komma över med mycket svårigheter och hjälp. T.ex personuppgifter vars obehöriga avslöjande kan påverka den registrerades rykte (t.ex. information om inkomst, socialförsäkringsförmåner, fastighetsskatt eller påföljder)	• Allvarlig fysisk påverkan som orsakar långsiktiga problem. • Handikapp och fysisk förändring som ett resultat av våld, olycka hemma eller på arbetet	• Bestående ekonomiska problem (måste låna) • Ej möjlighet att låna • Förlust av bostad, arbete, egendom • Separation • Finansiell förlust på grund av bedrägeri • Frysning av tillgångar • Nekad att studera, examen, utvisning	• Allvarliga psykiska problem (depression, fobier) • Känsla av intrång med bestående skada • Kränkning av grundläggande rättigheter (diskriminering, åsiktsfrihet) • Utpressning • Nätmobbning & trakasserier • Maktlöshet av att förlorat en process

[5] Enligt CNIL (Franska Tillsynsmyndigheten) Privacy Impact Assessment (PIA) samt ISO 29134 råd för konsekvensbedömning (Privacy impact assessment)

4 Mycket allvarlig	Registrerade påverkas med allvarliga besvär, eller oöverstigliga konsekvenser, som kanske inte kan komma över. T.ex personuppgifter vars obehöriga avslöjande, modifiering, förlust eller förstörelse kan påverka den registrerades existens eller hälsa, frihet och liv.	• Långsiktig påverkan med permanenta eller kronisk fysiska besvär • Död (mord, självmord, olycka) • Permanent funktionsnedsättning	• Förlust av bevis (rättsprocess) • Oförmåga att arbeta • Ej möjligt att flytta • Förlust av vital infrastruktur (vatten, el)	• Långsiktig eller permanent psykisk påverkan • Kriminell bestraffning • Förlust av familjeband • Förlust av myndighet eller förmyndarskap • Ej möjlighet att föra process

12.2 Sannolikhet

Sannolikheten för att varje hot utnyttjas bör uppskattas med hänsyn till sårbarheterna för behandlingar och deras stödsystem och kapaciteten hos riskkällor för att utnyttja dem (färdigheter, tillgänglig tid, ekonomiska resurser, närhet till informationssystem, motivation, känsla av straffrihet, etc.). Med andra ord, i vilken utsträckning kan egenskaperna för underlättande tillgångar utnyttjas för att utföra ett hot?

1. Osannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar inte möjligt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade i ett rum som skyddas av en kortläsare och åtkomstkod).

2. Möjlig: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara svårt för de valda riskkällorna (t.ex. stöld av pappersdokument som är lagrade i ett rum skyddat av en kortläsare).

3. Sannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara möjligt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade på kontor som inte kan nås utan att först kontrollera i receptionen).

4. Mycket Sannolikt: Att utföra ett hot genom att utnyttja sårbarheterna för behandlingar och deras stödsystem verkar vara extremt lätt för de valda riskkällorna (t.ex. stöld av pappersdokument lagrade i en lobby).

13 Appendix 2 – Lista på personuppgiftskategorier

Kategori (Tillgångar)	Exempel på personuppgifter
Anställningsinformation	• Uppgifter om anställningsförmåner • Anställningsnummer • Företagskredit- eller betalkortsnummer • Anspråk om ersättning till anställda • Jobbtitel/roll • Disciplinär åtgärd • Frånvaroregister/tidsspårning/årlig ledighet • Hälso- och säkerhetsrelaterad information och rapportering • Slutdatum och skäl för uppsägning • Tidigare arbetslivserfarenhet • Arbetstimmar • Avtalstyp - bestämd tidsperiod / tillfällig / fast anställning, etc. • Prestationsbedömning • Lön • Startdatum • Avgångsintervju och kommentarer • Detaljer om jobbansökan (t.ex. ansökningsblankett, intervjuanteckningar, referenser) • Överordnad chef • Klagomål • Kontorsadress • Verksamhet/Enhet • Personalnummer
Information om Arbetsmiljö	• Detaljer om mobbning och trakasserier
Information från Bakgrundskontroller	• Drogtestresultat • Referens- eller bakgrundskontroller • Belastningsregister • Trafikböter • Brottshistorik
Biometriska och genetiska uppgifter	• Näthinneskanning • Ansiktsigenkänning • Röstigenkänning • Fingeravtryck • Genetisk sekvens
Inloggningsuppgifter	• Kontonummer • Kontoålder • Kontolösenord
Familjeinformation	• Namn på föräldrar • Namn på barn • Namn på partner • Annan familjestatus & information om närstående
Finansiella uppgifter för individen	• Bankkontoinformation • Kontoutdrag • Bonusutbetalningar • Kreditkortsnummer • Ersättningsuppgifter • Uppgifter om lån, krediter, amorteringar etc • Finansiell status (inkomst, egendomar, investeringar)

Kontaktinformation	• Tidigare bostadsadress • Hemadress • Kontaktuppgifter vid nödfall • Telefonnummer • Personlig e-postadress • Kontaktuppgifter
Myndighetsutfärdad identifikation	• Personnummer • Körkortsnummer • Detaljer om nationellt identitetskort • E-tjänstekort • Pass • ID-kort • Skyddad identitet
Personlig identifikation	• Förnamn • Efternamn • Vikt • Födelsedatum • Religion/Religiös övertygelse • Sexuell läggning • Längd • Fullständigt namn • Civilstånd • Signatur • Etniskt ursprung • Nationalitet • Kön • Hälsa • Ålder • Foto, bild • Alias eller pseudonymer • Kännetecken
Information om resor och kostnader	• Resehistorik • Resebokningsinformation • Uppgifter om kostnader
Sociala välfärdsdata	• Arbetslöshetsersättning • Förtidspension • Försörjningsstöd eller andra bistånd (utsatthet, arbetslöshet, fattigdom)
Information om individens medverkan i Sociala medier	• Sociala medier - konto • Sociala medier - historik • Sociala medier - kontaktuppgifter
Personliga egenskaper, utbildning och arbete	• Examensbevis • Betyg • Utbildningshistorik • Språk • Akademiska meriter • Förbundsmedlemskap • Kvalifikationer/certifieringar • Curriculum vitae • Utvärderingsinformation • Fackligt medlemskap • Beteende och preferenser • Vanor, personliga preferenser & intressen, umgängesliv & kontakter • Utvärderingar av personlighet och beteende

Tekniska metadata	• Webbplatshistorik • Lokaliseringsdata (Position) • Cookie-information • IP-adress • Webbsökningstid • Trafikdata • Information om använda telefontjänster (Har ringt 1177 t.ex.) • Loggar (applikationsloggar, säkerhetsloggar etc.)

-